Note di Matematica Vol. IV, 149-434(1984)

I GRUPPI DI MATHIEU

Lino DI MARTINO

§ 1. INTRODUZIONE. Questa monografia intende presentare una "survey" (per quanto possibile, completa) delle proprietà dei cosiddetti gruppi di Mathieu. Si tratta di cinque gruppi semplici finiti, scoperti poco più di cent'anni fa da Emile Mathieu, e successivamente investigati da un numero considerevole di matematici. L'eccezionalità dei gruppi di Mathieu risiede nel fatto che, a differenza dei gruppi ciclici di ordine primo, dei gruppi alterni di grado > 4, e dei gruppi semplici di Chevalley (classici, eccezionali, e di tipo "twisted"), essi non fanno parte di una famiglia infinita di gruppi semplici, parametrizzata in modo naturale (mediante l'ordine, il grado, il rango (di' Lie) e l'ordine di un campo di Galois). Sono, in altre parole, dei gruppi semplici isolati, o, come si usa dire, "sporadici". I gruppi di Mathieu rimasero gli unici gruppi semplici sporadici conosciuti per circa un secolo, sino al 1965, quando Zvonimir Janko scoprì un nuovo gruppo sporadico (il "primo gruppo di Janko" J_1). Sono oggi noti 26 gruppi sporadici. Oltre ai gruppi di Mathieu, vi sono i gruppi di Conway Co_1, Co_2, Co_3; i gruppi di Fischer F_{22}, F_{23}, F_{24}'; i gruppi di Janko J_1, J_2, J_3, J_4; il gruppo di Fischer-Criess F_1 (Monster), e i suoi sottogruppi F_2 (Baby Monster), F_3 (gruppo

di Thompson, F_5 (gruppo di Harada Norton) ; i gruppi HS (di Higman-Sims), Mc (di McLaughlin), He (di Held), Ly (di Lyons), Sz (di Suzuki), ON (di O'Nan), Ru (di Rudvalis). E sono tutti, dal momento che la classificazione completa dei gruppi semplici finiti è giunta a termine (annuncio a Santa Cruz, California, nell'estate 1979; l'ultima tessera del mosaico essendo però, probabilmente, la dimostrazione dell'unicità di F_1, a Cambridge, da parte di S. Norton (febbraio 1981?)).

Si può ragionevolmente asserire che il ruolo dei gruppi di Mathieu nella scoperta di altri gruppi sporadici, nella loro caratterizzazione, e nella loro costruzione, è stato determinante. Oltre a ciò, delle geometrie naturali soggiacenti ai gruppi di Mathieu. e certe loro rappresentazioni, sono ben conosciute e stanno alla base di svariate applicazioni in altri settori di ricerca (e.g. teoria dei codici, geometrie finite e combinatorica). Sembra pertanto utile presentare una "survey" ragionata delle proprietà dei gruppi di Mathieu, e dei problemi in cui intervengono, in un ventaglio di prospettive abbastanza ampio.

Per la lettura del seguito, si ritengono indispensabili una conoscenza di base della teoria dei gruppi, e una certa familiarità con la teoria dei gruppi di permutazioni e delle rappresentazioni lineari dei gruppi finiti. Per ciò che riguarda specificamente i gruppi semplici, il lettore è rinviato a quanto contengono sull'argomento i testi standard di teoria dei gruppi (ma in particolare a Huppert (1967). Huppert. Blackburn (1982), e a Suzuki (1982)). alle "surveys" di vari specialisti

(e.g. Tits (1970). Feit (1970). Gorenstein (1974). Janko (1978). Aschbacher (1978). Gorenstein (1978). Gorenstein (1979). Aschbacher (1980), Syskin (1980). e ai seguenti volumi: "Finite simple groups" (Powell, Higman, ed. (1971)); "Finite simple groups 11" (Collins. ed. (1980)); "The Santa Cruz conference on finite groups" (Cooperstein. Mason, ed. (1980)); "Finite simple groups. An introduction to their classification " (Gorenstein (1982); "The Classification of finite simple groups. Volume 1: Groups of noncharacteristic 2 type" (Gorenstein (1983)). In particolare, Gorenstein (1982) (versione riveduta e ampliata di Gorenstein (1979) contiene: a) una descrizione dell'apparato concettuale necessario a percorrere le tappe del programma (di Gorenstein-Aschbacher) che ha condotto alla classificazione dei gruppi semplici; b) una descrizione abbastanza dettagliata dei 26 gruppi sporadici e del modo in cui sono stati scoperti e costruiti. Sui gruppi di Mathieu. ci risulta sia stata scritta una sola monografia con intenti sistematici (Greenberg (1973)). per molti versi limitata e superata. Non è possibile tuttavia non segnalare anche le lezioni di Conway (1971), che contengono un' elegante trattazione di vari aspetti dei gruppi di Mathieu, in relazione soprattutto ai legami con altri gruppi sporadici. Ad esse ci si riferirà più volte nel seguito. Notiamo infine che, salvo cenni concisi là dove era possibile e necessario, nèlla presente "survey" saranno omesse le dimostrazioni dei risultati, per le quali si rinvia, quando esistano, ai pertinenti riferimenti bibliografici.

Le notazioni adottate sono per lo più standard. Ci limitiamo dunque a fissarne alcune. e richiamiamo anche alcune nozioni, non necessariamente note a chi non si occupi di teoria dei

gruppi :

Sia G un gruppo finito. $|G|$ denota l'ordine di G. 1 denota sia l'unità di G, sia il sottogruppo banale costituito dall'unita di G, sia il gruppo banale di ordine uno. $H \simeq G$ denota che H è un gruppo isomorfo a G. G/N denota il gruppo quoziente di G rispetto a un sottogruppo normale N, $|G:H|$ l'indice di un sottogruppo H in G.

Siano A,B sottoinsiemi di G. AB denota l'insieme $\{ab \mid a \in A, b \in B\}$, prodotto di A e B. La notazione si estende in modo ovvio al prbdotto di un numero finito di sottoinsiemi di G. A^B denota l'insieme $\{ b^{-1}ab \mid a \in A, b \in B \}$. $\langle A \rangle$ denota il sottogruppo generato dal sottoinsieme A. e $\langle A^G \rangle$ la chiusura normale di A. Per ogni $x,y \in G$, $[x,y]$ denota il commutatore $x^{-1}y^{-1}xy$, e $[A,B]$ denota il sottogruppo $\langle \{ [a,b] \mid a \in A, b \in B \} \rangle$. $C_G(A)$ e $N_G(A)$ denotano risp. il centralizzante e il normalizzante di A in G.

Z(G) denota il centro di G. G' denota $[G,G]$, il sottogruppo derivato di G; inoltre $G^{(2)} = G'' = (G')'$, e in generale induttivamente $G^{(n)} = (G^{(n-1)})'$. O(G) denota il sottogruppo di Frattini di G, i.e. l'intersezione dei sottogruppi massimali di G. F(G) denota il sottogruppo di Fitting di G, i.e. il prodotto dei sottogruppi normali nilpotenti di G.

Sia p un numero primo. $Syl_p G$ denota un p-sottogruppo di Sylow di G. Un elemento di ordine p di G si dice p-centrale se è nel centro di un p-sottogruppo di Sylow di G. Un'involuzione (= elemento di ordine 2) 2-centrale si dice semplicemente

centrale. Un sottogruppo di G si dice p-locale se è il normalizzante di un p-sottogruppo non banale di G.

Sia π un insieme di numeri primi (e π' denoti l'insieme dei numeri primi non appartenenti a π). $O_\pi(G)$ denota il sottogruppo prodotto dei sottogruppi normali di G il cui ordine è divisibile solo per primi appartenenti a π ; $O^\pi(G)$ denota il sottogruppo intersezione dei sottogruppi H, normali in G, e tali che G/H abbia ordine divisibile solo per primi appartenenti a π. In particolare, $O_{p'}(G)$, p primo, è il pih grande sottogruppo normale di G di ordine primo con p (il "p'-core" di G). $O_{2'}(G)$ si denota semplicemente con O(G); è il "core" di G. Si supponga $O_{p'}(G) = 1$ (i.e. G "p'-core free"): G si dice p-costretto se $C_G(O_p(G)) \subseteq O_p(G)$. In generale: G si dice p-costretto se $G/O_{p'}(G)$ lo è.

Se A è un p-gruppo abeliano. m(A) denoti il numero minimo di generatori di A. Sia P un p-gruppo: $m(P) = \max\{ m(A) \mid A$ sottogruppo abeliano di P $\}$ è il rango di P; $r(P) = \max\{m(Q/Q') \mid Q$ sottogruppo di P$\}$ è il rango sezionale di P. Per ogni gruppo G, $m(Syl_p G)$ e $r(Syl_p G)$ sono rispettivamente il p-rango e il p-rango sezionale di G. (Il p-rango sezionale di G è il p-rango massimo di una sezione di G. (Si ricordi che si dice sezione di un gruppo X ogni immagine omomorfa di un sottogruppo di X)).

Aut (G) denota il gruppo degli automorfismi di G, Inn(G) il gruppo degli automorfismi interni di G. e Out(G) il gruppo degli "adtomorf ismi esterni" di G, Aut (G) /Inn(G) .

Siano A,B sottogruppi di G. Se G=AB, e [A,B] =1, si dice che G è pro

dotto centrale di A e B. Se, inoltre, $A \cap B = 1$, G è prodotto diretto di A e B, e si scrive $G = A \times B$. Se invece $A \cap B \neq 1$, si scrive $G = A * B$. Le precedenti definizioni e notazioni si estendono al prodotto di un numero finito di sottogruppi di G.

Siano A,B due gruppi, e si supponga che G contenga un sottogruppo normale $\bar{A} \simeq A$, tale che $G/\bar{A} \simeq B$. Si dice allora che G è un'estensione di A mediante B, e si scrive $G = A \cdot B$. Se inoltre G contiene un sottogruppo $\bar{B} \simeq B$. tale che sia $G = \bar{A}\bar{B}$ e $\bar{A} \cap \bar{B} = 1$ (i.e. $\bar{B}$ è un complemento di $\bar{A}$ in G). si dice che G è un'estensione spezzata (o prodotto semidiretto) di A mediante B, e si scrive $G = [A]B$. Se $\bar{A}$ non ammette complemento in G, si dice che G è estensione non-spezzata di A mediante B. Sia $G = [A]B$: per ogni $\bar{b} \in \bar{B}$, l'applicazione $\phi_{\bar{b}} : \bar{a} \to \bar{b}^{-1}\bar{a}\bar{b}$ è un automorfismo di $\bar{A}$, e $\phi : \bar{b} \to \phi_{\bar{b}}$ è un omomorf ismo da $\bar{B}$ a $\mathrm{Aut}(\bar{A})$. Se Φ è l'omomorf ismo nullo, $G = \bar{A} \times \bar{B}$, e si dice che l'estensione è banale; se Φ è un monomorfismo, si dice che l'estensione è fedele.

Hol(G) denota l'olomorfo di G, i.e. l'estensione spezzata "naturale" di G mediante Aut(G), definita come l'insieme delle coppie ordinate $(\phi, g)(\phi \in \mathrm{Aut}(G), g \in G)$, con il prodotto: $(\phi_1, g_1) \cdot (\phi_2, g_2) = (\phi_1 \phi_2, g_1^{\phi_2} g_2)$.

Un'estensione H di un gruppo A mediante un gruppo G si dice centrale se $A \subseteq Z(H)$. Se inoltre $A \subseteq Z(H) \cap H'$, si dice che H è un ricoprimento (covering) di G. In forza di un classico risultato di Schur. se G è un gruppo perfetto (i.e. $G = G'$), esiste un unico ricoprimento "universale" di G: i.e. esiste un unico ricoprimento $\ddot{H}$ di G, tale che ogni ricoprimento H

di G sia immagine omomorfa di $\ddot{H}$. $\ddot{H}$ è il ricoprimento completo (full covering) di G, e $\hat{Z} = Z(\hat{H})$ è il moltiplicatore di Schur di G. Per ogni ricoprimento H = A•G, A è immagine omomorfa di $\hat{Z}$. (Per una trattazione generale del moltiplicatore di Schur di un gruppo finito G, e dei nessi con le rappresentazioni projettive di G, rimandiamo ad es. a Huppert (1967). Kap. V, §23).

Un gruppo finito G si dice quasisempl ice se è perfetto e se G/Z(G) è semplice (i.e. se è un ricoprimento perfetto di un gruppo semplice). Un gruppo G si dice semisemplice se è prodotto centrale di sottogruppi quasisemplici. 0 se G=1. Si dice componente di un gruppo G ogni sottogruppo subnormale quasisemplice di G. Il sottogruppo generato da tutte le componenti di G si denota con E(G). E(G) è prodotto centrale delle componenti di G, è 1 'unico sottogruppo normale semisemplice massimale di G, e centralizza il sottogruppo di Fitting F(G) .F*(G)=E(G)F(G) si dice sottogruppo di Fitting generalizzato di G.

Per le nozioni elementari di teoria dei gruppi di permutazioni, si rinvia, oltre che ai testi standard di teoria dei gruppi, alle monografie di Wielandt (1964) e Passman (1968). Riguardo alle notazioni: Se G è un gruppo di permutazioni su un insieme Ω di cardinalità $n < \infty$, e Δ è un sottoinsieme di Ω, $G_{[\Delta]}$ denota lo stabilizzante di A come insieme, i.e. il sottogruppo $\{g \in G \mid \Delta^g = \Delta\}$, e G_Δ denota lo stabilizzante di ogni punto di A, i.e. il sottogruppo $\{g \in G \mid \delta^g = \delta, \forall \delta \in \Delta\}$, normale in $G_{[\Delta]}$. Se H è un sottogruppo di G, contenuto in $G_{[\Delta]}$, H^Δ denota la costituente di H su Δ, i.e. il gruppo di permutazioni, isomorfo

a H/H_Δ, indotto da H su Δ. Per ogni sottogruppo H di G, Fix{H} denota l'insieme dei punti di Ω fissati da ogni elemento di H. Se $g \in G$ è decomponibile nel prodotto di r_i cicli disgiunti di lunghezza i (i=1,...,n), si dice che g è una permutazione di tipo $\prod_{i=1}^{n} i^{r_i}$. S_Ω, A_Ω denotano rispettivamente il gruppo simmetrico e il gruppo alterno su Ω. Se $|\Omega| = n$, si scrive anche S_n per S_Ω, e A_n per A_Ω. Ricordiamo infine che una rappresentazione di permutazione di un gruppo X su un insieme Ω è un omomorfismo f da X a S_Ω, e che due rappresentazioni di permutazione f,f' di X su due insiemi Ω ; Ω' si dicono equivalenti se esiste una bijezione $\theta: \Omega \to \Omega'$, tale che sia $f' = \theta^{-1} f \theta$.

Con il termine comune di gruppi di Chevalley (definiti su campi di Galois GF(q)) si indicano nel seguito tutti i gruppi finiti "del tipo di Lie", i.e. sia i gruppi di tipo A_ℓ, B_ℓ, C_ℓ D_ℓ ; sia i gruppi (eccezionali) di tipo G_2, F_4, E_6, E_7, E_8; sia le variazioni di Steinberg-Tits e Suzuki-Ree (gruppi "twisted"). Per le definizioni, e le notazioni corrispondenti, si rinvia a Steinberg (1967) e a Carter (1972). Si noti però che i gruppi "classici", i .e. i gruppi lineari, unitari, simplettici e ortogonali, saranno generalmente indicati con le loro notazioni tradizionali (e.g. GL,PGL,PSL,PSU,PSp,$O^{\pm}$, ecc.; cfr. ad es. Carter (1972)) , invece che con le notazioni della teoria di Lie.

In particolare, denotato con PG(n,q) lo spazio projettivo n-dimensionale su GF(q), e con AG(n,q) lo spazio affine n-dimensionale su GF(q), P Γ L(n+l,q) denota il gruppo di tutte le collineazioni di PG(n,q), PGL (n+l,q) il gruppo generato

dalle collineazioni centrali, e PSL(n+1,q) il gruppo generato dalle elazioni (il "piccolo gruppo projettivo"); $A\Gamma L(n,q)$, AGL(n,q) e ASL(n,q) denotano i gruppi affini corrispondenti, operanti su AG(n,q). (Per le varie nozioni di natura geometrica, usate ma non definite esplicitamente nel seguito, si rinvia a Dembowski (1968).)

Le presentazioni di un gruppo G sono denotate nel modo usuale. Precisamente, se $\{x_1,\ldots,x_n\}$ è un insieme di generatori, e $\{r_1,\ldots,r_m\}$ è un sistema completo di relatori che definiscono G, si scriverà: $G = \langle x_1,\ldots,x_n | r_1 = \ldots = r_m = 1 \rangle$.

C_n denota il gruppo ciclico di ordine n. D_{2n} $(n \geq 2)$ denota il gruppo diedrale di ordine 2n, i.e. $D_{2n} = \langle x,y | x^n = y^2 = 1, y^{-1}xy = x^{-1} \rangle$. S_{2^n} $(n \geq 4)$ denota il gruppo quasidiedrale di ordine 2^n, i.e. $S_{2^n} = \langle x,y | x^{2^{n-1}} = y^2 = 1, y^{-1}xy = x^{-1+2^{n-2}} \rangle$. Q_{2^n} $(n \geq 3)$ denota il gruppo quaternionale di ordine 2^n, i.e. $Q_{2^n} = \langle x,y | x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, y^{-1}xy = x^{-1} \rangle$. E_{p^n} (p primo) denota il gruppo abeliano elementare di ordine p^n (i.e. $E_{p^n} \simeq \overset{n}{\underset{1}{\times}} C_p$).

Ricordiamo che un p-gruppo P si dice speciale se è abeliano elementare, oppure se $P' = \Phi(P) = Z(P)$ è abeliano elementare. Un p-gruppo speciale non abeliano di ordine p^n, con centro di ordine p^s, si denoterà a volte concisamente con $p^{s+(n-s)}$. Un p-gruppo P speciale non abeliano, con centro di ordine p. si dice extraspeciale. Ogni p-gruppo extraspeciale è prodotto centrale di p-sottogruppi extraspeciali di ordine p^3 se P

$= H_1 * H_2 * \ldots * H_r$, H_i extraspeciale di ordine p^3, si dice che r è l'"ampiezza" di P. In tal caso. $|P| = p^{1+2r}$, e P si denota concisamente con p^{1+2r}. Per ogni primo p, vi sono due classi d'isomorfismo di p-gruppi extraspeciali di ordine p^3. In particolare, per p = 2, un 2-gruppo extraspeciale di ordine 2^3 è isomorfo a D_8, oppure a Q_8, e si ha $D_8 * D_8 \simeq Q_8 * Q_8$. Scende subito che un 2-gruppo extraspeciale P di ampiezza r è isomorfo al prodotto centrale di r gruppi diedrali D_8, oppure al prodotto centrale di r gruppi, di cui r-l diedrali DB, e uno quaternionale Q,: i.e. $P \simeq * \Pi_1^r D_8$, oppure $P \simeq (* \Pi_1^{r-1} D_8) * Q_8$. Nel primo caso si si dice che P è di tipo +, e si denota con il simbolo 2_+^{1+2r}, mentre nel secondo caso si dice che P è di tipo -, e si denota con 2_-^{1+2r}. (Le notazioni sono motivate dal fatto che, considerando $P/Z(P) \simeq E_{2r}$ come uno spazio vettoriale su GF(2), l'applicazione $xZ(P) \to x^{22}$ definisce una forma quadratica su GF(2), rispetto alla quale risulta $Out(P) \simeq O^-(2r,2)$, e $Out(P) \simeq O^+(2r,2)$, i.e. l'indice di Witt è massimale, se e solo se $P \supseteq E_{2n+1}$).

Avvertenza: Nel seguito sarà a volte indicata in modo sommario la struttura normale di certi gruppi (e.g. centralizzanti di involuzioni di gruppi semplici). Si scriverà, ad esempio, H = (A•B)•C per indicare che H si ottiene estendendo A mediante B, ed estendendo poi A•B mediante C. Se necessario, si specificheranno l'azione di B su A, e quella di C su A•B, e in particolare si useranno le notazioni già introdotte per indicare eventuali estensioni spezzate o banali.

§2. COSTRUZIONE DEI GRUPPI DI MATHIEU

1 gruppi di Mathieu furono scoperti da E. Mathieu nell'ambito dello studio delle "funzioni transitive di più variabili" (Mathieu (1860,1861,1873)). Si tratta di cinque grupgi di permutazioni, di grado 11,12,22,23,24 rispettivamente: sono usualmente denotati con M_i (i=11,12,22,23,24).

M_{12} è un gruppo sottilmente S-transitivo di ordine 12.11.10.9.8; M_{11} è lo stabilizzante di un punto in M_{12}, e pertanto è un gruppo sottilmente 4-transitivo di ordine 11.10.9.8.
M_{24} è un gruppo 5-transitivo di ordine 24.23.22.21.20.48 (i.e. lo stabilizzante di 5 punti è un sottogruppo di ordine 48); M_{23} è lo stabilizzante di un punto in M_{24}, e pertanto è 4-transitivo di ordine 23.22.21.20.48; M_{22} è lo stabilizzante di 2 punti in M_{24}, 3-transitivo di ordine 22.21.20.48.
M_{12} è un sottogruppo di M_{24} (Frobenius (1904)). e M_{11} è un sottogruppo di M_{23} (ma $M_{12} \not\subset M_{23}$, e $M_{11} \not\subset M_{22}$).

I gruppi $M_{11}, M_{12}, M_{23}, M_{24}$ sono gli unici gruppi di permutazioni 4- e j-transitivi, che non siano simmetrici o alterni.

Numerosi contributi sono stati portati al tentativo di dimostrare per via diretta la non-esistenza di gruppi di permutazioni 6-transitivi, che non siano simmetrici o alterni. A tutt'oggi, questo risultato non è stato raggiunto. Tuttavia, 1 'avvenuto completamento della classificazione dei gruppi semplici finiti produce come risultato collaterale la. classificazione di tutti i gruppi di permutazioni 2-transitivi. Da ciò segue per ispezione 1 'unicità dei gruppi di Mathieu, e la

non-esistenza di gruppi o-transitivi non banali (Cfr.§9. Per una discussione dell'impatto della classificazione dei gruppi semplici su varie aree della teoria dei gruppi di permutazioni, cfr. l'eccellente "survey" di Cameron (1981)).

1) Nella memoria del 1860 Mathieu inaugura lo studio delle funzioni transitive di più variabili. Se $F=F(x_1,\ldots,x_n)$ è una funzione di n variabili $x_1,\ldots,x_n$, a F è naturalmente associato un gruppo di permutazioni su $\{1,\ldots,n\}$, i.e. il gruppo delle permutazioni sulle variabili $x_1,\ldots,x_n$ che lasciano F invariante. Nella terminologia di Mathieu, F si dice k-transitiva se il gruppo di permutazioni corrispondente è k-transitivo su $\{1,\ldots,n\}$. Pertanto, ogni risultato enunciato e dimostrato da Mathieu in termini di funzioni transitive, è immediatamente traducibile in un risultato sui gruppi di permutazioni corrispondenti. In particolare Mathieu (1860), dopo aver esposto alcuni risultati elementari sui gruppi transitivi, dimostra l'esistenza delle funzioni 3-transitive corrispondenti ai gruppi proiettivi PGL(2,q). Nella memoria del 1861, Mathieu sviluppa la teoria delle funzioni transitive, elaborando un metodo di calcolo che gli consente di ottenere funzioni multiplamente transitive di $p = 2q+1$, e di $p+1$ variabili (con p e q numeri primi). Il metodo di Mathieu (ripreso con varianti nella memoria del 1873). equivale, di fatto, alla costruzione di estensioni di gruppi transitivi assegnati (e in ciò adombra la tecnica delle estensioni transitive sviluppata da Jordan (cfr.II)). In particolare, nel caso p=7 Mathieu costruisco $PSL(2,7) \simeq GL(3,2)$ e il gruppo affine AGL(3,2), e nel caso p=11 scopre

il gruppo S-transitivo M_{12}. Si limita poi ad asserire di avere trovato una funzione di 24 variabili, invariante per un gruppo di permutazioni S-transitivo di ordine 24.23.22.21.20.48. Solo nella memoria del 1873, Mathieu torna su M_{24}. In questa memoria, riesamina il caso p=11, e produce generatori espliciti per i gruppi M_{11} e M_{12} (cfr. 510). Si volge poi al caso $p = 23 = 2.11 + 1$, e sulla base di calcoli molto laboriosi costruisce M_{23}; previa aggiunzione di una ulteriore variabile e di una permutazione opportuna, ottiene infine M_{24}. Il procedimento dà luogo anche in questo caso a generatori espliciti per M_{23} e M_{24} (cfr. §10.).

La costruzione di M_{24} secondo le linee di Mathieu (1873) non è interamente persuasiva, e resta comunque piuttosto "misteriosa" Lo stesso Mathieu, del resto, ammette che le dimostrazioni nel caso di M_{24} non hanno "ni la netteté ni l'élégance" degli altri suoi risultati, e che a ciò è dovuto il ritardo nella pubblicazione. Si può perciò convenire con Witt (1938A), che M_{24} era destinato ad "avere una vita difficile". Jordan (1874). pur non avanzando dubbi espliciti sulla costruzione di Mathieu, osservo che l'esistenza di gruppi così notevoli sembrava dipendere dal concorso di circostanze eccezionali, piuttosto che dall'essere il numero delle variabili uguale a p o p+1, con p=2q+1, p e q numeri primi (come riteneva Mathieu). Nulla di simile accadeva infatti per p=47 e p=59. Miller (1898) giunse a "dimostrare" la non-esistenza di M_{24}. Ma si corresse successivamente, mettendo in evidenza una lacuna nella "dimostrazione", e provò la semplicità di M_{22}, M_{23} e M_{24} (Miller (1900)). Frobenius

(1904) determinò le classi di coniugio e le tavole dei caratteri dei gruppi di Mathieu. Osservo inoltre che M_{24} contiene sottogruppi isomorfi a M_{12}, e che M_{12} contiene due classi di sottogruppi isomorfi a M_{11} (la classe degli stabilizzanti di punto, e una classe di sottogruppi 3-transitivi di grado 12. fuse da un automorfismo esterno di M_{12}). La dimostrazione di tali risultati, omessa da Frobenius, si trova in Witt (1938 A) (cfr.§3.). de Séguier (1904) costruì M_{24} e M_{12} ampliando i gruppi proiettivi PSL(2,23) e PSL(2,11), rispettivamente. Anche il metodo di de Séguier, che consiste nell'ampliare il gruppo proiettivo, nella sua azione naturale sulla retta, mediante un'opportuna permutazione, comporta calcoli eccessivamente laboriosi (in particolare, de Séguier produce generatori espliciti per M_{12} e M_{24} (cfr. 510.)).

II) La prima costruzione concettualmente soddisfacente dei gruppi di Mathieu si deve a Witt (1938A), e si fonda su risultati di carattere generale concernenti il metodo delle estensioni transitive, sviluppato da Jordan (cfr. Jordan (1870)).

Se G è un gruppo di permutazioni su un insieme Ω, si dice *estensione transitiva* (puntuale) di G ogni gruppo di permutazioni H, transitivo su un insieme $\Omega' = \Omega \cup \{\alpha\}$, con $\alpha \notin \Omega$, e tale che sia $H_\alpha = G$ (convenendo che sia $(\alpha)g = \alpha$ per ogni $g \in G$). Se H ha rango r su Ω' (i.e. $H_\alpha = G$ ha r orbite su Ω'), si dice che H è una *estensione di* G *di rango* r. In particolare, r=2 se e solo se G è transitivo su Ω, e, se G è k-transitivo su Ω ($k > 1$). H è (k+1)-transitivo su Ω'.

Jordan (1870) per primo affronta in modo esplicito il problema di stabilire sotto quali condizioni, assegnato un gruppo G transitivo su Ω, si possa aggiungere un nuovo punto α ad Ω e definire una opportuna permutazione h su $\Omega \cup \{\alpha\}$, in modo che il gruppo $H = \langle G,h \rangle$ sia transitivo su $\Omega \cup \{\alpha\}$, e sia $H_\alpha = G$. Jordan formula alcune condizioni. necessarie e sufficienti per l'esistenza di un'estensione, e se ne serve in particolare per costruire M_{12} (cfr. Jordan (1870),pp.33-34).

Witt (1938A) sviluppa ulteriormente il metodo di Jordan, e fonda la sua costruzione sul seguente:

TEOREMA. Sia $G = G_k$ un gruppo k-transitivo ($k \geq 2$) su un insieme $\Omega_k = \{\alpha_{k-1}, \alpha_k, \dots\}$. e sia $\Omega_{k+1} = \Omega_k \cup \{\alpha_{k+1}\}$.

Si supponga che esistano h_k e G_k e $h_{k+1} \in S_{\Omega_{k+1}}$ soddisfacenti le condizioni seguenti: i) h_k scambia fra loro α_{k-1} e α_k; ii) h_{k+1} scambia fra loro α_k e α_{k+1}, e fissa α_{k-1}; iii) $(h_{k+1})^2$ e $(h_k h_{k+1})^3$ appartengono a G_k; iv) $h_{k+1}(G_k)_{\alpha_k} h_{k+1} = (G_k)_{\alpha_k}$. Allora il gruppo $G_{k+1} = \langle G_k, h_{k+1} \rangle = G_k \cup G_k h_{k+1} G_k$ è un'estensione transitiva di G_k su Ω_{k+1}.

Il Teorema precedente è applicabile nei casi seguenti:

(1) Si consideri come gruppo $G=G_2$ il gruppo projettivo PSL(3,4), 2-transitivo nella sua azione naturale sui 21 punti del piano PG(2,4). Si ponga $\alpha_1=(0,1,0)$, $\alpha_2=(0,0,1)$, $h_2=(x,y,z) \to (y,x,z)$, $h_3=s_3(\alpha_2\ \alpha_3)$, $h_4=s_4(\alpha_3\ \alpha_4)$, $h_5=s_5(\alpha_4\ \alpha_5)$, dove $s_3=$:

$(x,y,z) \to (x^2+yz, y^2, z^2)$, $s_4 =: (x,y,z) \to (x^2, y^2, \rho z^2)$, $s_5 =: (x,y,z) \to (x^2, y^2, z^2)$, e $\langle \rho \rangle = GF(4)^*$.

In forza del Teorema precedente, si ottengono tre successive estensioni G_3, G_4, G_5, che sono precisamente i gruppi di Mathieu M_{22}, M_{23}, M_{24}, di grado 22,23,24. (Nel seguito,pertanto,si porrà spesso $PSL(3,4) = M_{21}$.)

(2))(Si consideri come -gruppo $G=G_3$ il sottogruppo del gruppo $P\Gamma L(2,9)$, costituito dalle permutazioni della retta projettiva $PG(1,9) = GF(9) \cup \{\infty\}$ così definite: $x \to (ax^\gamma + b)/(cx^\gamma + d)$, dove $\gamma = 1$ se ad-bc è un quadrato non nullo di GF(9), $\gamma = 3$ se ad-bc non è un quadrato in GF(9). Tale sottogruppo si indica con M_{10}, ha indice 2 in $P\Gamma L(2,9)$, ed è sottilmente 3-transitivo su PG(1,9). ($P\Gamma L(2,9) = Aut(A_6)$ ha tre sottogruppi distinti di indice 2: $PGL(2,9), S_6$ e M_{10}.)

In forza del Teorema precedente, si ottengono due successive estensioni $G_4 = \langle M_{10}, h_4 \rangle$, e $G_5 = \langle G_4, h_5 \rangle$, qualora si ponga $h_4 = s_4(\alpha_3\ \alpha_4)$, $h_5 = s_5(\alpha_4\ \alpha_5)$, con $\alpha_3 = \infty$, $s_4 =: x \to \sigma^2 x + \sigma^3$, $s_5 =: x \to x^3$ e $\langle \sigma \rangle = GF(9)^*$, $\sigma^2 + \sigma = 1$.

G_4 è il gruppo di Mathieu M_{11}, sottilmente 4-transitivo di grado 11, e G_5 è il gruppo di Mathieu M_{12}, sottilmente 5-transitivo di grado 12.

Witt dimostra poi senza difficoltà che i gruppi di Mathieu sono semplici. Infatti, $M_{21} = PSL(3,4)$ è semplice (come tutti i gruppi $PSL(n,q)$ con $(n,q) \neq (2,2),(2,3)$), e si può provare direttamente, con argomenti "ad hoc", che M_{11} è semplice. La semplicità dei restanti gruppi di Mathieu segue allora

immediatamente, poiché un gruppo di permutazioni G, primitivo su un insieme Ω e privo di sottogruppi normali regolari, è semplice se G_α è semplice ($\alpha \in Sa$).

Witt prova infine che M_i ($i=11,12,22,23,24$) è l'*unica* estensione transitiva di M_{i-1}, e che M_{12} e M_{24} non ammettono ulteriori estensioni transitive.

Questi ultimi risultati, per i gruppi M_{22}, M_{23}, M_{24} erano già stati ottenuti, in un contesto spiccatamente geometrico, da Zassenhaus (1935). Zassenhaus dimostra che, se G è un gruppo di collineazioni di $PG(n,q)$, $n \geq 2$, contenente il piccolo gruppo projettivo $PSL(n+1,q)$, esiste un'estensione transitiva H di G, considerato come gruppo di permutazioni sui punti di $PG(n,q)$, se e solo se $q=2$, oppure $q=4, n=2$ e $|G:PSL(3,4)| \leq 2$. Se $q=2$, un'estensione H di G è ad esempio il gruppo affine $[T]G \leq AGL(n+1,2)$, ove T è il gruppo delle traslazioni di $AG(n+1,2)$; se $q=4$, H è isomorfo a M_{22} oppure a $Aut(M_{22})$. Infine, M_{22} è ulteriormente estendibile, e in modo unico, a M_{23} e a M_{24}.

(Allo stesso risultato giunge Hughes (1965B), sotto le ipotesi più deboli che G sia transitivo sui punti di $PG(n,q)$, e contenga una collineazione non banale che fissa i punti di un iperpiano).

Tits (1964) ha generalizzato il risultato di Zassenhaus (1935) a un campo arbitrario. Se G è un gruppo di collineazioni di uno spazio projettivo di dimensione $n \geq 2$ su un campo K, contenente un gruppo di projettività transitivo sulle r-ple di punti linearmente indipendenti, con $r=\inf(4,n+1)$, e se G ammette un'estensione transitiva, allora $K=GF(2)$, oppure $n=2$ e $K=GF(4)$.

Tits (1970) enuncia poi (senza dimostrazione) l'ulteriore generalizzazione: Se G è un gruppo di collineazioni di uno spazio projettivo di dimensione $n \geq 1$ su un corpo K (non necessaria mente commutativo), contenente PSL(n+1,K), G ammette un'estensione transitiva solo nei casi seguenti: i) K=GF(2); ii) n=l e K= GF(3), GF(4); iii) $G=M_{10},M_{21},[M_{21}]C_2$.

(L'indagine delle estensioni transitive ha avuto esiti molto importanti nella teoria dei gruppi finiti. Ci limitiamo a segnalare che:

1) Risultati conclusivi sono stati ottenuti da vari autori, circa l'esistenza di eventuali estensioni transitive dei gruppi classici, considerati nell'azione transitiva su varie configurazio ni delle loro geometrie naturali. In quest'ordine di problemi, si sono sovente utilizzati metodi geometrico-combinatori, legati all'estendibilita o meno di disegni (cfr.§3), associati ai gruppi in questione (si veda ad es. Dembowski (1965), Hughes (1965A,1965B), Liineburg (1969)). Si tratta di risultati che assicurano, in generale, la non-esistenza di estensioni transitive dei gruppi considerati, i.e. la non-esistenza di "analoghi" inaspettati dei gruppi di Mathieu. Più in generale, risultati dello stesso tipo sono stati ottenuti per i gruppi di Chevalley su GF(q) (e.g. nell'azione sui laterali di un sottogruppo parabol ico (Tits) , ovvero quando (q,|Ω|)=1 (Seitz)).

2) Tutti i gruppi di Chevalley su GF(q) ammettono rappresentazio ni di permutazione transitive di rango ≤ 5, in cui lo stabilizzante di un punto è un sottogruppo parabolico. In particolare, i gruppi classici (e il gruppo di Dickson E_6) ammettono rappresentazioni

cosiffatte di rango 3. Ciò motivò D.Higman (cfr. D. Higman (1964)) ad iniziare lo studio generale dei gruppi semplicemente transitivi di rango 3. Tale studio, proseguito da Higman e da altri, ha conosciuto uno sviluppo intensivo dopo la costruzione del gruppo sporadico J_2 come estensione transitiva di rango 3 di PSU(3,3) (Hall, Wales (1968)), avendo appunto come obiettivo primario la scoperta e la costruzione di nuovi gruppi semplici come estensioni transitive di rango 3 di gruppi noti. Per questa via sono stati effettivamente scoperti quattro gruppi sporadici (HS, Mc, Sz e Ru; cfr. §13). Notiamo infine che estensioni di rango > 3 intervengono nella costruzione di altri gruppi sporadici (e.g. di rango 5 nel caso di F_2).)

§3. COSTRUZIONE DEI SISTEMI DI STBINER ASSOCIATI AI GRUPPI DIMATHIEU

La costruzione di Witt mette in luce delle "geometrie" naturali, soggiacenti ai gruppi di Mathieu. Witt (1938A,1938B) fa infatti seguire alla costruzione dei gruppi di Mathieu la loro caratterizzazione come gruppi di automorfismi di certi sistemi di Steiner.

1) Ricordiamo, qui di seguito, alcuni concetti e risultati della teoria dei disegni, indispensabili sia in questo paragrafo che nei successivi.

Sia Ω un insieme di cardinalità $n < \infty$, $\Omega^{(m)}$ l'insieme dei sottoinsiemi di Ω aventi cardinalità m. e sia B un sottoinsieme (non vuoto) di $\Omega^{(m)}$ con la proprietà che ogni sottoinsieme di Ω di cardinalità t è contenuto in esattamente λ elementi di B. Si dice allora che la coppia (Ω,B) è un t-*disegno* D di parametri n,m,λ, o brevemente che $D=(\Omega,B)$ è un t-(n,m,λ) disegno. Per escludere casi banali si suppone generalmente $n>m>t>1$. Gli elementi di Ω sono i *punti* di D, e gli elementi di B sono i *blocchi* di D; si vede subito che $|B|=\binom{n}{t}\lambda/\binom{m}{t}$. In ogni 2-$(n,m,\lambda)$ disegno D, con $2\leq m<n$, si ha $n=|\Omega| \leq |B|$ (disuguaglianza di Fischer), e $\Omega| = |B|$ se e solo se, per ogni $b_1,b_2\in B$, $b_1\neq b_2$, è $|b_1 \cap b_2) = \lambda$. Un 2-disegno per il quale $\Omega| = |B|$ si dice *simmetrico*. Un 2-disegno simmetrico, con $n=2m+1$, si dice 2-*disegno di Hadamard*. Un disegno D, con $\lambda = 1$, si dice *sistema di Steiner*, e si indica con S(t,m,n).

Sia $D = (\Omega, B)$ un $t\text{-}(n,m,\lambda)$ disegno, e sia B_α l'insieme dei blocchi di D contenenti α, ciascuno privato del punto α. La coppia $D_\alpha = (\Omega \setminus \{\alpha\}, B_\alpha)$ è un $(t-1)\text{-}(n-1.m-1,X)$ disegno, che si dice *contrazione* di D nel punto α. Se posto $\Omega^+ = \Omega \dot{\cup} \{\infty\}$, esiste un $(t+1)\text{-}(n+1,m+1,\lambda)$ disegno $D^+=(\Omega^+,B^+)$, la cui contrazione nel punto ∞ coincide con (Ω,B), si dice che D^+ è un' *estensione* di D. Siano $Dl = (\Omega_1,B_1)$, $D_2 = (\Omega_2,B_2)$ due t-disegni. Una bijezione $f : \Omega_1 \to \Omega_2$ che induca una bijezione $\bar{f} : B_1 \to B_2$ (i.e. che porti blocchi in blocchi) si dice *isomorfismo* fra Dl e D_2. In particolare, se $D = (\Omega, B)$ è un disegno, una permutazione su Ω che porta blocchi in blocchi si dice *automorfismo di* D. Il gruppo degli automorfismi di D si indica con Aut(D).

Centrali nella teoria dei disegni sono i problemi: 1) dell'*esistenza* di t-disegni di assegnati parametri n,m,λ; 2) della classificazione dei $t\text{-}(n,m,\lambda)$ disegni di assegnati parametri (in particolare della loro eventuale *unicità* a meno d'isomorfismi); 3) dell'*estendibilità* di un assegnato disegno D (un'estensione può non esistere, o, se esiste, non essere unica); 4) della determinazione di Aut(D), ovvero. della determinazione dei disegni D per i quali Aut(D) soddisfa certe condizioni (e.g. condizioni di transitivita sui punti e/o sui blocchi).

Per una trattazione sistematica dei disegni, e dei problemi sopra accennati, ci si può riferire a Hall (1967). e a Dembowski (1968) (che contiene una bibliografia pressoché completa fino al 1968, e di cui è in preparazione una nuova edizione aggiornata). Segnaliamo inoltre le belle monografie di Cameron (1976) e Cameron, van Lint (1980), la "survey" di Kantor (1975B) e,

con riferimento specifico ai sistemi di Steiner, la raccolta di articoli edita da **Lindner,Rosa** (1980). che contiene fra l'altro una completa "survey" bibliografica a cura di **Doyen** e Rosa.

Ci limitiamo qui a menzionare alcuni risultati sui sistemi di Steiner, che riguardano direttamente il nostro argomento:

a) Esempi classici di sistemi di Steiner sono gli spazi projettivi e gli spazi affini su un campo di Galois GF(q). I punti e le rette di uno spazio projettivo PG(d,q) di dimensione $d > 1$ su GF(q) sono infatti i punti e i blocchi di un sistema di Steiner $S(2,q+1,(q^{d+1}-1)/(q-1))$. I punti e le rette di uno spazio affine AG(d,q) di dimensione $d > 1$ su GF(q) sono invece i punti e i blocchi di un sistema di Steiner $S(2,q,q^d)$. AG(d,2), considerato come sistema di Steiner. è banale. Tuttavia, per q=2, i punti e i piani dello spazio affine formano un sistema di Steiner $S(3,4,2^d)$, che si indica solitamente con $AG_2(d,2)$.

b) In ogni sistema di Steiner S(t,m,n), con $n > m > t \geq 2$, vale la disuguaglianza: $n-t+1 \geq (m-t+2)(m-t+1)$. Si ha l'uguaglianza solo nei casi seguenti: i) t=2, m=h+1, $n=h^2+h+1$; ii) $t \geq 2$, (t,m,n) = (3,4,8), (3,6,22), (4,7,23), (5,8,24), (3,12,112) (cfr. Cameron (1980)).

Un sistema di Steiner $S(2,h+1,h^2+h+1)$ si dice *piano projettivo* di ordine h. (In particolare, dunque, PG(2,q) è un piano projettivo di ordine q). Un'eventuale estensione di un piano projettivo di ordine h ha necessariamente una delle terne di parametri

elencate in ii): si deduce quindi che un piano projettivo è estendibile solo se h=2,4, o 10 (Cfr. questo risultato con gli analoghigruppali descritti in §2). Si noti che PG(2,2) è l'unico piano projettivo di ordine 2. e PG(2,4) è l'unico piano projettivo di ordine 4, mentre la questione dell'esistenza di un piano di ordine 10 è irrisolta. Infine: 1) nel caso di PG(2,2), l'estensione esiste ed è unica: esiste infatti un unico sistema S(3,4,8), non ulteriormente estendibile, ed è $AG_2(3,2)$; 2) nel caso di PG(2,4), esistono tre successive estensioni, che sono precisamente i sistemi di Steiner associati a M_{22}, M_{23}, e M_{24}.

c) Rimuovendo un blocco (la "retta impropria") e tutti i suoi punti da un piano projettivo di ordine h, si ottiene un sistema di Steiner $S(2,h,h^2)$. Un sistema con tali parametri si dice *piano affine* di ordine h. (In particolare, dunque, AG(2,q) è un piano affine di ordine q). Un'eventuale estensione di un piano affine di ordine h è un sistema di Steiner $S(3,h+1,h^2+1)$: un sistema di Steiner con tali parametri si dice *piano inversivo* (o piano di Mobius) di ordine h. Per una trattazione generale dei piani inversivi, rinviamo a Dembowski (1968). Ricordiamo soltanto che, se $\mathcal{O}$ è un ovoide di PG(3,q), i.e. un insieme di q^2+1 punti di PG(3,q) che non contiene tre punti allineati, i punti di $\mathcal{O}$ e le sue sezioni piane non banali sono i punti e i blocchi di un piano inversivo di ordine q. Se $\mathcal{O}$ è una quadrica non rigata di PG(3,q), tale piano si dice *classico* (o *miqueliano*), e si indica con M(q). Alternativamente, M(q) può essere costruito assumendo come punti i punti di $PG(1,q^2)$,

e come blocchi le immagini di PG(1,q) c PG(1,q^2) per l'azione di P $\Gamma L(2,q^2)$. In particolare, Aut(M(q)) = P $\Gamma L(2,q^2)$. Notiamo infine che: 1) AG(2,3) è l'unico piano affine di ordine 3; 2) AG(2,3) ammette una sola estensione, il piano inversivo classico M(3); 3) M(3) è l'unico piano inversivo di ordine 3, è estendibile due volte in un unico modo, e le sue estensioni sono precisamente i sistemi di Steiner associati a M_{11} e M_{12}. Di fatto, un piano inversivo di ordine h > 2 ammette un'estensione solo se h=3 o h=13, e in quest'ultimo caso l'eventuale estensione ammette almeno una contrazione costituita da un piano inversivo non classico di ordine 13 (cfr. Kantor (1974)).

2) (Le costruzioni di Witt).

i) Witt osserva che M_{24}, in forza della sua struttura di gruppo 5-transitivo, determina in modo naturale un sistema di Steiner S(5,8,24). Vale infatti, in generale, il seguente:

TEOREMA (Witt (1938A)). Sia $G \leq S_\Omega$ t-transitivo su Ω, e $\Delta \subset \Omega$, con $|\Delta| = t$. Sia $U \neq 1$ un sottogruppo di G_Δ, $\Phi = Fix\{U\}$, $|\Phi| = m > t$, e si supponga che se $U^g \subseteq G_\Delta$ ($g \in G$), allora $U^g = U$. Posto $B = \{ \Phi^g \mid g \in G \}$, (Ω, B) è un sistema di Steiner S(t,m,n), e G è un gruppo di automorfismi di (Ω, B).

Se G è M_{24}, S-transitivo su Ω, e A è un sottoinsieme di Ω di cardinalità 5, G_Δ è un gruppo di ordine $2^4 \cdot 3$, prodotto semidiretto di un 2-gruppo abeliano elementare U di ordine 2^4 per un gruppo ciclico di ordine 3. $\Phi = Fix\{U\}$ ha cardinalità 8, e in forza del teorema precedente i coniugati di U in M_{24}

producono i 759 blocchi (ottadi) di un sistema di Steiner S(5.8.24).

Con una contrazione in un punto α di Ω, a $(M_{24})_\alpha \simeq M_{23}$ resta allora associato un sistema di Steiner S(4,7,23), costituito da 253 blocchi (7-adi). Con una seconda contrazione in β ($\neq \alpha$) a $(M_{24})_{\alpha,\beta} \simeq M_{22}$ è associato un sistema di Steiner S(3,6,22), costituito da 77 blocchi (esadi). E infine una terza contrazione riconduce al piano projettivo S(2,5,21) = PG(2,4).

Naturalmente, la costruzione precedente mostra che M_i (i=22,23, 24), è (i-19)-transitivo sui punti, e transitivo sui blocchi del corrispondente sistema di Steiner. Si ha inoltre: $Aut(S(5,8,24)) = M_{24}$, $Aut(S(4,7,23)) = M_{23}$, e $Aut(S(3,6,22)) = Aut(M_{22}) = M_{22}\cdot C_2$. ($M_{24}$ e M_{23} sono privi di automorfismi esterni. $Aut(M_{22}) = M_{22}\cdot C_2$ è realizzato in M_{24} dal normalizzante di M_{22}).

ii) Nel caso di M_{11} e M_{12}, Witt (1938A) deve procedere diversamente. Innanzitutto, Witt prova che l'insieme Ω su cui opera M_{24} si può suddividere in due sottoinsiemi complementari Δ_1, Δ_2 di cardinalità 12 (dodecadi), in modo che lo stabilizzante in M_{24} di Δ_1 e Δ_2 sia un gruppo isomorfo a M_{12}, 5-transitivo sia su Δ_1 che su Δ_2. Pur essendo entrambe S-transitive, le due azioni di M_{12} su Δ_1 e Δ_2 non sono equivalenti. M_{24} contiene infatti un'involuzione u che normalizza lo stabilizzante di Δ_1 e Δ_2, e realizza un automorfismo esterno ϕ_u di M_{12} che scambia fra loro le azioni su Al e Δ_2. Lo stabilizzante di un punto di Δ_1 in M_{12}, i.e. il gruppo di Mathieu M_{11}, ha come immagine mediante ϕ_u un gruppo 3-transitivo su Al, nel quale

lo stabilizzante di un punto è isomorfo a PSL(2,11). In particolare, essendo M_{11} privo di automorfismi esterni, si ottengono in tal modo le due classi di sottogruppi coniugati di M_{12}, isomorfi a M_{11}, già osservate da Frobenius (cfr.§2.). Da ciò che precede si deduce infine che $Aut(M_{12}) = [M_{12}]C_2 : Aut(M_{12})$ è realizzato in M_{24} da $N_{M_{24}}(M_{12}) = \langle M_{12}, u \rangle$.

In modo simile, Witt (1938A) prova che, se si considera l'azione di M_{12} su una dodecade Δ, si può suddividere Δ in due esadi complementari Σ_1, Σ_2 in modo che lo stabilizzante di Σ_1 e Σ_2 in M_{12} sia il gruppo simmetrico S_6. Si consideri infatti lo stabilizzante in M_{12} di cinque punti $\delta_1, \ldots, \delta_5$ di Δ: tale sottogruppo, isomorfo a S_5, ha orbite di lunghezza 5,1,6 su Δ, e determina quindi un sesto punto $\delta_6 \in \Delta$. Posto $\Sigma_1 = \{\delta_1, \ldots, \delta_5, \delta_6\}$, e $\Sigma_2 = \Delta \setminus \Sigma_1$, lo stabilizzante in M_{12} di Σ_1 e Σ_2 è isomorfo a S_6. (Come sopra, si vede che le azioni di S_6 su Σ_1 e Σ_2 non sono equivalenti. M_{12} contiene un'involuzione v che scambia fra loro le azioni su Σ_1 e Σ_2, realizzando un automorfismo esterno di S_6: per tale automorfismo lo stabilizzante in S_6 di un punto di Σ_1, i.e. S_5, ha come immagine un gruppo 3-transitivo su Σ_1. In particolare, $Aut(S_6)$ è realizzato in M_{12} da $\langle S_6, v \rangle$.)

Le coppie di esadi complementari Σ_1, Σ_2 che si ottengono mediante la procedura descritta costituiscono i 132 blocchi di un sistema di Steiner S(5,6,12). $Aut(5,6,12) = M_{12}$ è 5-transitivo sui punti e transitivo sui blocchi del sistema. Con una contrazione in punto δ di Δ, a $(M_{12})_\delta = M_{11}$ resta allora

associato un sistema di Steiner S(4.5.11). con $Aut(S(4,5,11))=M_{11}$ 4-transitivo sui punti e transitivo sui 66 blocchi del sistema. (Con una seconda contrazione, si ottiene il piano inversivo M(3). e con una terza il piano affine AG(2.3)).

iii) Witt (1938B) tratta di sistemi di Steiner in generale, e prova fra l'altro l'unicità (a meno d'isomorfismi) di AG(2,3), di M(3). e dei sistemi di Steiner associati ai gruppi di Mathieu. In particolare, vale dunque il seguente:

TEOREMA. a) Esiste un unico sistema di Steiner S=S(t,m,n) con t=3,4,5; m=6,7,8; n-22.23.24. Si ha: $Aut(S) = Aut(M_{22}), M_{23}, M_{24}$, rispettivamcntc.

b) Esiste un unico sistema di Steiner S=S(t,m,n) con t=4,5; m=5,6; n=11,12. Si ha:$Aut(S)=M_{11}$, M_{12}, rispettivamente.

iv) Prima di Witt, Carmichael (1931) aveva già limpidamente descritto la connessione fra sistemi di Steiner e gruppi di Mathieu (omettendo le dimostrazioni). Le costruzioni di Carmichael (riportate in Carmichael (1937)) prescindono dai gruppi di Mathieu, basandosi soltanto sui gruppi projettivi PSL(2,23) e PSL(2,11):

a) Posto $\Omega = PG(1,23) = GF(23) \dot{\cup} \{\infty\}$, e $PSL(2,23)=\langle x\to x+1, x \to -x^{-1} \pmod{23} \rangle$, Carmichaei osserva che lo stabilizzante in PSL(2,23) dell'ottade $0 =\{\infty ,0,1,3,12,15,21,22\}$ è il sottogruppo $\langle x \to (1+x)/(1-x),\ x \to (3x+1)/(x-3) \pmod{23}\rangle$, di ordine 8. Le immagini di 0 per l'azione di PSL(2,23) su Ω sono in numero di $24\cdot 23\cdot 11/8 = 759$, e costituiscono i blocchi di un sistema di Steiner S(5,8,24). (Una lista completa delle ottadi è contenuta

ad es. in Todd (1966)).

b) In modo analogo, posto $\Delta = PG(1,11) = GF(11) \cup \{\infty\}$, e $PSL(2,11) = \langle x \to x+1,\ x \to -x^{-1} \pmod{11} \rangle$, Carmichael osserva che lo stabilizzante dell'esade $E = \{\infty, 1, 3, 4, 5, 9\}$ è un sottogruppo di ordine 5 di $PSL(2,11)$. Le immagini di E per l'azione di $PSL(2.11)$ su Δ costituiscono le $12 \cdot 11 \cdot 5/5 = 132$ esadi di un sistema di Steiner $S(5,6,12)$.

Dopo di ciò. Carmichael nota che $Aut(S(5,8,24)) = M_{24}$ e $Aut(S(5,6,12)) = M_{12}$, e deduce alcune delle proprietà gruppali salienti di M_{24} e di M_{12}.

(Si noti che le inclusioni $PSL(2.23) < M_{24}$ e $PSL(2,11) < M_{12}$ sono il fondamento della citata costruzione di de Séguier (1904). e furono già osservate dallo stesso Mathieu. Di tali inclusioni dà una elegante dimostrazione. "a posteriori", anche Witt (1938A). Posto $\Omega = PG(1,23)$, Witt prova che $M_{24} < S_\Omega$ contiene le permutazioni $(0.1,\ldots,22)$, i.e. $x \to x+1 \pmod{23}$. e $(0,\infty)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)(18,14)$, i.e. $x \to -x^{-1} \pmod{23}$. Allo stesso modo, posto $A = PG(1,11)$, si vede che $M_{12} < S_\Delta$ contiene le permutazioni $(0,1,\ldots,10)$ e $(0, \infty)(1,10)(2,5)(3,7)(4,8)(6,9)$, i.e. $x \to x+1$ e $x \to -x^{-1} \pmod{11}$. Dopo di ciò. Witt propone le stesse costruzioni di Carmichael, a partire dai blocchi $(\infty,0,1,2,3,5,14,17)$ e $(\infty,0,1,2,3,5)$.)

3) (Le costruzioni di **Lüneburg**)

Carmichael (1931) adombra un approccio alternativo alla

descrizione dei gruppi di Mathieu, che consiste nel rovesciare il procedimento di Witt, costruendo prima con metodi geometrico-combinatori i sistemi di Steiner, definendo poi i gruppi di Mathieu come gruppi di automorfismi di tali sistemi, e deducendone quindi le proprietà strutturali salienti. La prima costruzione pienamente dispiegata secondo queste linee si deve a Lüneburg, (1968.1969). Essa è simile nello spirito a quella di Witt: si fonda infatti su teoremi di estensione dei sistemi di Steiner, che sono l'esatto parallelo geometrico delle estensioni di Witt.

a) Attraverso una dettagliata analisi della geometria di PG(2,4) (l'unico sistema di Steiner con parametri 2,5,21), Luneburg prova che PG(2,4) può essere esteso tre volte, e in un unico modo, sino ad ottenere un sistema di Steiner S(5,8,24).

Più precisamente, Lüneburg esamina le seguenti configurazioni in PG(2,4): i) gli *iperovali*, i.e. gli insiemi di 6 punti di PG(2,4), a tre a tre non allineati; ii) i *sottopiani* di Baer di PG(2,4), i.e. le configurazioni di 7 punti e 7 rette di PG(2,4) che formano un piano projettivo di ordine 2; iii) gli insiemi di punti di PG(2,4) che si ottengono considerandole *differenze simmetriche* di due rette distinte di PG(2,4). Vi sono rispettivamente: 168 iperovali, che si distribuiscono in tre orbite $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$ di uguale lunghezza rispetto all'azione di PSL(3,4) sui punti di PG(2,4); 360 sottopiani di Baer, che si distribuiscono anch'essi in tre orbite 61, $\mathcal{B}_2$, $\mathcal{B}_3$ di uguale lunghezza rispetto all'azione di PSL(3,4); 21· 20/2 = 210 "differenze simmetriche".

Luneburg dimostra che, se si considera un'eventuale estensione di PG(2.4) ottenuta per aggiunzione di tre nuovi punti ξ_1, ξ_2, ξ_3, è possibile scegliere gli indici 1,2,3 in modo che i blocchi dell'estensione siano necessariamente: i) gli insiemi $r \cup \{\xi_1, \xi_2, \xi_3\}$, dove r è una retta di PG(2.4); ii) gli insiemi che si ottengono aggiungendo a tutti gli iperovali di $\mathcal{O}_i$ i punti ξ_j, ξ_k ($\{i,j,k\} = \{1,2,3\}$); iii) gli insiemi che si ottengono aggiungendo a tutti i sottopiani di Baer di $\mathcal{B}_i$ il punto ξ_i ($i = 1,2,3$); iv) le "differenze simmetriche". Pertanto l'estensione cercata, se esiste. è unica (a meno d'isomorfismi) . Dopo di ciò. per provare che un'estensione effettivamente esiste,basta a Liineburg verificare che, posto Ω = PG(2.4) $\cup \{\xi_1, \xi_2, \xi_3\}$, 5 punti qualsiasi di Ω appartengono a uno e uno solo dei 759 (=21+3·56+3·120+210) sottoinsiemi i),ii),iii),iv).

b) Con metodi simili a quelli usati nel caso di PG(2,4), cioé analizzando la geometria di AG(2,3), Lüneburg prova che il piano affine di ordine 3 può essere esteso tre volte, e in un unico modo, sino ad ottenere un sistema di Steiner S(5,6,12).

Precisamente. Lüneburg osserva che AG(2.3) contiene 54 *ovali* (= *quadrangoli*),che s i possono suddividere in tre sottoinsiemi Q_1, Q_2, Q_3 di cardinalità 18. con la proprietà che due ovali di uno stesso insieme Q_i (i-1.2.3) hanno al più 2 punti in comune (considerando AG(2.3) come contrazione in un punto α del piano M(3), i blocchi di M(3) non passanti per CZ costituiscono un siffatto insieme Q_i). Inoltre, il gruppo delle collineazioni di AG(2,3) opera come il gruppo simmetrico S_3 sugli insiemi

Q_1, Q_2, Q_3.

Dopo di ciò, è possibile provare che i 132 blocchi di un'eventuale estensione di AG(2,3) mediante tre nuovi punti η_1, η_2, η_3 sono necessariamente: i) gli insiemi $r \cup \{\eta_1, \eta_2, \eta_3\}$, dove r è una retta di AG(2,3); ii) gli insiemi $q \cup \{\eta_i, \eta_j\}$, $i \neq j$, $(i,j \in \{1,2,3\})$, dove q varia in uno degli insiemi Q_i (e si può allora supporre i=1); iii) gli insiemi $\hat{q} \cup \{\eta_i\}$, i=1,2,3, dove $\hat{q}$ è l'insieme che si ottiene da un ovale $q \in Q_1$ aggiungendovi il punto d'intersezione delle diagonali, al variare di $q \in Q_1$; iv) le coppie di rette parallele di AG(2,3).

D'altra parte, posto $\Delta = AG(2,3) \cup \{\eta_1, \eta_2, \eta_3\}$, 5 punti qualsiasi di A appartengono a uno e uno solo dei 132 (= 12+3·18+3·18+12) sottoinsiemi i),ii),iii),iv). Si conclude che l'estensione cercata.esiste ed è unica, e dunque esiste ed è unico S(5,6,12).

c) Le costruzioni in a) e b) sono simili, ma indipendenti l'una dall'altra. Alternativamente, si può ricavare la costruzione di S(5,6,12) da quella di S(5,8,24) osservando che:

1) un *unital* U di PG(2,4), i.e. la configurazione dei punti assoluti e delle rette non assolute rispetto a una polarità unitaria. è un sistema di Steiner S(2,3,9), e dunque è isomorfo al piano affine AG(2,3);

2) se si considera il sistema di Steiner S=S(5,8,24) costruito su PG(2.4) $U \cup \{\xi_1, \xi_2, \xi_3\}$, un'ottade di S che contiene 5 punti di $U \cup \{\xi_1, \xi_2, \xi_3\}$ contiene esattamente 6 punti di $U \cup \{\xi_1, \xi_2, \xi_3\}$ Dunque, i punti di $U \cup \{\xi_1, \xi_2, \xi_3\}$ e le ottadi di S che intersecano $U \cup \{\xi_1, \xi_2, \xi_3\}$ in 6 punti, danno luogo a un sistema di Steiner

$S(5,6,12)$.

(Si noti che la situazione descritta corrisponde, da un punto di vista gruppale, al fatto che il gruppo delle collineazioni di $AG(2,3)$ è isomorfo a $P\Gamma U(3,2)$.)

Una caratteristica essenziale delle costruzioni di Lüneburg è, come si è visto, quella di far precedere la dimostrazione di unicità a quella di esistenza: l'analisi delle geometrie di $PG(2,4)$ e $AG(2,3)$, rispettivamente, sulla quale si fondano le prove di unicità, consente infatti l'effettiva costruzione dei sistemi di Steiner richiesti.

Di natura simile, ma anche più complessa, è la costruzione dei sistemi di Steiner associati a M_{22}, M_{23} e M_{24}, ottenuta da. Jónsson

Sia $AG(2,4)$ il piano affine che si ottiene da $PG(2,4)$ rimuovendo una retta e tutti i suoi punti. Considerando $AG(2,4)$ come spazio vettoriale di dimensione 2 su $GF(4)$, e indicando con A il suo gruppo additivo, abeliano elementare di ordine 24, si può dare ad A, in modo ovvio, la struttura di uno spazio projettivo $PG(3,2)$. Jónsson (1972) fonda la sua costruzione su una puntuale analisi della geometria subordinata su $PG(3,2)$ dalle polarità simplettiche. Riprendendo in parte risultati di Conwell (1910) e di Edge (1954), Jónsson prova che $PG(3,2)$ contiene esattamente otto insiemi $P_1,\ldots,P_8$, ciascuno costituito da sette complessi lineari corrispondenti a sette polarità simplettiche a due a due non permutabili. L'unicità di un (eventuale) sistema $S(5,8,24) = (\Omega, B)$ segue allora osservando

che: i) (Ω, B) determina su $\Omega \setminus b$ $(b \in B)$ una struttura di spazio projettivo $PG(3,2)$; ii) vi è una bijezione $\alpha \to P_\alpha$ fra i punti di b e le otto collezioni di polarità simplettiche P_i, che risultano così determinate da (Ω, B); iii) la geometria delle polarità simplettiche di $PG(3,2)$ determina a sua volta in modo univoco i blocchi di (Ω, B). E' poi possibile, al solito, verificare che la configurazione ottenuta in iii) da effettivamente luogo a un sistema $S(5,8,24)$.

4) (Le costruzioni di Higman-Cameron)

Un'elegante costruzione di $S(5,6,12)$, parzialmente ispirata a lezioni di G.Higman, è descritta da P. Cameron (cfr. Cameron (1975,1980), **e Cameron.van Lint (1980)).**

La costruzione si fonda sull'esistenza di un automorfismo esterno ϕ di ordine 2 del gruppo simmetrico S_6, mediante il quale a una trasposizione di S_6 corrisponde il prodotto di tre trasposizioni disgiunte, e a un 3-ciclo corrisponde il prodotto di due 3-cicli disgiunti (e viceversa). E' possibile perciò considerare due rappresentazioni di permutazione inequivalenti di S_6 su due insiemi A, X di cardinalità 6, in modo che a una trasposizione (a,b) e a un 3-ciclo (a,b,c) su A corrispondono rispettivamente le permutazioni $(a,b)\phi$ e $(a,b,c)\phi$ su X. Sia ora S un sistema di Steiner di parametri 5,6,12: è facile provare che 1) se la differenza simmetrica $b_1 \Delta b_2$ di due blocchi di S ha cardinalità 6, $b_1 \Delta b_2$ è necessariamente un blocco di S, e dedurre da ciò che 2) se b_1, b_2 sono blocchi di S, tali che sia $|b_1 \cap b_2| = |b_1 \Delta b_2|$,

allora esistono dei blocchi b_3, b_4 tali che sia $b_1 \cap b_2 = b_3 \Delta b_4$ e $b_1 \Delta b_2 = b_3 \cap b_4$. Senza ledere la generalità. si può allora supporre che $A \cup X$ sia l'insieme dei punti di un tale sistema $S = S(5,6,12)$, e che A sia un blocco di S. Usando 1) e 2) si vede che i blocchi di S sono necessariamente costituiti dagli insiemi seguenti : i) A,X; ii) $(A \setminus \{a,b\}) \cup (x,y), (X \setminus \{x,y\}) \cup \{a,b\}$, ogniqualvolta (x,y) è un ciclo di $(a,b)\phi$; iii) $\{a,b,c\} \cup \{x,y,z\}$, ogniqualvolta (x,y,z) o (x,z,y) è un ciclo di $(a,b,c)\phi$. Basta allora verificare che gli insiemi i),ii),iii) sono effettivamente i blocchi di un sistema di Steiner per ottenere, dopo l'unicità, l'esistenza di S(5,6,12).

La costruzione precedente può anche ottenersi per via puramente combinatoria (cfr. Cameron. van Lint (1980)), considerando A come l'insieme dei vertici del grafo completo K_6, e X come l'insieme delle l-fattorizzazioni di A Un l-fattore di A è un insieme di 3 spigoli mutuamente disgiunti che coprono A; una 1-fattorizzazione di A è una partizione degli spigoli di A iti 5 l-fattori. Poiché ogni 1-fattore di A è contenuto in esattamente 2 1-fattorizzazioni di A, si può indicare un l-fattore mediante una coppia di elementi, ovvero uno "spigolo" di X. Sussiste una "dualità" fra A e X (che riflette l'esistenza di un automorfismo esterno di S_6) in cui i vertici e gli spigoli di A corrispondono alle l-fattorizzazioni e agli l-fattori di X (e reciprocamente). In virtù di tale dualità, è possibile definire 1) una relazione autoduale fra gli spigoli di A e di X, ponendo $\{a,b\} \sim \{x,y\}$ sse $\{a,b\}$ è uno spigoli appartenente all'i-fattore x,y ; 2) una relazione autoduale fra i sottoinsiemi

di cardinalità 3 di A e di X, ponendo $\{a,b,c\} \sim \{x,y,z\}$ sse $\{a,b,c\}$ è uno dei due triangoli formati dai 6 spigoli che restano dopo aver rimosso gli spigoli di A che appartengono agli 1-fattori $\{x,y\}$, $\{y,z\}$, $\{z,x\}$. I blocchi di S(5,6,12) descritti in ii) e iii) corrispondono precisamente alle coppie $\{a,b\} \sim \{x,y\}$ e $\{a,b,c\} \sim \{x,y,z\}$.

Una costruzione simile permette di provare l'esistenza e l'unicità di S(5,8,24), partendo dall'esistenza di S(5,6,12) e di un automorfismo esterno di M_{12}, e considerando due rappresentazioni inequivalenti di M_{12} su due insiemi $\tilde{A}, \tilde{X}$ di cardinalità 12. Alternativamente, si può procedere per via puramente combinatoria (cfr. Cameron, van Lint (1980). A tal fine si considera $\tilde{A}$ come l'insieme dei punti di un S(5,6,12), e, osservando che in un S(5,6,12) il complemento di un blocco b è un blocco b', si costruisce sull'insieme V delle 66 coppie di blocchi disgiunti di S(5,6,12) un grafo (non orientato) congiungendo due vertici $\{b,b'\}$, $\{c,c'\}$ di V sse $|b \cap c| = 3$. Si ottiene un grafo isomorfo al grafo triangolare T(12), i cui vertici sono le coppie non ordinate di elementi di un insieme $\tilde{X}$ di cardinalità 12. e in cui due vertici sono congiunti da uno spigolo sse hanno in comune un elemento di $\tilde{X}$. E' possibile costruire un sistema S(5,6,12) su $\tilde{X}$, reciproco di quello definito su $\tilde{A}$ (nel senso che ripetendo la procedura sopra descritta su $\tilde{X}$, ci si riporta ad $\tilde{A}$): ciò stabilisce una "dualità" fra $\tilde{A}$ e $\tilde{X}$, nella quale si corrispondono coppie di blocchi disgiunti e coppie di punti dei sistemì di Steiner su $\tilde{A}$ e $\tilde{X}$. Tale dualità induce una relazione (autoduale) fra i sottoinsiemi di cardinalità

4 di $\tilde{A}$ e di $\tilde{X}$, definita ponendo $\{a,b,c,d\} \sim \{x,y,z,u\}$ sse $\{x,y,z,u\}$ è il complemento in $\tilde{X}$ dell'unione delle 4 coppie di punti, mutuamente disgiunte, corrispondenti ai 4 blocchi del sistema S(5,6,12) su $\tilde{A}$ ches'intersecanoin $\{a,b,c,d\}$. Allora, un sistema S(5,8,24) su $\tilde{A} \cup \tilde{X}$ ha necessariamente i blocchi seguenti : i) $b \cup \{x,y\}$, dove b è un blocco del sistema di Steiner S(5,6,12) su $\tilde{A}$, e $\{b,b'\}$ corrisponde a $\{x,y\}$; ii) $\overset{*}{b} \cup \{a,b\}$, dove $\overset{*}{b}$ è un blocco del sistema di Steiner S(5,6,12) su X, e $\{\overset{*}{b},\overset{*}{b}'\}$ corrisponde a $\{a,b\}$; iii) $\{a,b,c,d\} \cup \{x,y,z,u\}$, dove $\{a,b,c,d\} \sim \{x,y,z,u\}$. La costruzione delineata consente, in particolare. di esibire mediante la dualità fra $\tilde{A}$ e $\tilde{X}$ un automorfismo esterno di M_{12}.

5) 1 sistemi di Steiner associati ai gruppi di Mathieu sorgono naturalmente nel contesto della teoria dei codici lineari, e in altri settori della combinatorica. Ne derivano altre costruzioni dei sistemi suddetti, di cui si tratterà diffusamente nei successivi §5 e 56.

§4. ALCUNE CARATTERIZZAZIONI DEI SISTEMI DI STEINER ASSOCIATI AI GRUPPI DI MATHIEU.

I sistemi di Steiner associati ai gruppi di Mathieu sono soprattutto notevoli perché 1) hanno "grandi" gruppi di automorfismi, altamente transitivi sui punti di Ω ; 2) $t=5$ nel caso di M_{12} e di M_{24}. Altri sistemi $S(5,m,n)$ sono noti solo per cinque valori del parametro n. Precisamente: Denniston (1976) ha provato l'esistenza di sistemi di Steiner $S(5,6,24)$, $S(5,7,28)$, $S(5,6,48)$ e $S(5,6,84)$, e Mills (1978) ha costruito un sistema di Steiner $S(5,6,72)$. (Notiamo incidentalmente che, in tutti i casi conosciuti, $Aut(S(5,m,n)) \supseteq PSL(2,n-1)$. Per vari problemi legati all'esistenza di sistemi $S(5,m,n)$, cfr. Denniston (1980)). Non si conoscono sistemi di Steiner con $t \geq 6$. Se si dimostrasse che sistemi cosiffatti non esistono, ne deriverebbe come conseguenza che non esistono gruppi di permutazioni o-transitivi non banali (cfr.§9).

In questo paragrafo descriveremo varie caratterizzazioni dei sistemi di Steiner associati ai gruppi di Mathieu: alcune di esse hanno carattere puramente combinatorio, mentre altre coinvolgono proprietà del gruppo degli automorfismi (eventualmente indotte da restrizioni di tipo combinatorio).

Conviene innanzitutto elencare alcune proprietà combinatorie dei sistemi in questione, che intervengono nelle caratterizzazioni seguenti :

1) In $S(5,8,24)$ l'intersezione di due ottadi distinte ha

cardinalità 0,2, o 4. Date due ottadi b_1, b_2, con $|b_1 \cap b_2| = 4$, anche la differenza simmetrica $b_1 \Delta b_2$ è un'ottade di $S(5,8,24)$. M_{24} è transitivo sulle coppie ordinate di ottadi aventi intersezione della stessa cardinalità: in altre parole, M_{24} è transitivo di rango 4 sulle ottadi di $S(5,8,24)$.

2) Da 1) si deduce che in $S(4,7,23)$ l'intersezione di due 7-adi distinte ha cardinalità 1 o 3, e che M_{23} è transitivo di rango 3 sulle 7-adi di $S(4,7,23)$. In modo analogo, si deduce che in $S(3,6,22)$ l'intersezione di due esadi distinte ha cardinalità 0, oppure 2, e che M_{22} è transitivo di rango 3 sulle esadi di $S(3,6,22)$.

3) In $S(5,6,12)$ l'intersezione di due esadi distinte ha cardinalità 0,2,3, o 4. Inoltre, il complemento di un'esade è un'esade, e, se b_1, b_2 sono due esadi con $|b_1 \cap b_2| = 3$, anche $b_1 \Delta b_2$ è un'esade. M_{12} è transitivo sulle coppie ordinate di esadi aventi intersezione della stessa cardinalità, i.e. M_{12} è transitivo di rango 5 sulle esadi di $S(5,6,12)$. Si deduce che in $S(4,5,11)$ due blocchi distinti hanno intersezione di cardinalità 1,2, o 3, e M_{11} è transitivo di rango 4 sui blocchi di $S(4,5,11)$.

A) Sia $S=S(t,m,n)$ un sistema di Steiner, con $1 < t < m < n$. E' facile provare che vale la disuguaglianza: $n \geq (t+1)(m-t+1)$. Ne segue in particolare che è sempre $n > 2m$, e si ha $n=2m$ se e solo se $t=1$ (i.e. S corrisponde a una partizione dell'insieme dei punti in due blocchi), oppure $m=t+1$. Se $n=(t+1)(m-t+1)$, accade che, assegnati $t+2$ punti di S, esiste un blocco che

ne contiene t+1. S(3,4,8), S(5,6,12) e S(5,8,24) sono i soli sistemi noti., con t >1, soddisfacenti tale condizione. Camerbn (1980) ha congetturato che, se n >2m, la suddetta condizione caratterizzi S(5,8,24). Tale congettura è stata confermata da Hauck (1982). il quale ha provato che, se S = S(t,m,n) è un sistema di Steiner, con 1< t < m-l, e n = (t+1) (m-t+l) , allora S = S(5,8,24). Infine, si può provare che: a) in ogni sistema S di parametri t,t+1,2t+2, t+2 è necessariamente un numero primo; b) un sistema S = (Ω,B) di parametri t-1,t,2t+1 esiste se e solo se ammette un'estensione $S^+(\Omega^+,B^+)$ (di parametri t,t+1,2t+2). In tal caso l'estensione è unica, e $\Omega^+ = \Omega \cup \{\infty\}$, $B^+ = \{b \cup \{\infty\}, \Omega^+ \setminus b | b \in B$. Mendelsohn (1970); cfr. anche Alltop (1972).

B) Sia S = S(t,m,n) e sia b = $\{\alpha_1, \ldots, \alpha_m\}$ un blocco di S. Il numero x_j dei blocchi di S che intersecano b in $\{\alpha_1, \ldots \alpha_j\}$ (0 $\leq$ j $\leq$ m) dipende soltanto da j e dai parametri di S (Mendelsohn (1970)). Più in generale, il numero μ_{ij} dei blocchi $b' \in B$, tali che sia $b' \cap \{al, \ldots, \alpha_i\} = \{\alpha_1, \ldots \alpha_j\}$ (0 < j $\leq$ i $\leq$ m), dipende solo da i,j e dai parametri di S (cfr. Gross (1974).

1 numeri μ_{ij} si possono disporre in un assetto triangolare (*triangolo delle intersezioni*) in modo che μ_{ij} sia l'elemento di posto j+1 della riga (i+l)-esima del triangolo. Ad esempio, il triangolo delle intersezioni di S(5,8,24) è il seguente:

							759							
						506		253						
					330		176		77					
				210		120		56		21				
			130		80		40		16		5			
		78		52		28		12		4		1		
	46		32		20		8		4		0		1	
30		16		16		4		4		0		0		1
30	0		16		0		4		0		0		0	1

I numeri μ_{ij} sono determinati induttivamente dalle formule:

1) $\mu_{ii} = \binom{n-i}{t-i}/\binom{m-i}{t-i}$ per $0 \leq i \leq t$; $\mu_{ii} = 1$ per $t \leq i \leq m$.

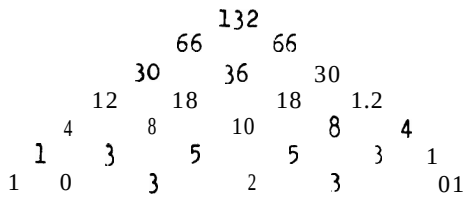
2) $\mu_{i+1,j} + \mu_{i+1,j+1} = \text{“}_{ij}$ per $0 \leq j \leq i \leq m$.

Naturalmente si ha $\mu_{ij} = 0$ se $t \leq j < i$: questi sono gli *zeri banali* del triangolo. Inoltre, è $x_j = \mu_{mj}$.

In particolare, nel caso di $S(5,8,24)$ vi sono due zeri non-banali: $\mu_{8,1} = \mu_{8,3} = 0$. Ciò corrisponde al fatto che due ottadi non si intersecano mai in 1 0 3 punti. In effetti, l'ultima riga del triangolo delle intersezioni ci dice che due ottadi distinte si intersecano in 0,2, 0 4 punti, e che, fissata un'ottade b, vi sono esattamente 3 0 ottadi disgiunte da b, 1 6 ottadi che intersecano b in 2 punti, e 4 ottadi che intersecano b in 4 punti.

Per ogni sistema di Steiner S di parametri t,t+1,2t+2 il

triangolo delle intersezioni è simmetrico rispetto all 'asse verticale. In particolare, nel caso di S(5.6.12) si ha il seguente triangolo d'intersezioni:



La simmetria assiale mostra in particolare che il complemento di un'esade è un'esade ($\mu_{6\ 6} = \mu_{6\ O} = 1$), e che due esadi non si intersecano mai in un punto ($\mu_{6,5} = 0$ (banale) $= \mu_{6,1}$).

Il problema di determinare quali sistemi di Steiner ammettono zeri non-banali nel triangolo delle intersezioni è stato risolto da Gross (1974), il quale ha provato il seguente:

TEOREMA (Gross (1974): Sia S = S(t,m,n) un sistema di Steiner, con $2 \leq t < m < n$, e si supponga che il triangolo delle intersezioni di S abbia zeri non-banali. Allora si ha:

i) $\mu_{m,0} = 0$, e S è un piano projettivo, oppure S(4,7,23), oppure S = S(t,t+1,2t+3) e t+3 è un numero primo (cfr. A));

ii) $\mu_{m\ 1} = 0$, e S = S(3,4,8), S(3,6,22), S(3,12,112) (se un tale sistema esiste), S(5,8,24), oppure S ha parametri t,t+1,2t+2;

iii) $\mu_{m\ 2} = 0$, e S = S(4,7,23);

iv) $\mu_{m,3} = 0$, e S = S(5,8,24).

Si deducono i seguenti corollari: 1) i soli sistemi di Steiner in cui due blocchi hanno sempre intersezione non vuota sono i piani projettivi, S(4,7,23), e i sistemi con parametri t,t+1,2t+3; 2) il numero massimo di zeri non-banali di un sistema di Steiner S è 2, e in tal caso S = S(4,7,23) o S(5,8,24); 3) zeri non-banali si hanno solo nell'ultima riga del triangolo delle intersezioni.

In particolare il Teorema di Cross generalizza risultati di **Noda** (1972). il quale aveva provato che gli unici sistemi di Steiner S(4,m.n) con $\mu_{m,o} = 0$ sono S(4,5,11) e S(4,7,23), e che in un sistema di Steiner con t = 3, o 5, si ha $\mu_{m,c} \neq 0$.

C) **Noda** (1972) ha usato i risultati summenzionati per caratterizzare i sistemi di Steiner associati ai gruppi di Mathieu in funzione dell'azione di Aut(S) sull'insieme dei blocchi. Precisamente, Noda ha provato i seguenti teoremi:

TEOREMA 1. Sia S = S(t,m,n), e si supponga che G $\subseteq$ Aut(S) sia transitivo di rango 3 sui blocchi di S. Allora t $\leq$ 4, e:

i) se t = 3, S = S(3,4,8) e G = PSL(3.2) o AGL(3,2), oppure S = S(3.6.22) e G = M_{22} o Aut(M_{22});

ii) se t = 4, S = S(4,7,23) e G = M_{23}.

TEOREMA 2. Sia S = S(t,m,n), e si supponga che G $\subseteq$ Aut(S) sia transitivo di rango 4 sui blocchi di S. Allora t $\leq$ 5. e:

i) se $t = 4$, $S = S(4,5,11)$ e $G = M_{11}$;

ii) se $t = 5$, $S = S(5,8,24)$ e $G = M_{24}$.

Si noti che i teoremi precedenti sono derivabili, in linea di principio, da Gross (1974). Infatti, se $G \subseteq Aut(S)$ ha rango r sui blocchi di S. e si indica con σ il numero di valori che assume la cardinalità dell'intersezione di due blocchi distinti di S. si ha $\sigma \leq r-1$. D'altra parte, i sistemi di Steiner per i quali $\sigma < t$, sono quelli che ammettono zeri non-banali, cioé quelli classificati da Gross (1974). Dunque, se $t \geq r$, s è determinato (e in particolare, le restrizioni $r=3,4$, implicano $t \leq 4$ e $t \leq 5$, rispettivamente (cfr. il corollaai. 2)). Notiamo infine, incidentalmente, che $r = 2$ se e solo se $S = PG(2,q)$ e $G \supseteq PSL(3,q)$. (Ostrom.Wagner (1959)).

D) Sia $D = (\Omega, B)$ un $t-(n,m,\lambda)$ disegno, con $t = 2s$, $t \leq m \leq n-s$. Allora $|B| = \binom{n}{s}$, e si ha l'uguaglianza se e solo se $s = \sigma$ (ove σ è, come in C), il numero dei valori che assume $|b \cap b'|$, $b \neq b' \in B$). Questo risultato si deve a Ray-Chaudhuri,Wilson (1975), e generalizza la disuguaglianza di Fischer, valida per i 2-disegni. Un disegno D per il quale sia $s = \sigma$ $(=t/2)$, si dice tight (in particolare, un a-disegno tight non è altro che un disegno simmetrico). N.Ito ha perseguito la classificazione dei 4-disegni tight, ottenendo infine, con il contributo di H. Enomoto, R. Noda e A. Bremner, la seguente caratterizzazione di $S(4,7,23)$:

TEOREMA (Ito (1975.1978). Enomoto. Ito, Noda (1979), Bremner (1979)): Sia D un 4-disegno tight, con $2 < m < n-2$. Allora D =

= S(4,7,23) oppure D è il disegno complementare di S(4,7,23) (i.e. il disegno che ha come punti i punti di S(4,7,23), e come blocchi i complementi dei blocchi di S(4,7,23)).

E) (Proprietà della differenza simmetrica)

Sia S = S(t ,m,n) un sistema di Steiner, con m pari e $m < 2t$. Si dice che S ha la proprieta della differenza simmetrica (Δ) se, ogniqualvolta la differenza simmetrica $b_1 \Delta b_2$ di due blocchi di S ha cardinalità m, b_1 A b_2 è un blocco di S. La proprietà (A) è soddisfatta da S(5,6,12) e da S(5.8.24). e dai sistemi $AG_2(d,2)$, i.e. dagli spazi affini di dimensione d su GF(2), considerati come sistemi $S(3,4,2^d)$ (cfr. §3,1)).

Si hanno i seguenti notevoli teoremi:

TEOREMA 1 (Cameron (1974)): Sia S = S(t,m,n) un sistema di Steiner, con $m=2t-2 > t$. Se S gode della proprietà (Δ), allora S = S(5,8,24), oppure S = $AG_2(d,2)$.

TEOREMA 2 (Cameron (1975)): Sia S = S(t,m,n) un sistema di Steiner, con m pari e $m < 2t$, e si supponga che S goda della proprietà (A): 1) se m = 2t-4, oppure m=t+l con t > 3, allora $m \equiv 2 \pmod 4$; 2) se t = 5 e m = 6, allora n = 12 e S = S(5,6,12).

Si noti che i teoremi precedenti caratterizzano completamente i sistemi di Steiner soddisfacenti la proprietà (A). per $t \leq 6$. E' pertanto ragionevole supporre che la proprietà (Δ) caratterizzi, in effetti, i sistemi S(5,6,12) e S(5,8,24), insieme agli spazi affini su GF(2).

Il Teorema 2 è dimostrato mediante la caratterizzazione

di $S(5,6,12)$ in termini di 1-fattorizzazioni del grafo completo K_6 (cfr.§3,4)). (Cameron (1975) prova, fra l'altro, che per un sistema $S(5,6,n)$ la proprietà (A) è equivalente alla proprietà (A)*: se b_1, b_2 sono blocchi per i quali $|b_1 \cap b_2| = |b_1 \Delta b_2|$, allora vi sono dei blocchi b_3, b_4 tali che sia $b_1 \cap b_2 = b_3 \Delta b_4$ e $b_1 \Delta b_2 = b_3 \cap b_4$ (cfr.§3,4)). Pertanto sia (A) che (A)* caratterizzano S(5.6.12) nella classe dei sistemi S(5,6,n).)

La dimostrazione del Teorema 1 è invece ricondotta, in ultima analisi, a risultati sui codici lineari, che saranno discussi in §5. Innanzitutto, Cameron considera una qualsiasi contrazione S' di S, e osserva che, per le ipotesi su S, i) $S' = (\Omega, B)$ ha parametri t-l, 2t-3,n-1, e determina univocamente S; ii) se $\alpha, \beta \in \Omega$, e q_1, q_2, q_3, q_4 sono sottoinsiemi di Ω di cardinalità t-2 tali che $\{\alpha\} \cup q_1 \cup q_2$, $\{\alpha\} \cup q_3 \cup q_4$ e $\{\beta\} \cup q_1 \cup q_3$ siano dei blocchi di S', allora anche $\{\beta\} \cup q_2 \cup q_4$ è un blocco di S' (in particolare, per t=3, ciò implica $S' = PG(d-1.2)$. $d > 2$ (cfr. Hall (1960)). Dopo di ciò, indicando con $\hat{\Omega}$ l'insieme dei sottoinsiemi di Ω di cardinalità $\leq t-2$, e con $c_1, c_2, \ldots, c_{n-1}$ n-l colori, definisce su $\hat{\Omega}$ un grafo colorato $\mathcal{G}$ nel modo seguente: i) se $q \in \hat{\Omega}$, $|q| < t-2$, e $\alpha_i \notin q$, congiunge q a $q \cup \{\alpha_i\}$ con uno spigolo di colore c_i; ii) se $q \in \hat{\Omega}$, $|q| = t-2$, e $\alpha_i \notin q$, congiunge q a $b \setminus (q \cup \{\alpha_i\})$, ove b è il blocco di S' che contiene $q \cup \{\alpha_i\}$. $\mathcal{G}$ è un grafo connesso, e indicando con γ_i l'involuzione su $\hat{\Omega}$ che scambia fra loro i vertici di ogni spigolo di colore c_i, si ha che $\Pi = \langle \gamma_i \quad i=1,2,.\ n-1 \rangle$ è un sottogruppo abeliano elementare di $Aut(\mathcal{G})$, che preserva i colori ed è transitivo sui vertici di $\mathcal{G}$. Sia ora V =

= V(n-1,2), $\{e_i\}$ una base di V, e si consideri E come uno spazio vettoriale su GF(2): il nucleo dell'applicazione lineare f : V → E, definita ponendo f $(e_i) = \gamma_i$, risulta essere un codice binario $\mathcal{C}$, perfetto e correttore di t-2 errori (e i blocchi di S' corrispondono ai vettori del codice a distanza minima 2t-3 da $\underline{0}$). Ne segue (cfr.§5) che il codice trovato è: i) un codice di Hamming, con t-1=2, $n-1=2^d-1, d > 2$. e in tal caso S' = PG(d-1,2); ii) il codice binario di Golay, con t-1=4, n-1=23, e in tal caso S'=S(4,7,23). Si deduce di qui che, nel caso i), $S=AG_2(d,2), d > 2$; mentre nel caso ii) S=S(5,8,24).

F) (Reticoli geometrici)

Un reticolo L, denotato di 0 e 1 e avente lunghezza finita, si dice *geometrico* (cfr. **Birkhoff** (1966)) se: i) ogni elemento di L è unione di elementi che coprono 0 (punti, o atomi); ii) per ogni $x,y \in L$, se x e y coprono $x \wedge y$, allora $x \vee y$ copre x e y (condizione di copertura). In un reticolo geometrico L, ad ogni elemento x di L è possibile associare una "dimensione" dim(x), data dalla lunghezza comune di tutte le catene massimali da 0 a x, diminuita di 1. In particolare, dim(0)=-1, dim(x)=0 sse x è un punto, e dim(1)=dim(L). (Il reticolo dei sottospazi di uno spazio projettivo è, ovviamente, un esempio di reticolo geometrico).

Kantor (1974,1975,1976) ha provato importanti teoremi d'immersione ("strong embedding") di reticoli geometrici in reticoli geometrici modulari (in particolare: in spazi projettivi finiti). Poiché ad ogni t-(n,m,λ) disegno D è associato in modo naturale

il reticolo geometrico di dimensione t, i cui elementi sono gli insiemi di punti di D aventi cardinalità r $\leq$ t-l, i blocchi di D, e 1 (di dimensione r-l, t-l e t, rispettivamente), dai teoremi d'immersione di Kantor derivano risultati sui disegni. e in particolare alcune notevoli caratterizzazioni dei sistemi di Steiner associati ai gruppi di Math'ieu. Rinviando alle note di Kantor per maggiori precisazioni sui teoremi d'immersione (e a Percsy (1981) per generalizzazioni delle tecniche di Kantor in varie direzioni), menzioniamo il seguente:

TEOREMA. Sia D = (Ω ,B) un t-(n,m, λ) disegno, con m >t $\geq$ 3 . Si supponga che, per. ogni sottoinsieme X di Ω di cardinalità t-2, i punti di $\Omega \setminus X$ e i blocchi di D che contengono X formino il disegno dei punti e degli iperpiani di uno spazio affine finito. Allora si hanno i casi seguenti: i) t=3, e D è un piano inversivo; ii) t=4, e D=S(4,5,11); iii) t=5, e D=S(5,6,12); iv) t=4, e D è un sistema di Steiner di parametri 4,15,171 che ammette in un punto $\alpha \in \Omega$ una contrazione D , isomorfa a un piano inversivo non classico di ordine 13.

(Ovviamente, il Teorema precedente pub considerarsi una classificazione delle possibili estensioni di un piano inversivo (cfr.§3). In particolare, non è noto un sistema soddisfacente le condizioni iv)).

Le tecniche di Kantor mostrano, fra l'altro, che il reticolo geometrico associato a S(4,5,11) (rispettivamente, S(5,6,12)) è immergibile nel reticolo modulare PG(4,3) (rispettivamente, PG(5.3)). Si ottengono così una rappresentazione di M_{11} in

PSL(5,3), che si solleva a una rappresentazione lineare in SL(5,3), già considerata da Assmus, Mattson (1966A) e una rappresentazione projettiva o-dimensionale di M_{12}, già considerata da Coxeter (1958) (cfr.§5).

Nel contesto dei reticoli geometrici trovano collocazione anche alcune caratterizzazioni dei sistemi di Steiner associati ai gruppi di Mathieu, originariamente formulate in termini di "gruppi di Jordan" (cfr. Kantor (196912)). Sia infatti D = = (Ω, B) un t-(n,m, λ) disegno, e sia $G \leq Aut(D)$ 2-transitivo su Ω (ma non m-transitivo su λ) e transitivo su B; si supponga inoltre che Gb (il sottogruppo di G che fissa i punti di beB) sia transitivo su $\Omega \setminus b$. G è allora un "gruppo di Jordan" su Ω, e i sottoinsiemi di Ω che sono intersezioni di sottoinsiemi di B formano un reticolo geometrico di dimensione t (cfr. Kantor (1975B)). In quest'ordine d'idee si collocano le caratterizzazioni seguenti:

1) Se $|\Omega| \leq 6m$. D è uno spazio projettivo o affine, oppure D = S(3,6,22), S(4,7,23), S(5,8,24), e G è determinato. In particolare, nel caso dei sistemi associati ai gruppi di Mathieu, G è rispettivamente M_{22} o $Aut(M_{22})$, M_{23}, M_{24} (cfr. Kantor (1969A)).

2) Ciascuna delle ipotesi : i) $G_{[b]}$ (il sottogruppo di G che lascia invariante il blocco b) è L-transitivo su $\Omega \setminus b$; ii) G_b contiene un sottogruppo abeliano transitivo su $\Omega \setminus b$; iii) $|\Omega \setminus b|$ è potenza di un numero primo, implica che D è uno spazio projettivo, o uno spazio affine su GF(2), oppure D = S(3,6,22),

S(4,7,23), S(5,8,24) (cfr. Kantor (1969A, 1975B)).
(Per un altro risultato dello stesso tipo, riguardante S(3,6,22), cfr. Kantor (1974), Theorem 3.)

G) (Caratterizzazioni mediante l'azione di Aut(S) su Ω)

Abbiamo già accennato a varie caratterizzazioni dei sistemi di Steiner associati ai gruppi di Mathieu, in funzione della struttura di Aut(S) come gruppo di permutazioni sui punti e sui blocchi di S (cfr. C) e F)). Caratterizzazioni conclusive, in termini del grado di transitività di Aut(S) sui punti di S, si possono ottenere utilizzando la classificazione dei gruppi semplici finiti. Conviene pero menzionare, innanzitutto, alcune caratterizzazioni parziali di questo tipo che prescindono dalla classificazione. In ordine "storico":

1) Sia S=S(t,m,n) uno dei sistemi associati a M_{22}, M_{23}, M_{24}. Si vede facilmente che: i) Aut(S) è transitivo sulle (t+1)-ple ordinate di punti non appartenenti a uno stesso blocco; ii) Aut(S) è transitivo sulle (t+2)-ple ordinate di punti tali che t+1 di essi non appartengono mai a uno stesso blocco. Tits (1964) ha provato che un sistema di Steiner non banale S = S(t,m,n), con t > 1, soddisfa le condizioni i) e ii) se e solo se S=PG(2,q), $AG_2(d,2)$, oppure è uno dei sistemi associati a M_{22}, M_{23}, M_{24}.

2) Come corollario di teoremi sui gruppi altamente transitivi (cfr. §9), Nagao (1965) ha dato la seguente caratterizzazione di S(4,5,11): Sia S = S(4,5,n), e si supponga Aut(S) 4-transitivo

sui punti di S. Allora S è il sistema banale S(4,5,5), oppure S=S(4,5,11)). (Per un'elegante dimostrazione, di tipo combinatorio, dello stesso risultato, cfr. anche **Kantor** (1975B)).

Oyama (1978) ha poi provato la generalizzazione: Sia D un 4-(n,m,λ) disegno, con m=5,6; λ = 1.2. Se Aut(D) è 4-transitivo sui punti di D. allora D = S(4,5,5), S(4,6,6), D è un 4-(6,5,2) disegno (banale), oppure D ≅ S(4,5,11).

Come corollario della classificazione dei gruppi semplici. e della determinazione di tutti i gruppi di permutazioni 2-transitivi che da essa' deriva, **Kantor** (1983) ha recentemente ottenuto una completa classificazione dei sistemi di Steiner S(2,m.n) che possiedono un gruppo di automorfismi 2-transitivo sui punti. Np consegue, in particolare, il seguente conclusivo risultato (del quale i precedenti sono casi speciali):

TEOREMA. Sia S = S(t,m,n) un sistema di Steiner, con $m \geq t+1 \geq 4$, e si supponga che G sia un gruppo di automorfismi di S, t-transitivo sui punti di S. Si danno allora i casi seguenti : i) S = $AG_2(d,2)$, e G = AGL(d,2), oppure G = $[E_{24}]A_7$ c AGL(4,2) (e d = 4); ii) S è il sistema di Steiner i cui punti sono i punti di $GF(q^a) \cup \{\infty\} = PG(1,q^a)$, e i cui blocchi sono le immagini di $GF(q) \cup \{\infty\} = PG(1,q)$ per l'azione di $PGL(2,q^a)$, a ≥ 2 , e $PSL(2,q^a) \trianglelefteq G$; iii) S = S(4,5,11),S(5,6,12), S(3,6,22),S(4,7,23),S(5,8,24), e G = M_{11}, M_{12}, M_{22} o $Aut(M_{22})$, M_{23}, M_{24}.

H) A conclusione di questo paragrafo, citiamo alcuni risultati riguardanti le *proprietà d'intersezione* dei sistemi di Steiner

associati ai gruppi di Mathieu.

Si dice che due sistemi di Steiner $S1 = (\Omega, B_1)$, $S_2 = (\Omega, B_2)$ hanno intersezione k se $|B_1 \cap B_2| = k$, i.e. se hanno in comune k blocchi. In particolare, se k = 0 Sl e S_2 si dicono disgiunti. Il numero massimale di sistemi S(t,m,n) mutuamente disgiunti si indica con d(t,m,n).

Assmus, Matt son (1966B) hanno provato, con semplici argomenti di teoria dei codici (cfr. §5), che è $d(t,m,n) \geq 2$ per i cinque sistemi associati ai gruppi di Mathieu (cf r. anche **Hughes** (1965A) per S(4,5,11) e S(5,6,12)), chiedendosi SC fosse d(t,m,n)=2. Successivamente Kramer, Mesner (1974) hanno determinato i possibili valori di k nel c a s o d i S(4,5,11) e S(5,6,12), confermando in particolare la congettura d(4,5,11) = d(5,6,12) = 2, e provando che due coppie qualsiasi di sistemi fra loro disgiunti sono isomorfe. Nel caso dei sistemi associati ai grandi gruppi di Mathieu, **Kramer,Magliveras** (1974) hanno invece provato, usando il computer, c h e $d(5,8,24) \geq 9$, $d(4,7,23) \geq 24$, e $d(3,6,22) > 60$.

§5. CODICI E GEOMETRIE

I sistemi di Steiner associati ai gruppi di Mathieu ammettono costruzioni semplici e naturali a partire da certi codici lineari, i cosiddetti codici di Golay (introdotti da Golay (1949)). Inversamente, questi codici sono generabili dai sistemi di Steiner corrispondenti.

A) Testo di riferimento per la teoria dei codici lineari può considerarsi MacWilliams, Sloane (1977). Altri testi eccellenti sono i recenti van Lint (1982) e Pless (1982). Riprendiamo qui soltanto alcune nozioni fondamentali, indispensabili alla comprensione del seguito.

Ricordiamo innanzitutto che, posto $F = GF(q)$ e indicato con F^n lo spazio vettoriale n-dimensionale su F, si dice *codice* di lunghezza n su F ogni sottoinsieme non vuoto C di F^n. F è l' *alfabeto*, e gli elementi di C sono le *parole* del codice. Se $q = 2$, risp. 3, il codice si dice binario, risp. ternario. Se $C = \{\underline{0}\}$, si dice che C è un codice banale. Un codice C_1 si dice *equivalente* a un codice C_2 se C_2 si ottiene da C_1 applicando una (fissata) permutazione delle coordinate alle parole di C_1.

Sia C un codice non banale di lunghezza n su F. Si definisce su F^n una metrica d (*distanza di Hamming*) ponendo per ogni $x = (x_i)$, $y = (y_i) \in F^n$, $d(x,y) = |\{i \mid 1 \leq i \leq n, x_i \neq y_i\}|$, e si dice che $\min\{d(x,y) \mid x,y \in C, x \neq y\}$ è la *distanza* (minima) di C. Per ogni $x=(x_i) \in F^n$, si dice che $\{i \mid 1 \leq i \leq n, x_i \neq 0\}$ è il *supporto* di x, e che $w(x) = d(x,\underline{0}) = |\{i \mid 1 \leq i \leq n, x_i \neq 0\}|$ è il *peso* di

x. $\min\{w(x) \mid x \in C, x \neq \underline{0}\}$ è il pesa (minimo) del codice C.

Se, per ogni $x,y \in C$, $x \neq y$ implica $d(x.y) \geq 2e+1$, si dice che C è un *codice correttore di e errori.* . Se C ha distanza $2e+1$, e, per ogni $x \in F^n$, esiste una (e una sola) parola di C a distanza $\leq$ e da x, si dice che C è un codice *perfetto.* (Sono considerati codici perfetti banali il codice banale, l'intero spazio F^n, e il codice ripetitivo binario $C = \{\underline{0}, \underline{1} = (1,1,\ldots,1)\}$ con n dispari.)

Un codice C di lunghezza n, con $|C| = M$ e distanza d, si dice (n,M,d)-codice. n,M *e* d sono i *parametri* del codice C.

Un codice C di lunghezza n si dice *lineare* se C è un sottospazio di F^n, e se $\dim_F(C) = k$. si dice che C è un [n,k]-codice (su F). In un codice lineare, distanza e peso ovviamente coincidono. (D'altra parte, poiché una traslazione di F^n non altera la distribuzione delle distanze, si suppone sempre che un codice (non lineare) contenga $\underline{0}$).

Sia C un [n,k]-codice (su F). Una matrice G di tipo (k,n), le cui righe costituiscano una base per C, si dice *matrice generatrice* di C. A meno d'equivalenza, si può supporre che G sia nella forma standard: $G = [I_k \mid P]$. Allora la matrice $H = [-P^t \mid I_{n-k}]$ è una matrice generatrice del codice $C^{\perp} = \{y \mid y \in F^n, (x,y) = 0 \quad \forall x \in C\}$. $C^{\perp}$ è un [n,n-k]-codice su F, che si dice *duale* di C. In particolare, se $C \subseteq C^{\perp}$, si dice che C è un codice *autoortogonale, e se* $C = C^{\perp}$, si dice che C è un codice *autoduale.* Una matrice generatrice di $C^{\perp}$ (e.g.H) si dice *matrice controllo di parità* per C.

Se C è un codice di lunghezza n su F. si può "estendere" C aggiungendo ad ogni parola $x = (x_1,\ldots,x_n)$ un'extra-coordinata $x_{n+1} \in F$, in modo che sia $x_1+\ldots+x_n+x_{n+1} = 0$. Si ottiene così il codice *esteso* $\bar{C} = \{(x_1,\ldots,x_{n+1}) \; (x_1,\ldots,x_n) \in C,\; x_{n+1}\in F,$ $\Sigma_1^{n+1} x_i = 0\}$. Se C è un $[n,k]$-codice su F, $\bar{C}$ è un $[n+1,k]$-codice su F, ed è un ' estensione non banale se x_{n+1} non è sempre 0. (In particolare, se C è un codice binario con distanza d dispari, $\bar{C}$ è un'estensione non banale con distanza d+1). Se $G = [G^1|\ldots|G^n]$ è una matrice generatrice di C, $\bar{G} = [G \mid G^{n+1}]$, con $\Sigma_1^{n+1} G^i = \underline{0}$ è una matrice generatrice di $\bar{C}$; se H è una matrice controllo di parità per C, $\bar{H} = \left[\begin{array}{c|c} \underline{1} & 1 \\ \hline H & \underline{0} \end{array}\right]$ è una matrice controllo di parità per $\bar{C}$.

Sia ora $n = (q^k-1)/(q-1)$, e si consideri un $[n,n-k]$-codice C su $F = GF(q)$, con una matrice controllo di parità H formata da colonne a due a due indipendenti. Poiché le colonne di H individuano gli n punti distinti di $PG(k-1,q)$, il codice C è univocamente determinato, a meno d'equivalenza. Si dice che C è il $[n,n-k]$-*codice di Hamming su* GF(q) (cfr. Hamming (1950). Golay (1949.)). C ha distanza 3 (i.e. è correttore di un singolo errore). E' poi facile dimostrare che C è un codice lineare perfetto.

Il *gruppo delle invarianze* di un codice lineare C di lunghezza n su F è, per definizione, il gruppo I delle trasformazioni monomiali di F^n che preservano C. Se ad ogni invarianza di C si associa la corrispondente permutazione sulle coordinate

delle parole di C, si ottiene un omomorfismo $f : I \to S_n$; l'immagine f(1) è il *gruppo degli automorfismi*, Aut(C), del codice C.

Un [n,k]-codice C su F si dice *ciclico* se Aut(C) contiene il ciclo (O,l....,n-1). i.e. se, per ogni $(a_0,a_1,\ldots,a_{n-1})\epsilon C$, anche $(a_{n-1},a_0,a_1,\ldots,a_{n-2})\epsilon C$ (*). Un codice ciclico si può rappresentare mediante un ideale di polinomi. Precisamente, sia F[x] l'anello dei polinomi in x su F, e si consideri l'anello quoziente $R = F[x]/(x^n-1)$ rispetto all'ideale generato da x^n-1. Come gruppo additivo, R è canonicamente isomorfo a F^n, previa identificazione del polinomio rappresentativo $a(x) = a_0+\ldots+a_{n-1}x^{n-1}$ con il vettore $a = (a_0,\ldots,a_{n-1})$. Si può dunque considerare un [n,k]-codice C su F come un sottoinsieme di R, e si vede subito che, traducendosi la condizione (*) nella seguente: a(x) e C implica x.a(x)eC, C è ciclico se e solo se è un ideale di R. In particolare, un [n,k]-codice ciclico C è generato da un polinomio g(x), divisore di x^n-1.

Particolari codici ciclici sono i cosiddetti *QR-codici* (*codici a residui quadratici*), che si ottengono nel modo seguente. Sia n un numero primo dispari, e sia α una radice primitiva n-esima dell'unità in un'estensione di GF(q). Si supponga inoltre che q sia un residuo quadratico mod n, e si indichino con Q e N rispettivamente l'insieme dei quadrati non nulli di GF(n) e l'insieme GF(n) \(Q U { 0)). Il polinomio x^n-1 si decompone allora su GF(q) nella forma: $x^n-1=(x-1)g_0(x)g_1(x)$, ove $g_0(x) = \Pi_{r\epsilon Q}(x-\alpha^r)$, $g_1(x)=\Pi_{r\epsilon N}(x-\alpha^r)$. I codici ciclici di lunghezza n su GF(q), generati da $g_0(x)$ e da $(x-1)g_0(x)$

si dicono QR-*codici*. (Si noti che, se $j \in N$, la permutazione $\gamma \to \gamma^j$ ($\gamma \in GF(n)$) scambia fra loro Q e N: ne segue che i codici generati da $g_1(x)$ e $g_1(x)$ sono equivalenti. Inoltre, se $q=2$, il codice generato da $(x-1)g_0(x)$ consiste delle parole di peso pari del codice generato da $g_1(x)>$. Nel caso dei QR-codici, per $q \neq 2$ si conviene in genere di modificare la definizione di codice esteso: se C è il QR-codice di lunghezza n su GF(q) generato da $g_0(x)$, si richiede di aggiungere alle parole di C un'extra-coordinata, in modo da ottenere un codice $\bar{C}$ autoortogonale se $n \equiv -1(4)$, e ortogonale all'estensione del codice generato da $g_1(x)$ se $n \equiv 1(4)$. Poiché C è un $[n,(n+1)/2]$-codice su GF(q), $\bar{C}$ è in ogni caso un $[n+1,(n+1)/2]$-codice su' GF(q).

B) (Costruzioni dei codici di Golay)

1) Sia Ha il $[7,4]$-codice binario di Hamming. A meno d'equivalenza, si può supporre che la matrice controllo di parità di Ha sia

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

, e Ha sia dunque costituito da $\underline{0}$, dalle 7 parole che si ottengono, permutando ciclicamente le coordinate di $(1,1,0,1,0,0,0)$, e dai complementi delle 8 parole precedenti. L'estensione $\overline{Ha}$ è allora costituita da $\underline{0}$, $\underline{1}$, e da 14 parole di peso 4, ed è quindi un codice autoduale con distanza 4.

Sia ora Ha' il codice che si ottiene da Ha invertendo l'ordine delle coordinate nelle parole di Ha, e si consideri il sottoinsieme $\bar{C}$ di $GF(2)^{24}$ così definito: $\bar{C} = \{(a+x,b+x,a+b+x) \mid a,b \in \overline{Ha}; x \in \overline{Ha'}\}$.

$\bar{C}$ è un codice binario di lunghezza 24, e non è difficile verificare che $\bar{C}$ è un [24,12]-codice autoduale con distanza 8. (Se a e b variano in una base di $\overline{Ha}$, e x varia in una base di $\overline{Ha}'$, si vede facilmente che i vettori (a,0,a) ,(0,b,b), (x,x,x) formano una base per $\bar{C}$, tale che due suoi vettori qualsiasi sono fra loro ortogonali. Pertanto $\bar{C}$ ha dimensione 12 su GF(2) ed è autoduale. Poiché, inoltre, i vettori della base considerata hanno peso divisibile' per 4, ciò accade per ogni parola di $\bar{C}$. E' facile provare che $\bar{C}$ non contiene parole non nulle di peso < 8, e quindi una parola di $\bar{C}$ ha peso 0,8,12,16, o 24. Si può verificare infine che $\bar{C}$ contiene, oltre a $\underline{0}$ e a $\underline{1}$, 759 parole di peso 8 e i loro complementi, e 2576 parole di peso 12.)

Se si elide l'ultima coordinata in ogni parola di $\bar{C}$, si ottiene un [23,12]-codice C con distanza 7. C è il cosiddetto *codice binario di Golay*: è un codice perfetto, correttore di 3 errori.

(La costruzione del codice esteso di' Golay $\bar{C}$, sopra delineata, è attribuita a E.F.Assmus e H.F.Mattson, ma appare anche in Turyn (1966). E' essenzialmente la stessa costruzione proposta da Curtis (1976) come base per l'analisi combinatoria delle proprietà strutturali di M_{24} mediante il cosiddetto MOG (cfr.§6).)

Alternativamente, il [23,12]-codice binario di Golay può essere costruito direttamente, mediante la matrice generatrice

$G = \left[I_{12} \middle| \frac{1}{S} \right]$, ove S è la matrice circolante con prima riga

(1,1,0,1,1,1,0,0,0,1,0) (Karlin (1969)).

2) Siano $x_0 = 0$, $x_1,\ldots,x_{q-1}$ gli elementi di GF(q), q dispari, e si consideri la funzione $\chi: GF(q) \to \{0,1,-1\}$ definita ponendo $\chi(0) = 0$, $\chi(x) = 1$ per $x \in Q$, $x(x) = -1$ per $x \in N$. La matrice $P_q = (a_{ik})$, con $a_{ik} = \chi(x_i - x_k)$, si dice *matrice di Paley* (di ordine q).

Sia ora GF(5) = {0,1,2,3,4}, e si consideri la matrice di Paley di ordine 5, $P_5 = \begin{vmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \end{vmatrix}$. La matrice $G = \left[\begin{array}{c|c} I_6 & \begin{matrix} 1 \\ \hline \\ P_5 \end{matrix} \end{array}\right]$ è la matrice generatrice di un [11,6]-codice ternario C con distanza 5. il cosiddetto codice *ternario di Golay*. C è un codice perfetto, correttore di 2 errori; la sua estensione $\bar{C}$ è un [12,6]-codice ternario autoduale con distanza 6. (In questa costruzione, $\bar{C}$ appare come un esempio di *codice di simmetria ternario*, nel senso di V.Pless (cfr. Pless (1972,1975)). Si noti altresì che la matrice G è formalmente analoga alla matrice generatrice del codice binario C, considerata in 1)).

Una costruzione alternativa del codice esteso $\bar{C}$ si ottiene partendo dal [4,2]-codice ternario di Hamming. Si consideri, a tale scopo, la matrice $G = \left[\begin{array}{c|c|c} \begin{matrix} J_4 - I_4 \\ \hline 0 \end{matrix} & \begin{matrix} I_4 \\ \hline H \end{matrix} & \begin{matrix} I_4 \\ \hline -H \end{matrix} \end{array}\right]$, ove H è la ma-

trice controllo di parità del predetto codice di Hamming, J_4 è la matrice di ordine 4 composta di 1. e I_4 è la. matrice identica di ordine 4. Si può verificare che G genera un $[12,6]$-codice equivalente a $\bar{C}$.

3) 1 codici di Golay ammettono delle costruzioni in termini di QR-codici.

i) Sia n = 23, q=2. Allora $x^{23}-1=(x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+$ $+ x^{10}+x^6+x^5+x^4+x^2+1)$. Per una scelta opportuna di α, si ha $g_0(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$. Il QR-codice generato da $g_0(x)$, perfetto e con distanza 7, è il codice binario di Golay.

ii) Sia n=11, q=3. Allora $x^{11}-1 = (x-1)(x^5-x^3+x^2-x-1)(x^5+x^4$ -x3+x2-1), e posto $g_0(x) = x^5-x^3+x^2-x-1$ il QR-codice generato da $g_0(x)$, . perfetto e con distanza 5, è il codice ternario di Golay.

4) (Unicità dei codici di Golay)

1 codici di Golay sono univocamente determinati dai loro parametri. Precisamente, valgono i seguenti:

TEOREMA 1. Sia C un $(24,2^{12},8)$-codice binario. Allora C è equivalente al codice binario esteso di Golay, e ogni $(23,2^{12},7)$-codice binario è equivalente al codice binario di Golay.

TEOREMA 2. Sia C un $(12,3^6,6)$-codice ternario. Allora C

equivalente al codice ternario esteso di Golay, e ogni $(11,3^6,5)$-codice ternario è equivalente al codice ternario di Golay.

1 precedenti teoremi di unicità sono stati provati, nell'ipotesi che C sia un codice lineare, da Pless (1968). Nella loro generalità, si devono a Delsarte. Goethals (1975). e nel caso binario anche a Snover (1973). Essi coronano, per la parte relativa ai codici di Golay, l'analisi dei codici perfetti definiti su campi di Calois, condotta soprattutto da van Lint e Tietäväinen. Risultati di van Lint (cfr. ad es. van Lint (1971)), completati da Tietäväinen (1973), provano infatti che un codice perfetto non banale definito su GF(q) ha necessariamente gli stessi parametri di un codice di Hamming o di Golay. Nel caso binario, ne discende in particolare che un codice lineare binario perfetto. non banale e correttore di e errori, è equivalente a: i) un codice di Hamming $(n=2^k-1, d=2e+1=3)$; ii) il codice binario di Golay $(n=23, d=2e+1=7)$.

C) (Costruzione dei sistemi di Steiner associati ai gruppi di Mathieu)

1 sistemi di Steiner associati ai gruppi di Mathieu ammettono costruzioni dirette a partire dai codici di Golay.

1) Sia $\overline{C}$ l'estensione del codice binario C di Golay, e si ponga $\Omega = \{1,\ldots,24\}$. Poiché $\overline{C}$ ha distanza 8, i supporti di due parole distinte di $\overline{C}$ di peso 8 hanno al più 4 punti in comune, i.e. 5 punti di Ω sono contenuti in al più un sottoinsie

UNIVERSITÀ DEGLI STUDI DIPAR. DI MAT. M. LECCE

me di Ω, supporto di una parola di peso 8. D'altra parte, come si è osservato in B), $\bar{C}$ contiene 759 parole di peso 8, i cui supporti contengono dunque $759 \cdot \binom{8}{5} = \binom{24}{5}$ (cioé tutti i) sottoinsiemi di Ω di cardinalità 5. Si conclude che i supporti delle parole di C di peso 8 formano un sistema di Stoiner S(5,8,24) (e lo parole di C di peso 7 formano un sistema di Steiner S(4,7,23)).

2) Sia $\bar{C}$ l'estensione del codice ternario C di Golay, e si ponga $\Omega = 1\ 1,\ldots,12)$. Il codice C ha 132 parole di peso 5, 132 parole di peso 6, 330 parole di peso 8, 110 parole di peso 9, e 24 parole di peso 11. $\bar{C}$ ha, di conseguenza, 264 parole di peso 6, 440 parole di peso 9. e 24 parole di peso 12. Poiché $\bar{C}$ ha distanza 6. due parole x,y di $\bar{C}$ di peso 6, con $x \neq \pm y$, hanno supporti con al più 4 punti in comune, i.e. 5 punti di Ω sono contenuti in al più un sottoinsieme di Ω, supporto di una parola $\pm x \in \bar{C}$ di peso 6. Poiché vi sono in $\bar{C}$ 132 coppie $\{x,-x\}$, i loro supporti contengono $132 \cdot 6 = 792 = \binom{12}{5}$ (cioé tutti i) sottoinsiemi di Ω di cardinalità 5. Si conclude che i supporti delle coppie $\{x,-x\}$ con $x \in \bar{C}$ e $w(x) = 6$, formano un sistema di Steiner S(5,6,12). Analogamente, i supporti delle coppie $\{x,-x\}$, con $x \in C$ e $w(x) = 5$. formano un sistema di Steiner S(4,5,11).

3. Le costruzioni precedenti sono anche derivabili, come casi particolari, da teoremi generali che mostrano come da certi codici lineari si possano ottenere in vari modi dei disegni:

(a) Benché si debba a Paige (1956). pur sotto spoglie diverse (cfr. D)) la scoperta del legame fra il codice binario di Golay e S(4,7,23), e fra il codice ternario di Golay e S(4,5,11), e già in Bose (1961) si trovino disegni costruiti a partire da codici, sembra che Assmus, Mattson (1967) abbiano per primi posto i fondamenti di una descrizione delle connessioni fra codici e disegni. In particolare, Assmus. Mattson (1967) provano il seguente (non difficile):

TEOREMA. Sia C un codice lineare di lunghezza n su GF(q), con distanza 2e+1. C è perfetto se e solo se i supporti delle parole di peso minimo formano un (e+1)-(n,2e+1,λ) disegno D, con $\lambda = (q-1)^e$. In particolare, se C è un codice binario perfetto (non necessariamente lineare), D è un sistema di Steiner S(e+1,2e+1,n) estendibile a un sistema di Steiner

$S(e+2,2e+2,n+1)$, costituito dai supporti delle parole di peso $2e+2$ del codice esteso $\bar{C}$.

Il risultato precedente, applicato ai codici di Hamming e ai codici di Golay, dà luogo alle seguenti costruzioni:

i) Sia C un $[n,n-k]$-codice di Hamming su $GF(q)$. Allora $n = (q^k-1)/(q-1)$, $e = 1$, e le parole di peso 3 di C danno luogo a un $2-(n,3,q-1)$ disegno D, i cui punti e blocchi sono rispettivamente i punti e le terne di punti collineari di $PG(k-1,q)$. In particolare, per $q=2$, $D=S(2,3,2^k-1)$ è il disegno dei punti e delle rette di PG(k-1.2). e il codice esteso $\bar{C}$ dà luogo al sistema di Steiner $D^+ = AG_2(k,2)$.

ii) Sia C il $[23,12]$-codice binario di Golay. 1 supporti delle parole di peso 7 formano un sistema di Steiner $S(4,7,23)$, che si estende in $\bar{C}$ a $S(5,8,24)$.

(Come si è accennato in B), i codici di Hamming e il $[23,12]$-codice di Golay sono gli unici codici lineari perfetti non banali su GF(2). Si noti inoltre che il risultato di Cameron (1974) analizzato in §4,E) (Teorema 1), rivela quali siano le semplici proprieta geometriche necessarie affinché un sistema di Steiner di parametri $e+1,2e+1,n$, o una sua estensione, originino da un codice binario perfetto nel modo sopra descritto).

iii) Sia C il $[11,6]$-codice ternario di Golay. 1 supporti delle parole di C di peso 5 formano un $3-(11,5,4)$ disegno D. Tenendo poi conto del fatto che C è perfetto, correttore di 2 errori, si vede facilmente che 4 punti di $\Omega = \{1,\ldots,11\}$

sono contenuti in uno e un solo blocco di D, i.e. D è un sistema di Steiner S(4,5,11). Considerando infine il codice esteso $\bar{C}$, non è difficile estendere D a S(5,6,12).

(b) Forse il più importante teorema che connette a un assegnato codice lineare, sotto certe condizioni, vari disegni, è il seguente:

TEOREMA (Assmus. Mattson (1969). Siano C un $[n,k]$-codice su GF(q), $C^{\perp}$ il codice duale di C, d e $d^{\perp}$ le distanze di C e $C^{\perp}$ rispettivamente. Siano t un intero minore di d, v_0 il massimo intero per il quale $v_0 - [(v_0+q-2)/(q-1)] < d$, w_0 il massimo intero per il quale $w_0 - [(w_0+q-2)/(q-1)] < d^{\perp}$ (ove si ponga $v_0 = w_0 = n$ se $q = 2$). Si supponga che il numero dei pesi delle parole di $C^{\perp} \setminus \{0\}$ che non superano n-t, non sia superiore a d-t. Allora, per ogni peso v con $d \leq v \leq v_0$, i supporti delle parole di C di peso v formano un t-disegno, e per ogni peso w con $d^{\perp} < w \leq \min\{n-t, w_0\}$, i supporti delle parole di $C^{\perp}$ di peso w formano un t-disegno. (La condizione su v_0 implica che due parole di C di peso $\leq v_0$ con lo stesso supporto, differiscono per un multiplo scalare. Analogamente per w_0.)

Applicando questo teorema, Assmus e Mattson produssero vari nuovi 5-disegni e riottennero 5-disegni già noti. In particolare:

i) Se C è perfetto, è noto che il numero dei pesi non nulli in $C^{\perp}$ non supera (d-1)/2. Si può allora porre $t = (d+1)/2$

e ottenere dei t-disegni, fra i quali quelli ottenuti in (a) usando Assmus. Mattson (1967).

ii) Se C è il $[12,6]$-codice ternario esteso di Golay, $C=C^{\perp}$, e le parole di $C \setminus \{\underline{0}\}$ hanno peso 6,9, o 12. Per $t=5$, $v=6$, si ottiene allora $S(5,6,12)$. (Anche per $v=9$ si ottiene un 5-disegno, ma è il disegno costituito dalla totalità dei sottoinsiemi di cardinalità 9 di $\Omega = \{1,\ldots,12\}$).

iii) Se C è il $[24,12]$-codice binario esteso di Golay. $C=C^{\perp}$ e le parole di $C\setminus\{\underline{0}\}$ hanno peso 8,12,16 o 24. Per $t=5$ si ottengofio allora i seguenti disegni: a) il sistema di Steiner $S(5,8,24)$ costituito dai supporti delle parole di C di peso 8; b) il 5-(24,12,48) disegno costituito dai supporti delle parole di C di peso 12; c) il 5-(24.16.78) disegno complementare di $S(5,8,24)$.

4) E' possibile provare, dopo l'esistenza. anche l'*unicità* dc *i sistemi di Steiner associati ai gruppi* di Mathieu, usando soltanto i codici corrispondenti:

a) Per provare l'unicità di $S(5,8,24)$ si può ad esempio, dati due sistemi di Steiner S,S' di parametri 5.8.24. rappresentarne le ottadi come vettori binari di dimensione. 24. e considerare i codici binari C,C' generati dalle ottadi di S, S'. Con argomenti elementari si prova che: i) $C(C')$ è un codice autoortogonale con distanza 8, in *cui ogni parola ha peso divisibile per 4; ii) le parole di peso 8 di $C(C')$ sono precisamente le ottadi di $S(S')$; iii) $C(C')$ ha dimensione 12.i.e. $C(C')$ è autoduale;

iv) le 30 ottadi di S(S') disgiunte da un'assegnata ottade di S(S') formano un [16,5]-codice binario D(D'), autoortogonale e con distanza 8; v) un codice con i parametri di D è unico, a meno d'equivalenza: in particolare, D è equivalente a D', e pertanto esiste una permutazione σ su 16 delle 24 coordinate che manda D in D'; vi) l'ultimo, e cruciale, passo: σ si estende a una permutazione sulle 24 coordinate che manda C in C'. In forza di ii) si conclude che S è isomorfo a S'.

La dimostrazione di unicità sopra riassunta si deve a J.H.Conway ed è pubblicata in dettaglio in Bergstrand (1982). Essa si può altresì considerare come un'applicazione della teoria dell'incollamento ("gluing") fra codici, cfr. Pless (1982), p. 141 e segg..

Secondo linee simili, Bergstrand (1982) ha provato anche l'unicità di S(4,7,23) e S(3,6,22):

b) Si considerino due sistemi di Steiner S,S' di parametri 4,7,23 , i codici binari C,C' da essi generati, e le loro estensioni $\bar{C},\bar{C}'$. Le parole di peso 8 di $\bar{C}(\bar{C}')$ formano un sistema $\bar{S}$ ($\bar{S}'$) di parametri 5,8,24, la cui contrazione nella nuova coordinata $\infty(\infty')$ coincide con S(S'). Poiché $\bar{S}$ e $\bar{S}'$ sono fra loro isomorfi, e hanno gruppi di automorfismi transitivi, esiste una permutazione di grado 24 che manda S in S' e ∞ in ∞': segue che S è isomorfo a S'.

c) I codici binari C,C' generati da due sistemi S,S' di parametri 3,6,22 sono dei [22,11]-codici autoduali con distanza

6. che si possono estendere, aggiungendo due nuove coordinate e un opportuno nuovo vettore, a due [24,12]-codici con distanza 8. Contraendo questi codici nell'ultima coordinata si ottengono due [23,12]-codici perfetti, le cui parole di peso minimo formano dei sistemi S(4.7.23). Poiché tali sistemi sono fra loro isomorfi, e hanno gruppi di automorfismi transitivi, si conclude che S e S' sono fra loro isomorfi. (Alternativamente, l'unicità di S(3,6,22) segue dal fatto che vi è un unico [22,11]-codice autoduale con distanza 6. cfr. Pless, Sloane (1975)).

d) Di carattere essenzialmente computazionale è invece la dimostrazione di unicità di S(5,6,12), sempre di Bergstrand (1982). Viene infatti prodotto un algoritmo per la costruzione di una base B per uno specifico [12,6]-codice su GF(3), e si dimostra che i 6 vettori di B possono considerarsi come 6 esadi di un arbitrario S(5,6,12). L'unicità di S(5,6,12) si deduce dal fatto che le esadi in B determinano completamente le 132 esadi del sistema S(5,6,12) (le quali sono precisamente i supporti delle parole di peso 6 del codice costruito). In modo del tutto analogo si prova l'unicità di S(4,5,11).

D) (1 gruppi di Mathieu come gruppi di automorfismi dei codici di Golay).

I) Considerando i sistemi di Steiner "contenuti" nei codici di Gola)

e nei codici da essi derivabili per estensione o contrazione, si può dedurre che i gruppi di Mathieu sono i gruppi degli automorfismi dei codici corrispondenti.

1) Sia $\bar{C}$ l'estensione del codice binario di Golay C, e sia C' il $[22,12]$-codice binario che si ottiene elidendo l'ultima coordinata nelle parole di C. Il gruppo delle invarianze e il gruppo degli automorfismi di $\bar{C}$ ovviamente coincidono, ed è $\mathrm{Aut}(\bar{C})=M_{24}$. Basta infatti osservare che i) $\mathrm{Aut}(C)$ preserva i pesi delle parole, e dunque preserva il sistema di Steiner $S(5,8,24)$ formato dai supporti delle parole di peso 8 di $\bar{C}$; ii) le parole di peso 8 generano $\bar{C}$. Scende poi che $\mathrm{Aut}(C)=M_{23}$, e $\mathrm{Aut}(C')=M_{22}$.

2) Nel caso ternario la situazione è leggermente più complessa. Precisamente: i) Il gruppo delle invarianze dell'estensione $\bar{C}$ del codice ternario di Golay C, è estensione non spezzata del gruppo ciclico di ordine 2 generato dalla matrice $-I_{12}$ mediante M_{12}, e $\mathrm{Aut}(C)=M_{12}$. ii) Il gruppo delle invarianze del codice di Golay C è il prodotto diretto $\langle -I_{11} \rangle \times M_{11}$, e $\mathrm{Aut}(C)=M_{11}$.

In forza di 1) e 2) i codici binari $\bar{C}$,C,C', e i codici ternari $\bar{C}$,C, danno luogo a moduli naturali per i gruppi di Mathieu corrispondenti. Dai suddetti codici si ottengono anche facilmente rappresentazioni irriducibili di grado minimo (su GF(2) e GF(3)) per i gruppi di Mathieu. Infatti:

1') Il $[24,12]$-codice binario $\bar{C}$ contiene il sottospazio $\langle 1 \rangle$, invariante per M_{24}, e lo spazio quoziente $\bar{C}/\langle 1 \rangle$ è un modulo

irriducibile per M_{24} di dimensione 11, la minima possibile per M_{24} su GF(2). In modo del tutto analogo, dal [23,12]-codice binario C si ottiene un modulo irriducibile per M_{23}, di dimensione minima 11 su GF(2). Infine, il complemento ortogonale del [22,12]-codice C' è un modulo irriducibile per M_{22}, di dimensione minima 10 su GF(2).

(Questi moduli, e i loro duali, saranno discussi più dettagliatamente, e da un punto di vista leggermente diverso, in §ll,B). Cfr. anche il seguente punto II).)

2') Il [12,6]-codice ternario $\bar{C}$ è un modulo per il ricoprimento $C_2 \cdot M_{12}$, di dimensione minima 6 su GF(3). Ad esso corrisponde una rappresentazione projettiva di M_{12} in PG(5,3), che non si solleva a una rappresentazione lineare di M_{12} (il grado minimo di una rappresentazione lineare di M_{12} su GF(3) essendo 10). Segue da 2), ii) che C è un modulo per M_{11}. Il sottospazio di C, costituito dalle parole con somma delle coordinate nulla, coincide con $C^{\perp}$, ed è un modulo irriducibile di dimensione 5 per M_{11}. Questo modulo, e il suo duale, sono i moduli di dimensione minima per M_{11} su GF(3).

Come si è già accennato in C), Paige (1956) fu il primo a connettere gruppi di Mathieu e codici di Golay, pur non usando la terminologia della teoria dei codici. In particolare, Paige descrive una rappresentazione irriducibile di M_{23}, di grado 11 su GF(2), e lo spazio in cui tale rappresentazione viene descritta è naturalmente equivalente al codice binario di Golay. Traendo spunto da Paige (1956). Assmus, Mattson (1966A) hanno per primi illustrato in modo esplicito le relationi fra gruppi di Mathieu e codici di Golay, provando i risultati descritti in 1), 2), e parte di quelli descritti in 1') e 2').

Un'altra dimostrazione del fatto che M_{24} e M_{12} sono i gruppi degli automorfismi dei codici estesi di Golay si trova in Shaughnessy (1971). Vi si prescinde dai sistemi di Steiner "contenuti" in tali codici. usando invece la loro struttura di QR-codici per esibire direttamente degli automorfismi che generano M_{24} e M_{12}.

Nello stesso ordine d'idee. ma in un contesto più generale. si collocano i risultati di Rasala (1976):

Sia C un QR-codice di lunghezza n su GF(q), con q=p o $q=p^2$ secondo che il numero primo p sia o no un residuo quadratico mod n, e sia $\bar{C}$ l'estensione di C (cfr. A)). A.M.Gleason e E.A.Prange hanno provato che $Aut(\bar{C})$ contiene PSL(2,n), nella sua azione naturale di grado n+l (per una discussione dettagliata, cfr. Assmus, Mattson (1969)). Rasala (1976) assume la proprietà $Aut(\bar{C}) \supseteq PSL(2,n)$ in una definizione alternativa molto generale di QR-codice (su un opportuno anello commutativo). In particolare, ad ogni QR-codice esteso $\bar{C}$ di lunghezza n+l su $GF(p^2)$ Rasala associa, considerando $GF(p^2)^{n+1}$ come spazio lineare di dimensione 2(n+1) su GF(p), il *codice spezzato* (split code) costituito dallo stesso $\bar{C}$, pensato come codice di lunghezza 2(n+1) e dimensione n+l su GF(p) . Se n=2s+1, con s primo, e $s \neq p$, è interessante confrontare il QR-codice $\bar{C}$ di lunghezza n+l su GF(p) con il codice spezzato di lunghezza 2(s+1)=n+1 s u GF(p). Rasala (1976) prova che questi codici risultano isomorfi esattamente nei tre casi seguenti: i) n=7, s=3, p=2, e il codice in questione è l'estensione del [7,4]-codice binario di Hamming; ii) n=11, s=5, p=3, e il codice è il [12,6]-codice ternario esteso di Golay; iii) n=23, s=11, p=2, e il codice è il [24,12]-codice binario esteso di Golay.In virth di questi "isomorfismi speciali", si riconosce che in ii) $Aut(\bar{C}) = < PSL(2,11), PSL(2,5) > = M_{12}$, e in iii) $Aut(\bar{C}) = < PSL(2,23), PSL(2,11) > = M_{24}$. In particolare, per questa via Rasala ottiene i generatori di Conway (1971)

(cfr. §10), e deriva alcune delle proprietà strutturali di M_{12} e M_{24} (e.g. descrive sottogruppi notevoli, e illustra l'immersione di M_{12} in M_{24}).

(Per le applicazioni di tecniche di teoria dei codici all'esame di proprietà strutturali di M_{24}, "riducendo al minimo" la teoria dei gruppi necessaria. cfr. anche Berlekamp (1971)).

(Il problema di determinare per quali valori di n sia $\mathrm{Aut}(\bar{C}) \supset \mathrm{PSL}(2,n)$, parzialmente indagato in Assmus, Mattson (1969) e Shaughnessy (1971). pub considerarsi virtualmente risolto se si assume la classificazione dei gruppi di permutazioni 2-transitivi, poiché $\mathrm{Aut}(\bar{C})$ è certamente 2-transitivo. e anzi 3-transitivo se $n \geq 5$ (Shaughnessy (1971)). In particolare, se $\mathrm{Aut}(\bar{C})$ è semplice, la sua determinazione si connette al problema di determinare i gruppi .di permutazioni G per i quali $\mathrm{PSL}(2,n) < G \leq A_{n+1}$, problema che risale a Mathieu (1873) (cfr. §9). 1 casi che si presentano sono i seguenti:. a) $n=5$, $p=2$, $q=4$: $\mathrm{Aut}(\bar{C}) = A_6 > A_5 = \mathrm{PSL}(2,5)$; b) $n=7$, $p=2$: $\mathrm{Aut}(\bar{C}) = \mathrm{AGL}(3,2)$; c) $n=11$, $p=3$: $\mathrm{Aut}(\bar{C}) = M_{12}$; d) $n=23$, $p=2$: $\mathrm{Aut}(\bar{C}) = M_{24}$.)

11) Alcune delle rappresentazioni descritte nei punti 1') e 2') della sezione precedente appaiono, sotto vesti diverse, in vari luoghi della letteratura precedente Assmus, Mattson (1966A). Così, Coxeter (1958) considera 12 punti di PG(5.3). che si possono distribuire in 66 coppie di esadi complementari, dando luogo a un sistema di Steiner $S(5,6,12)$, e rappresenta M_{12} come il gruppo delle collineazioni di PG(5.3) che preservano tale $S(5,6,12)$. (Notiamo, incidentalmente, che i 12 punti di

Coxeter, giustapposti a due a due, formano le righe di una matrice generatrice del codice ternario esteso di Golay). Ulteriori dettagli su questa rappresentazione projettiva di M_{12} si trovano in Whitelaw (1966). Garbe. Mennicke (1964) descrivono una rappresentazione di M_{12}, di dimensione minima 10 su GF(3), associata alla rappresentazione projettiva di Coxeter.

Todd (1959) mostra che M_{12} opera come un gruppo S-transitivo sui 12 iperpiani di PG(5,3) che non contengono alcuno dei punti di Coxeter. La rappresentazione che si ottiene è distinta da quella sui punti, e si scambia con essa mediante un automorfismo esterno di M_{12}. Todd mostra inoltre che sull'insieme costituito dai 12 punti e dai 12 iperpiani si può formare in modo naturale un sistema di Steiner S(5,8,24). 1 punti di questo S(5,8,24) sono identificabili con 24 punti dello spazio projettivo PG(11,2), così da ottenere una configurazione in cui 7 punti sono sempre indipendenti, e 8 punti sono dipendenti sse corrispondono a un'ottade di S(5,8,24). N e risulta una rappresentazione di M_{24} come gruppo di collineazioni d i PG(11,2) che preservano la configurazione, duale della rappresentazione di M_{24} come gruppo di automorfismi del codice binario esteso di Golay. Todd (1966) studia poi entrambe le rappresentazioni in grande dettaglio, basandosi Su un'elegante analisi delle proprietà combinatorie di S(5,8,24). Questo fondamentale lavoro di Todd è all'origine dell'approccio "puramente combinatorio" alla struttura di M_{24}, sviluppato da J.H. Conway e R.T.Curtis, e sarà pertanto ripreso in §6.

E)

Abbiamo descritto in C) delle tecniche che consentono di estrarre dei disegni da codici lineari. Inversamente, un disegno $D = (\Omega, \mathcal{B})$ genera in modo naturale un codice binario nel modo seguente. Si consideri la matrice $M = (m_{b,\alpha})$ avente righe e colonne indiciate rispettivamente da $\mathcal{B}$ e Ω, con $m_{b,\alpha} = 1$ se $\alpha \in b$, $m_{b,\alpha} = 0$ se $\alpha \notin b$ ($b \in \mathcal{B}$, $\alpha \in \Omega$). M è la *matrice d'incidenza* del disegno D : le righe di M. corrispondenti ai blocchi di D, formano un codice binario di lunghezza $n = |\Omega|$, e generano un codice lineare di lunghezza n. (In tal modo, ad es.. il codice binario esteso di Golay può essere costruito mediante la matrice d'incidenza di S(5,8,24)).

In quest'ordine d'idee si situa la rappresentazione di M_{12} come gruppo di automorfismi di una matrice di Hadamard di ordine 12 (Hall (1962)). che risulta essere equivalente alla rappresentazione di M_{12} come gruppo di automorfismi del codice ternario esteso di Golay:

Ricordiamo che una matrice $A_r = (a_{ij})$ di ordine r si dice *matrice di Hadamard* se $a_{ij} = \pm 1$ e $A_r A_r^t = r \cdot I_r$ (si vede allora facilmente che r = 1.2, oppure r è divisibile per 4). Una matrice di Hadamard A_r si dice equivalente a una matrice di Hadamard B_r se esiste una coppia (P,Q) di matrici monomiali di ordine r tali che sia $PA_rQ = B_r$. In particolare, a meno d'equivalenza si può sempre supporre A_r *normalizzata*, i.e. $a_{1j} = a_{i1} = 1$. Le coppie (P,Q) di matrici monomiali di ordine r tali che sia $PA_rQ = A_r$ si dicono *automorfismi* di A_r. GLi automorfismi di

A_r formano un gruppo $Aut(A_r)$, e $\overline{Aut(A_r)} = Aut(A_r)/\langle(-I_r,-I_r)\rangle$ è un gruppo di permutazioni fedele sull'insieme delle righe e delle colonne di A_r.

Se in una matrice di Hadamard normalizzata si sostituiscono con 0 gli elementi uguali a -1, e si sopprimono la prima riga $\ell = (a_{1j})$ e la prima colonna $c = (a_{i1})$, si ottiene una matrice di ordine r-l, che per $r > 4$ è la matrice d'incidenza di un 2-(4X +3,2X +1,λ) disegno, i.e. di un *2-disegno di Hadamard* con n=r-1 = 4X+3 (cfr. 53.1)). Inversamente, la matrice d'incidenza di ogni 2-disegno di Hadamard dà luogo, aggiungendovi una riga ℓ e una colonna c composte di uni, e sostituendo -1 al posto di 0, a una matrice di Hadamard normalizzata. (Si noti tuttavia che matrici di Hadamard equivalenti possono dar luogo a 2-disegni di Hadamard fra loro non isomorfi).

Esempi classici di 2-disegni di Hadamard sono i $2\text{-}(2^{d+1}-1, 2^d-1, 2^{d-1}-1)$ disegni formati dai punti e dagli iperpiani di PG(d,2). 2-disegni di Hadamard con $\lambda = (q-3)/4$ sono poi i cosiddetti *disegni di Paley* (Paley (1933)), i.e. i disegni $H_q = (\Omega, B)$ con $\Omega = GF(q)$, $q \equiv 3(4)$, e $B = \{ Q+x \mid x \in GF(q)\}$. Tali disegni si ottengono considerando la matrice di Hadamard

$$A_{q+1} = \left[\begin{array}{c|c} 1 & \underline{1} \\ \hline \underline{1}^t & P_q - I_q \end{array}\right],$$ dove P_q è la matrice di Paley di ordine q ($q \equiv 3(4)$). Per $\lambda = 2$, esiste un unico l-disegno

di Hadamard (a meno d'isomorfismi) : il disegno di Paley H_{11}. Si deduce in particolare da ci0 che precede, che a meno di equivalenze esiste una sola matrice di Hadamard di ordine 12.

Ogni 2-disegno di Hadamard H_{r-1} si può estendere in un unico modo a un 3-disegno H_r (che si dice 3-*disegno* di *Hadamard*). Pih in generale, è noto che ogni $2\text{-}(2m+1,m,\lambda)$ disegno D ammette sempre un' estensione (benché non necessariamente unica, se D non è simmetrico). Da $D = (\Omega, B)$ si può ottenere una tale estensione $D^+ = (\Omega^+, B^+)$ ponendo $\Omega^+ = \Omega \dot{\cup} \{\infty\}$, $B^+ = \{b \cup \{\infty\} \mid b \in B\} \cup \{\Omega \setminus b \mid b \in B\}$. E.g.: PG(d,2), considerato come 2-disegno di Hadamard, si estende al $3\text{-}(2^{d+1}, 2^d, 2^{d-1}-1)$ disegno di Hadamard formato dai punti e dagli iperpiani di AG(d+1,2). Se $D = H_{r-1}$, si ha $D^+ = H_r$. e la matrice d'incidenza di H_r si ottiene sopprimendo le righe $\ell, -\ell$ nella matrice $\begin{bmatrix} A_r \\ \hline -A_r \end{bmatrix}$. e sostituendovi con 0 gli elementi uguali a -1. E' allora facile- dedurre che $\mathrm{Aut}(H_r) = \overline{\mathrm{Aut}(A_r)}_\ell$.

In particolare, il 2-(11.5.2) disegno H_{11} si estende ad un unico $3\text{-}(12,6,2)$ disegno $H_{12} = (\Omega^+, B^+)$, con $|B^+| = 22$. Poiché $\mathrm{Aut}(H_{11}) = \mathrm{PSL}(2,11)$, 2-transitivo sui punti di H_{11} (cfr. Todd (1933), Hussain (1945)), si deduce (cfr. Hughes (1965A)) che $\mathrm{Aut}(H_{12}) = M_{11}$, 3-transitivo sui 12 punti di H_{12}. (Si può anche dimostrare direttamente, posto $\Omega^+ = \{0,1,\ldots,10,\infty\}$ e considerando la matrice d'incidenza. che $\mathrm{Aut}(H_{12}) = \langle \alpha, \beta, \gamma \rangle$, con $\alpha = (\infty,0)(1,2,4,10)(3,7,5,6)(8,9)$, $\beta = (\infty)(0,1,2,3,4,5,6,7,8,9,10)$,

$\gamma = (\infty)(0)(1,3,9,5,4)(2,6,7,10,8)$. $\langle \alpha, \beta, \gamma \rangle$ è il gruppo di Mathieu M_{11} nella sua rappresentazione S-transitiva di grado 12; $\langle \alpha^2, \beta, \gamma \rangle$ è $Aut(H_{11}) = PSL(2,11)$. Cfr. Hall (1980)). Dal fatto che $Aut(H_r) = \overline{Aut(A_r)}_{\ell}$, si può allora dedurre che $\overline{Aut(A_{12})}$ opera come il gruppo di Mathieu M_{12} sia sulle righe che sulle colonne di A_{12} (cfr. Kantor (1969B)). Le due azioni corrispondono alle due rappresentazioni S-transitive distinte di M_{12} (cfr.§3), e sono scambiate fra loro da un automorfismo esterno di M_{12}. In particolare, la matrice A_{12} consente di costruire in modo semplice e diretto una coppia di sistemi di Steiner S(5,6,12) fra loro reciproci (cfr. la costruzione di Higman-Cameron. §3,4)): basta osservare che, essendo $A_{12}A_{12}^t = 12\, I_{12}$, due righe di A_{12} coincidono su 6 colonne e differiscono sulle altre 6; ad ogni coppia di righe di A_{12} corrisponde così una coppia di esadi complementari, e le 132 esadi ottenute formano un sistema di Steiner S(5,6,12). Osservando che è anche $A_{12}^t A_{12} = 12\, I_{12}$, si costruisce in modo simile il sistema reciproco sulle righe di A_{12}: le coppie di punti distinti di questo sistema sono evidentemente in corrispondenza biunivoca con le coppie di blocchi complementari del precedente.

La rappresentazione di M_{12} sopra considerata è stata descritta per la prima volta da Hall (1962), ed è equivalente alla rappresentazione di M_{12} come gruppo degli automorfismi del codice ternario esteso di Golay (cfr. Assmus,Mattson (1966A)). Le righe di A_{12} considerate come vettori di $GF(3)^{12}$, e i loro opposti, sono precisamente le parole di peso 12 di tale codice,

e lo generano su GF(3).

(1 gruppi degli automorfismi dei 2- e dei 3-disegni di Hadamard sono stati investigati da vari autori: cfr. Norman (1968,1973), **Kantor** (1969B). Hall (1975). Ito (1980). In particolare, Norman (1968) prova il seguente: TEOREMA. Sia D un $3\text{-}(4\lambda+4, 2\lambda+2, \lambda)$ disegno (di Hadamard), con λ pari, e sia $G \leq \mathrm{Aut}(D)$ 3-transitivo sui punti di D. Allora $\lambda = 2$, $G = \mathrm{Aut}(D)$, e $G \simeq M_{11}$. Ito (1980) prova, facendo uso della classificazione dei gruppi 2 transitivi, i risultati seguenti:

1) Se $D = (\Omega, B)$ è un 3-disegno di Hadamard, e $\mathrm{Aut}(D)$ è un gruppo 2-transitivo su Ω privo di sottogruppi normali regolari, allora $|\Omega| = 12$, e $\mathrm{Aut}(D) \simeq M_{11}$;

2) Se $D = (\Omega, B)$ è un 2-disegno di Hadamard, e $\mathrm{Aut}(D)$ è un gruppo 2-transitivo su Ω privo di sottogruppi normali regolari, allora: i) $|\Omega| = 11$ e $G \simeq PSL(2,11)$; oppure ii) $|\Omega = 2^{d+1}-1$ e $G \simeq GL(d+1,2)$. i) si. presenta nel caso di H_{11}; ii) nel caso in cui D sia il disegno dei punti e degli iperpiani di $PG(d,2)$).)

Concludiamo questa sezione menzionando una costruzione di $S(3,6,22)$ mediante il disegno di Paley H_{11}, di Assmus. Mezzaroba e **Salwach**, e una costruzione combinatoria di $S(4,5,11)$ (e $S(5,6,12)$) mediante il 3-disegno di Hadamard H_{12}, proposta da D.R. Hughes:

1) Si consideri la matrice d'incidenza M del disegno H_{11}. Le righe della matrice $[I_{11}|M]$ generano su GF(2) un $[22,11]$-codice autoduale, le cui parole di peso minimo 6 danno luogo a un sistema di Steiner S(3,6,22) (Assmus,Mezzaroba,Salwach (1977)). In termini di gruppi di automorfismi, ciò corrisponde all'inclusione di PSL(2.11) = $Aut(H_{11})$ in $Aut(M_{22})$.

2) Ogni 3-$(4\lambda+4, 2\lambda+2, \lambda)$ disegno di Hadamard H da luogo a un 2-$(4\lambda+3, 2\lambda+1, 2\lambda(\lambda+1))$ disegno S. i cui punti sono le coppie (b,b'), ove b è un blocco di H e b' è il suo complemento e i cui blocchi sono le coppie (α, β), ove α e β sono punti distinti di H; l'incidenza in S è così definita: $(b,b') \in (\alpha,\beta)$ se $\alpha,\beta \in b$, oppure $\alpha,\beta \in b'$ (Hughes (1981A)). Se $\lambda = 2$. si ottiene un 2-(11,5,12) disegno, che di fatto risulta essere anche un 4-(11,5,1) disegno, i.e. un sistema di Steiner S(4,5,11). Da questa costruzione si può dedurre, con considerazioni combinatorie elementari, che Aut(S(4,5,11)) è un gruppo semplice, sottilmente 4-transitivo sui punti di S. Estendendo S(4,5,11) a S(5,6,12) si può allora provare che Aut(S(5,6,12)) è un gruppo semplice, transitivo, e quindi 5-transitivo. di grado 12. (I dettagli delle costruzioni precedenti dovrebbero apparire in Hughes (1981B). Modificando il metodo di Hughes, Beth (1981) prova poi, insieme all'esistenza, anche l'unicità di S(5,6,12)).

F) (Forme invarianti)

In D) si è osservato che: i) alla rappresentazione di M_{11}

realizzata dal codice ternario di Golay è associata una rappresentazione irriducibile di M_{11} in $V(5,3)$ (e la sua duale); ii) alla rappresentazione lineare del ricoprimento $C_2 \cdot M_{12}$, realizzata dal codice ternario esteso di Golay, corrisponde una rappresentazione projettiva di M_{12} in $PG(5,3)$ che preserva una configurazione di 12 punti e 12 iperpiani (Coxeter (1958), Todd (1959)). In un notevole lavoro, Ward (1975) caratterizza M_{11} e $C_2 \cdot M_{12}$ come i gruppi di certe forme multilineari, riottenendo da una diversa prospettiva la rappresentazione 5-dimensionale i) di M_{11} e la rappresentazione projettiva ii) di M_{12}.

Ward (1975) prova innanzitutto che esiste un'unica forma 3-lineare ϕ, simmetrica e non nulla, su $V = V(5,3)$, che soddisfi le condizioni seguenti: a) $Aut(\phi)$ $(= \{g \in GL(5,3) \mid \phi(g^{-1}x, g^{-1}y, g^{-1}z) = \phi(x,y,z)$, per ogni x,y,z e $V\})$ è irriducibile; b) esiste $0 \neq u \in V$, tale che sia $\phi(u,u,v) = 0$ per ogni $v \in V$. A meno d'equivalenza. si può assumere che sia $V = GF(3^5)$, considerato come spazio vettoriale su $GF(3)$, e $\phi = \phi(x,y,z) = Tr(xyz^9 + xy^9z + x^9yz)$, ove $Tr(a)$, a e $GF(3^5)$, è la traccia dell'endomorfismo $v \to av$ dello spazio $V = GF(3^5)$. Ne segue che l'insieme delle rette $\langle u \rangle$ di V. tali che sia $\phi(u,u,v) = 0$ per ogni $v \in V$, è l'insieme $E = \{\langle \varepsilon^i \rangle \mid i = 0, \ldots, 10\}$, ove $\varepsilon \in GF(3^5)^*$ ha ordine li e $Tr(\varepsilon) = 1$.

$Aut(\phi)$ opera naturalmente su E. e l'identificazione di $Aut(\phi)$ con M_{11} può essere ottenuta mostrando che $Aut(\phi)$ è sottilmente 4-transitivo su E, e certi 66 iperpiani di V contengono ciascuno un sottoinsieme di E di cardinalità 5. in modo che questi sottoinsiemi formano i blocchi di un sistema di

Steiner $S(4,5,11)$ preservato da $Aut(\phi)$. L'azione di M_{11} su E consente poi di descrivere esplicitamente vari sottogruppi di M_{11}. E.g.: per lo studio der sottogruppi transiviti su E, Ward "depolarizza" ϕ, passando a considerare lo spazio D delle funzioni $\theta : V \to GF(3)$ che soddisfano le condizioni: a) $\theta(cx) = c\theta(x), (c \in GF(3), x \in V)$: b) $\theta(x+y+z) - \theta(x+y) - \theta(x+z) - \theta(y+z) + \theta(x) + \theta(y) + \theta(z) = \nu\phi(x,y,z)$, $(\nu = \nu(\theta) \in GF(3); x,y,z \in V)$. D è uno spazio di dimensione 6 su $GF(3)$, e ogni $\theta \in D$ si scrive nella forma $\theta = -\nu(\theta)Tr(x^{11}) + v^*$, per un certo $v^* \in V^*$, il duale di V (si può assumere sia $V^* = \{v^* | v^*(y) = Tr(vy), \forall y \in V\}$). $M11 =$ $= Aut(\phi)$ opera su D con l'azione: $(g\theta)(x) = \theta(g^{-1}x)$. $g \in M_{11}$, $x \in V$; e preserva l'insieme $F_0 = \{\theta \in D |\ v(e) = -1,\ e(u) \neq 0.\ \forall \langle u \rangle \in E\} =$ $= \{Tr(x^{11}), Tr(x^{11} + \varepsilon^i x),\ 0 \leq i \leq 10\}$, M_{11} è 3-transivito su F_0, e da ciò è possibile dedurre, con qualche ulteriore considerazione, che un sottogruppo transivito massimale di M_{11} è necessariamente lo stabilizzante di un punto di F_0, isomorfo a $PSL(2,11)$.

Ward è poi in grado di costruire M_{12}. A tale scopo, definisce su D la forma 4-lineare $\Psi = \Psi(\theta_1,\theta_2,\theta_3,\theta_4) = (\sum_{\langle u \rangle \in E} \theta_1(u)\theta_2(u)\theta_3(u)\theta_4(u)) + \nu(\theta_1)\nu(\theta_2)\nu(\theta_3)\nu(\theta_4)$, e il prodotto scalare $(\theta_i, \theta_j) = - \nu(\theta_i)\nu(\theta_j) + Tr(x_i x_j)$. $Aut(\Psi)$ contiene M_{11}, e opera con nucleo $\langle -1 \rangle$ sull'insieme $F = \{\langle \theta \rangle | \theta \in F_0\}$. L'identificazione di $Aut(\Psi)/\langle -1 \rangle$ con M_{12} si può a questo punto ottenere in più modi: 1) costruendo un sistema di Steiner $S(5,6,12)$ sui punti di F; 2) generando la matrice di Hadamard A_{12} (cfr. E); posto

$F_o = \{\theta_1, \ldots \theta_{12}\}$, è $A_{12} = (a_{ik})$ con $a_{ik} = (\theta_i, \theta_k) = \pm 1$); 3) identificando D con il codice ternario esteso di Golay. In particolare, la rappresentazione di $Aut(\Psi) = C_2 \cdot M_{12}$ su D subordina la rappresentazione projettiva di Coxeter-Todd: i punti di Coxeter sono le rette di F. e gli iperpiani sono i 12 iperpiani di D che non contengono alcuna retta di F. L'esistenza di automorfismi esterni di M_{12}, e di due classi di sottogruppi coniugati di M_{12}, isomorfi a M_{11}, emerge in modo naturale: 1) per ogni $g \in GL(D)$, sia g^π l'inverso-aggiunto di g (i.e. $(g^\pi \theta_i, g\,\theta_j) = (\theta_i, \theta_j)$ per ogni $\theta_j, \theta_j \in D$). L'applicazione $g \to g^\pi$ preserva $Aut(\Psi)$ e subordina un automorfismo esterno di M_{12}. 2) $Aut(\phi)$, 3-transitivo su F, e $Aut(\phi))^\pi$, lo stabilizzante di $Tr(x^{11})$ in $Aut(\Psi)$, rappresentano le due classi di sottogruppi coniugati isomorfi a M_{11}.

(Notiamo, per completezza, che le forme ϕ e Y sopra considerate originano dallo studio degli invarianti delle rappresentazioni di dimensione 5 e 6 di SL(2,11) su GF(3), dedotte dalla rappresentazione di Weyl (cf.Ward (1972)).

56. L'ANALISI COMBINATORIA DI TODD-CONWAY-CURTIS

Todd (1966). già citato in §5,D), analizza in termini combinatori la rappresentazione di M_{24} realizzata dal codice binario esteso di Golay, e la sua duale, ottenendo in particolare una descrizione completa delle collineazioni di PG(11.2) contenute in M_{24}, e ricavandone un elenco di otto classi di coniugio di sottogruppi massimali di M_{24}, tutte immediatamente interpretabili (con l'eccezione di PSL(2,23)) in funzione della geometria di S(5,8,24).

L'analisi combinatoria di S(5,8,24) contenuta in Todd (1966) è il fondamento dell'approccio alla struttura dei gruppi di Mathieu, sviluppato da D. Livingstone e dai suoi studenti (in direzione dell'analisi dei sottogruppi dei gruppi di Mathieu; cfr.§7), e da J.H. Conway e R.T. Curtis.

1) Rimandando alle lezioni di Conway (Oxford, 1969). raccolte in Conway (1971). per una limpida e articolata trattazione degli esiti dell'analisi di Todd, riprendiamo qui alcuni punti essenziali di tale analisi (in parte già utilizzati senza riferimenti espliciti, oppure ottenuti per altra via, in §4 e §5).

Sia S = (Ω,$\mathcal{B}$) il sistema di Steiner S(5,8,24) costruito su Ω = PG(1.23) = GF(23) U {∞} (à la Carmichael, cfr.§3,2)), e si dia all'insieme delle parti 2^{Ω} la struttura di spazio vettoriale (di dimensione 24) su GF(2), definendo come somma di due elementi X, Y di 2^{Ω} la loro differenza simmetrica:

$X+Y = X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$. Todd (1966) osserva che i blocchi di S (ottadi) soddisfano le condizioni seguenti:

i) Se 01.02 e B. $|0_1 \cap 0_2| = 0,2,4,8$ (cfr. il triangolo delle intersezioni, in 54.A)).

ii) Se $|0_1 \cap 0_2| = 4$. $01 + 0_2$ e B.

Poiché 4 punti di Ω appartengono a 5 ottadi distinte, ne segue che 4 punti di Ω determinano una partizione di Ω in 6 tetradi, con la proprieta che la somma di due tetradi è un'ottade. Una tale partizione di Ω si dice *sestetto*. Vi sono $\binom{24}{6}/6 = 1771$ sestetti.

iii) Se $|0_1 \cap 0_2| = 0, \Omega \setminus (0_1 + 02)' = 03$ e B.

Tre ottadi mutualmente disgiunte costituiscono un *trio*. Fissata un'ottade 0, vi sono 30 ottadi disgiunte da 0, e quindi vi sono esattamente 15 trii contenenti 0. Si conclude che il numero dei trii è $759 \cdot 15/3 = 3795$.

iv) Se $(01 \cap 0_2| = 2$, $01 + 0_2$ ha cardinalità 12, i.e. è una dodccade.

Si verifica facilmente, usando i) e ii), che $A = 0_1 + 0_2$ non contiene ottadi. Poiché due ottadi si intersecano con cardinalità pari, si deduce allora che, scelti 5 punti in Δ, l'ottade da essi determinata contiene un unico ulteriore punto di A. Si viene a determinare in questo modo una configurazione di esadi contenute in Δ, che formano un sistema di Steiner S(5,6,12). Un sottoinsieme di cardinalità 6 di un'ottade

si dirà *esade speciale*: ogni ottade contiene 28 esadi speciali, e ogni esade speciale è contenuta in 16 dodecadi. Poiché le esadi di un sistema $S(5,6,12)$ sono 132, da ciò che precede segue che vi sono esattamente $759 \cdot 28 \cdot 16/132 = 2576$ dodecadi. Delle 759 ottadi, 132 intersecano Δ in esadi speciali (dando luogo a $S(5,6,12)$), $\binom{12}{4} = 495$ intersecano A in tetradi, e le restanti 132 intersecano A in 2 punti. L'ultima asserzione si giustifica osservando che, per ciascuna delle 66 coppie $\{\delta_1, \delta_2\}$ di punti di A, delle 77 ottadi che contengono δ_1 e δ_2 30 intersecano A in esadi speciali, 45 in tetradi, e 2 soltanto in δ_1 e δ_2. Queste ultime due ottadi non hanno altri punti in comune, e la loro somma è pertanto una dodecade, complementare di A.

Si rappresentino ora gli elementi di 2^Ω come vettori binari di dimensione 24 (identificando ogni $X \in 2^\Omega$ con il vettore binario (x_α), ove $x_\alpha = 1$ se $\alpha \in X$, $x_\alpha = 0$ se $\alpha \notin X$), e si consideri il sottospazio C di $2^\Omega = V(24.2)$ generato dalle ottadi di $S(5,8,24)$.

Poiché due ottadi si intersecano con cardinalità pari, si ha evidentemente $C \subseteq C^\perp$, e quindi $\dim(C) \leq 12$. D'altra parte, C contiene $\emptyset, \Omega$, le 759 ottadi e i loro complementi, e le 2576 dodecadi. Poiché $1+1+2 \cdot 759+2576 = 2^{12}$, si conclude che C ha dimensione 12, ed è unione disgiunta dei sottoinsiemi $C_0 = \{\emptyset\}$, $C_{24} = \{\Omega\}$, $C_8 = B$, $C_{16} = \{\Omega + O \mid O \in B\}$, $C_{12} = \{O_1 + O_2, O_1, O_2 \in B, |O_1 \cap O_2| = 2\}$.

Naturalmente. C non è altro che il codice binario esteso

di Golay, e M_{24} è il gruppo delle permutazioni su Ω che preservano C. (Poiché M_{24} è 5-transitivo sui punti di Ω, e un sestetto è individuato da una sua tetrade qualsiasi, scende subito che M_{24} è transitivo sulle ottadi e sui sestetti. Come si vedrà in §7, M_{24} è transitivo anche sui trii e sulle dodecadi di C).

Si è osservato in iv) che su una dodecade A si costruisce un sistema di Steiner S(5,6,12), realizzato dalle ottadi che intersecano Δ in esadi speciali. E' perciò possibile introdurre in modo naturale il gruppo di Mathieu M_{12}, definendolo come il gruppo degli automorfismi del sistema S(5,6,12) così ottenuto (ovvero, come lo stabilizzante di A in M_{24}). Questo tipo di approccio a M_{12}, particolarmente elegante in un contesto geometrico-combinatorio come quello delineato in questo paragrafo, è adottato ad es. da Beth, Jungnickel (1981), in una trattazione che, riprendendo l'analisi combinatoria di Todd, ha come obiettivo una presentazione unitaria dei gruppi di Mathieu con metodi combinatori essenzialmente elementari.

(Di Beth, Jungnickel (1981) cogliamo qui l'occasione di segnalare le dimostrazioni di unicità di S(5,6,12) e S(5,8,24):

a) Si consideri il sistema di Steiner S_Δ = S(5,6,12) costruito su una dodecade Δ, e sia A' la dodecade complementare di A. Per ogni $\alpha \in A'$, le ottadi che intersecano Δ' in α e in un solo altro punto determinano su A 11 coppie di esadi complementari, che formano un 3-(12,6,2) sottodisegno

di Hadamard di S_Δ . S_Δ contiene pertanto 12 3-disegni di Hadamard, che sono permutati transitivamente da $M_{12} = Aut(S_\Delta)$ **Beth,Jungnickel** (1981) provano che *ogni* sistema di Steiner S(5,6,12) contiene esattamente 12 sottodisegni di Hadamard, e che, se $H_{12} = (\Omega_H, B_H)$ è un 3-(12-6.2) disegno di Hadamard contenuto in un arbitrario sistema di Steiner $S = S(5,6,12) = (\Omega, B)$, si ha $B = B_H \cup \{ X+Y | X,Y \in B_H , X \neq Y, Y' \}$. Dunque B_H determina B, e dall'unicità del disegno di Paley H_{11} e della sua estensione H_{12} (cfr. §5,E)) segue l'unicità di S (e di $M_{12} = Aut(S)$).

b) Si considerino due dodecadi Al, Δ_2 relative a due sistemi di Steiner S_1, S_2 di parametri 5,8,24. **Beth. Jungnickel** (1981) provano che ogni isomorfismo fra i sistemi di Steiner di parametri 5,6,12 subordinati da Sl e S_2 sulle dodecadi Δ_1 e Δ_2 si estende in un unico modo a un isomorfismo fra S_1 e S_2. Dall'unicità di S(5,6,12) segue allora l'unicità di S(5,8,24) (e di $M_{24} = Aut(S(5,8,24))$).

2) Come si è detto, la descrizione delle proprietà dei gruppi di Mathieu. condotta in **Conway** (1971). si fonda sull'analisi di **Todd (1966).** In effetti, Conway (1971) definisce M_{24} mediante espliciti generatori in S_Ω (cfr.§10), e introduce il codice C come il sottospazio di 2^Ω generato da Ω e dai 23 sottoinsiemi $N_i = \{ n-i \mid n \in \Omega \setminus Q^\circ \}$, ove $i \in GF(23)$ e $Q^\circ = \{ x^2 \mid x \in GF(23) \}$. Dopo di ciò. prova che C ha dimensione 12 ed è invariante per M_{24}; e infine che C contiene ottadi, e che l'insieme delle ottadi contenute in C è un sistema

di Steiner $S(5,8,24)$. (Si noti che C è anche generabile. come sottospazio di 2^{Ω}, dalle immagini di Q° per l'azione di PSL(2.23) su Ω, "à la Carmichael".)

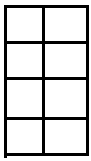
In modo simile, Conway (1971) definisce M_{12} mediante una esplicita presentazione in SA. $A = PG(1,11) = GF(11) \cup \{\infty\}$ (cfr.§10), e introduce il codice ternario esteso di Golay C come il sottospazio di $V(12,3)$ generato, rispetto alla base $\{e_i \mid i = \infty, 0, \ldots, 10\}$, dai vettori $w_{\infty} = \Sigma e_i$ e $w_j = \Sigma_{r \in N-j} e_r - \Sigma_{s \in Q^{\circ}-j} e_s$, o v e $j \in GF(11)$, $Q^{\circ} = \{x^2 \mid x \in GF(11)\}$, $N = \Omega \setminus Q^{\circ}$, $Q^{\circ}-j = \{q-j \mid q \in Q^{\circ}\}$, $N-j = \{n-j \mid n \in N\}$. Dopo di ciò, prova che C ha dimensione 6 su $GF(3)$, e che il gruppo delle invarianze di C è il ricoprimento $C_2 \cdot M_{12}$.

L'analisi della geometria di $S(5,8,24)$, nel solco di Todd (1966), conduce poi Conway alla descrizione delle proprieta strutturali di M_{12} e M_{24}, e in particolare dei sottogruppi massimali di M_{24}, di cui tratteremo in §7.

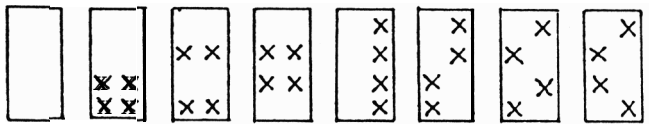
3) Curtis (1976) ha descritto un efficace ed elegante approccio alla struttura di M_{24}, basato sull'analisi di Todd e sull'uso sistematico di un ingegnoso schema combinatorio, il cosiddetto MOG (Miracle Octad Generator):

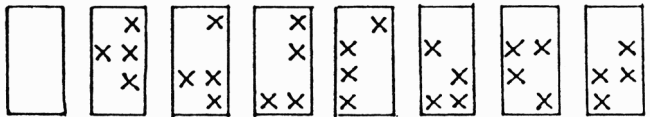
i) Punto di partenza di Curtis è una costruzione del codice binario esteso di Golay (interpretato come sottospazio di 2^{Ω}) che coincide essenzialmente con la costruzione descritta in §5, B), 1).

Si consideri un insieme Λ di cardinalità 8. e lo si visualizzi nel modo seguente:

Λ = 

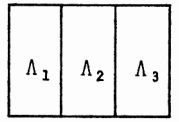
Nello spazio vettoriale 2^{Λ} si scelgano due sottospazi P,L di dimensione 3, con $P \cap L = \{\emptyset\}$, costituiti ciascuno da $\emptyset$ e da 7 tetradi: e.g.

P = 

L = 

Qualunque sia la scelta di P e di L, per ogni $X \in P \setminus \{\emptyset\}$, e per ogni $t \in L \setminus \{\emptyset\}$, si ha $|X+t| = 2.4$, o 6. Ne segue che ogni elemento del sottospazio di 2^{Λ}, costituito dai sottoinsiemi di Λ di cardinalità pari, si può scrivere in uno e un solo modo nella forma $X+t$, oppure $X'+t$, ove $X+X' = \Lambda$, $X \in P$, $t \in L$.

Se si considera Ω come l'insieme costituito da tre copie di Λ (tre "mattoni", nella terminologia di Curtis) Λ_1, Λ_2, Λ_3:

Ω = 

,

C è il sottospazio di 2^{Ω} costituito dai sottoinsiemi di Ω della forma:

$[(X\ 0\ X')+t \mid (Y\ 0\ Y')+t \mid (Z\ 0\ Z')+t]$, ove $X+Y+Z=\emptyset$.
in Λ_1 in Λ_2 in Λ_3

Si riconosce subito che $|C| = 2^7 \cdot 2^4 \cdot 2 = 2^{12}$, e l'analisi delle cardinalità degli elementi di C mostra che C non contiene elementi $\neq \emptyset$ di cardinalità < 8, e contiene esattamente 759 ottadi: pertanto le ottadi di C formano un sistema di Steiner S(5,8,24).

La costruzione di Curtis conduce a una descrizione suggestiva delle ottadi. Precisamente, le ottadi di C sono: i) Λ_1, Λ_2, Λ_3; ii) 84 ottadi del tipo $[X\ 0\ X' \mid X\ 0\ X' \mid \emptyset]$, con $X \neq \emptyset$; iii) 168 ottadi del tipo $[(X\ o\ X') + t \mid (X\ o\ X') + t \mid t]$, con $t \neq \emptyset$, e $|(X\ o\ X') + t| = 2$; iv) 504 ottadi del tipo $[(X\ o\ X') + t \mid (Y\ o\ Y') + t \mid (Z\ o\ Z') + t]$, con $|(X\ o\ X')+t| = 4$, e $|(Y\ o\ Y') + t| = |(Z\ o\ Z') + t| = 2$. Ne discende che:

a) ogni *ottade distinta da* $\Lambda_1, \Lambda_2, \Lambda_3$ *interseca almeno* u n

mattone in una tetrade. (Un tale mattone si dice pesante).
Si consideri poi un mattone, ad es. Al : Λ_1 contiene 70 tetradi, distribuite in 35 coppie di tetradi complementari; ogni tetrade determina un sestetto, costituito dalla tetrade stessa, dalla sua complementare in Al. e da 4 tetradi nel quadrato complementare $\Lambda_2 + \Lambda_3$. Orbene, si riconosce che le 4 tetradi in $\Lambda_2 + \Lambda_3$ hanno la seguente proprietà:

b) una *tetrade interseca le righe di* $\Lambda_2 + \Lambda_3$ *secondo* una *stessa parità*, e *interseca le colonne di* $\Lambda_3 + \Lambda_3$ *secondo* una *stessa parità* (vi sono $35 \cdot 4 = 140$ tetradi cosiffatte).

ii) Il MOG è una tavola composta da 36 figure (cfr. Fig.1). Una figura (la prima a sinistra nella seconda riga) riproduce un ordinamento di $\Omega = \{\infty, 0, 1, \ldots, 22\}$, identificando la posizione dei punti di Ω in $\Lambda_1 + \Lambda_2 + \Lambda_3$, e le ottadi Al, Λ_2, Λ_3. Ciascuna delle restanti 35 figure rappresenta un mattone isolato, diviso in una delle 35 coppie di tetradi complementari, e accanto ad esso la partizione del quadrato complementare nelle 4 tetradi atte a completare un sestetto. Ad esempio, la prima figura in alto a sinistra corrisponde al sestetto $\{\infty, 14, 20, 18\}$, $\{0, 8, 3, 15\}$, $\{17, 13, 5, 21\}$, $\{4, 11, 12, 6\}$, $\{16, 2, 1, 19\}$, $\{10, 7, 22, 9\}$. Se ora pero si conviene di poter scegliere come mattone isolato una qualsiasi delle' ottadi Λ_1, Λ_2, Λ_3, e come quadrato complementare le altre due in qualsiasi ordine, si nota che, in forza della proprietà a), *ogni ottade di c, distinta da* $\Lambda_1, \Lambda_2, \Lambda_3$, *si ottiene come unione di due tetradi in una delle* 35 *figure del* MOG. Ciò rende il

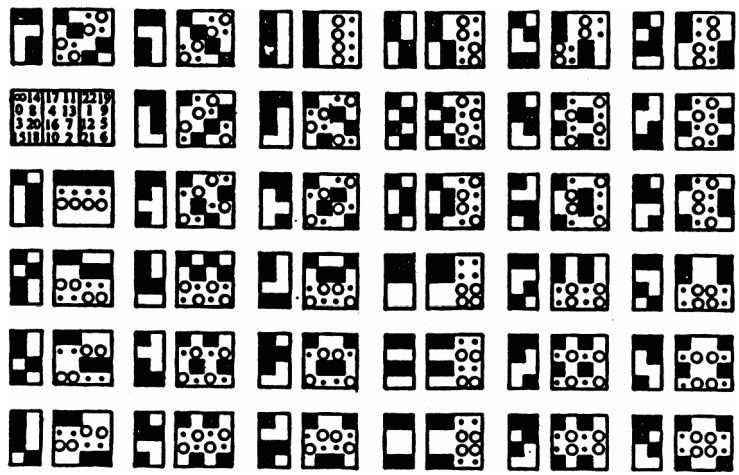


Fig. 1 (da Curtis (1976))

MOG particolarmente adatto a controllare e manipolare gli elementi di C. in modo da ottenere informazioni sugli elementi e sulla struttura di M_{24}.

Rimandando a Curtis (1976) per una descrizione dettagliata del MOG. e per molteplici esempi delle sue applicazioni, notiamo qui che *mediante il* MOG *si può:*

(1) *riconoscere* (immediatamente) *un'ottade di* C;

(2) *identificare* (con relativa facilità, se necessario usando la proprietà b)) *l'ottade contenente* 5 punti *assegnati* di Ω (e *altri elementi* di C *soddisfacenti date* condizioni);

(Si noti che (1) e (2) si traducono, in termini di teoria dei codici, nell'asserzione: *il* MOG è un *sistema di decodifica del codice binario ebtebo di Golay*. Un algoritmo di decodifica basato sul MOG è descritto in Gibson. Blake (1978). Un altro notevole algoritmo di decodifica di C, non basato sul MOG. si deve a Goethals (1971). Cfr. anche Fumy (1981) e l'annessa bibliografia).

(3) *completare tetradi e sestetti;*

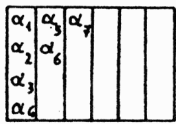
(4) *produrre e rappresentare esplicitamente nel rettangolo* $\Lambda_1 + \Lambda_2 + \Lambda_3$ *uahi elementi di* M_{24}, *corrispondenti a forme cicliche particolari.*

(E.g., usando il MOC Curtis è in grado di provare che M_{24} contiene esattamente due classi di coniugio di involuzioni, aventi rispettivamente le forme cicliche $1^8 2^8$ e 2^{12}.)

(5) *descrivere vari sottogruppi, e in particolare i sottogruppi massimali di* M_{24} (Curtis (1976.1977); cfr. §7).

Usando (3), Curtis (1976) prova l'unicità del sistema di Steiner S(5,8,24) nel modo seguente:

Si fissi un'esade speciale $\{\alpha_1, \alpha_2, \ldots, \alpha_6\}$ contenuta in un'ottade 0, si consideri un punto $\alpha_7 \notin 0$, *e si* supponga che le colonne della figura



costituiscono un sestetto (così

che 0 è formata dalle prime due colonne). Risulta possibile, effettuando opportune manipolazioni e eventualmente cambiando nome ai punti di Ω, ottenere tutti i 35 sestetti associati alle 35 partizioni di 0 in tetradi complementari, esattamente nella forma in cui sono rappresentati dalle figure del MOG. Poiché, d'altra parte, dalle ottadi che intersecano 0 in tetradi è possibile ottenere per differenze simmetriche tutte le ottadi di S(5,8,24), si deduce che, a meno di un riordinamento dei punti di Ω, l'unico S(5,8,24) è quello rappresentato dal MOG. In realtà, le argomentazioni di Curtis, volte a dimostrare l'unicità di S(5,8,24), provano anche che: i) $M_{24} = \mathrm{Aut}(S(5,8,24))$ è sottilmente transitivo sugli insiemi ordinati del tipo $\{\alpha_1, \alpha_2, \ldots, \alpha_6 \mid \alpha_7\}$. Ciò implica che: ii) M_{24} è S-transitivo su Ω, e ha ordine $24\cdot23\cdot22\cdot21\cdot20\cdot3\cdot16$; iii) M_{24} è transitivo sulle esadi speciali ordinate.

4) Una costruzione di S(5,8,24) che, pur risultando meno efficace del MOG, permette anch'essa di computare un'ottade contenente 5 punti assegnati, e in linea di principio di manipolare elementi e derivare informazioni sulla struttura di M_{24}, si deve a D.R.Mason (1977). La costruzione di Mason, che delineiamo qui in modo sommario, si può considerare una variazione sul tema di Todd (1959):

Si considerino i punti di S(5,8,24) come vettori dello spazio $V = GF(2^{11}) \oplus \langle v_\infty \rangle$, pensato come spazio vettoriale di dimensione 12 su GF(2). Precisamente, si ponga $\Omega = \{v_i, (0 \le i \le 22); v_\infty\}$, ove $v_i = \alpha^i + v_\infty$, e α è un elemento di ordine 23 di $GF(2^{11}) \setminus \{0\}$,

che si può assumere sia radice del polinomio irriducibile $x^{11}+x^9+x^7+x^6+x^5+x+1$ e $GF(2)[x]$. In particolare, $\{v_0,\ldots,v_{10}, v_\infty\}$ è una base per V, e quindi, per ogni $i = 11,\ldots,22$, è univocamente determinato (e facilmente computabile) il sottoinsieme X_i di $X = \{0,1,\ldots,10,\infty\}$, tale che sia $v_i = \Sigma_{x\in X_i} v_x$. Si può disegnare un dodecaedro, in modo tale che. per ciascun i, il complemento $X \setminus X_i$ si possa interpretare come l'insieme delle facce adiacenti a una certa faccia f_i del dodecaedro. Ne segue che il gruppo $M = \{g\in GL(V) \mid \Omega^g = \Omega\}$ contiene il gruppo delle simmetrie del dodecaedro, e ciò, insieme al fatto che M contiene il gruppo delle applicazioni semilineari di $GF(2^{11})$: $x \to (x\alpha_i)^\sigma$, ove σ e $Aut(GF(2^{11}))$ (un gruppo di Frobenius di ordine $23 \cdot 11$), implica che M i? 5-transitivo su Ω. La 5-transitività di M permette infine di dedurre che i sottoinsiemi Y di Ω, con $|Y|=8$ e $\Sigma_{y\in Y} y=0$ (cfr. Todd (1959) formano un sistema di Steiner $S = S(5,8,24)$, con $Aut(S) = M$. Le ottadi di S possono essere manipolate usando come congegno combinatorio il dodecaedro.

5) 1 sestetti e i trii associati a $S(5,8,24)$ sono legati alle nozioni di *parallelismo*, e di *risoluzione* di un disegno:

a) Sia $\Omega^{(m)}$ l'insieme dei sottoinsiemi di cardinalità m di un insieme Ω di cardinalità $n < \infty$. Una partizione di $\Omega^{(m)}$ in sottoinsiemi. tali che ognuno di essi costituisca una partizione di Ω, si dice *parallelismo* di $\Omega^{(m)}$. Condizione ovviamente necessaria (ma anche sufficiente!, Baranyai (1973) affinché $\Omega^{(m)}$ ammetta un parallelismo, è che m divida n. Gli elementi

di un parallelismo si dicono classi parallele, e sono in numero di $\binom{n-1}{m-1}$; se $b_1, b_2 \in \Omega^{(m)}$ stanno nella stessa classe parallela, si dice che sono paralleli, e si scrive $b_1 \| b_2$. Si dice che un parallelismo di $\Omega^{(m)}$ *ha la proprietà del parallelogramma* se, per ogni $b_1, b_2, b_3 \in \Omega^{(m)}$, $b_1 \| b_2$, $b_1 \neq b_2$ e $b_3 \subseteq b_1 \cup b_2$ implicano $b_3 \| (b_1 \cup b_2) \setminus b_3$. Infine, il gruppo degli automorfismi di un parallelismo di $\Omega^{(m)}$ è per definizione il gruppo delle permutazioni su Ω che mandano classi parallele in classi parallele.

Se Ω è l'insieme dei punti di S(5,8,24), si vede subito che i 1771 sestetti sono le classi parallele d-i un parallelismo di $\Omega^{(4)}$ che soddisfa la proprietà del parallelogramma e il cui gruppo di automorfismi è M_{24}. L'usuale parallelismo fra rette nello spazio affine AG(d,2) è anch'esso un parallelismo con la proprietà del parallelogramma, e il suo gruppo di automorfismi è il gruppo affine AGL(d,2).

Cameron (1974) ha dimostrato che i precedenti sono i soli esempi non banali di parallelismi con la proprietà del parallelogramma. Precisamente, vale il seguente:

TEOREMA. $\Omega^{(m)}$ ammette un parallelismo con la proprietà del parallelogramma solo nei casi seguenti:

i) m = 1, m = n/2, m = n (casi banali);

ii) m = 4. n = 24. e il parallelismo è quello costituito dai sestetti associati a S(5,8,24);

iii) $m = 2$. $n = 2^d$, Ω è l'insieme dei punti di $AG(d,2)$, e il parallelismo è l'usuale parallelismo fra rette.

(Questo risultato è conseguenza del Teorema 1,§4,E). Infatti, posto $S = (\Omega, B)$, ove B è la collezione dei sottoinsiemi di Ω che sono unione di due elementi paralleli di $\Omega^{(m)}$, si vede facilmente che la proprietà del parallelogramma implica che S è un sistema di Steiner di parametri $m+1, 2m, n$. D'altra parte, se $b_1 \cup b_2$ e $b_1 \cup b_3$ sono blocchi di S, con $b_1, b_2, b_3 \in \Omega^{(m)}$, $b_2 \neq b_3$, anche $b_2 \cup b_3 = (b_1 \cup b_2) \triangle (b_1 \cup b_3)$ è un blocco di S. Dunque S gode della proprietà (A). e quindi $S = S(5,8,24)$, oppure $S = AG_2(d,2)$. Ne seguono ii) e iii), rispettivamente.)

b) Un sistema di Steiner $S(t,m,n) = (\Omega, B)$ si dice *risolubile* se esiste una partizione di B : $B = \bigcup_j B_j$, tale che per ogni j (Ω, B_j) sia un sistema di Steiner $S(1,m,n)$, i.e. una partizione di Ω. Una tale partizione di B si dice *risoluzione* di $S(t,m,n)$. (La prima questione di risolubilità che appare nella letteratura è il celebre problema delle 15 "schoolgirls", -proposto e risolto da Kirkman (1847,1850), che corrisponde all'esistenza di una risoluzione di $S(2,3,15)$. Il problema "generale" di Kirkman è stato risolto da Ray-Chauduri,Wilson (1971), i quali hanno provato che un sistema $S(2.3.n)$ è risolubile sse $n \equiv 3(6)$.) Il concetto di risoluzione generalizza quello di parallelismo: un parallelismo non è altro infatti, che una risoluzione del sistema di Steiner banale $S(m,m,n)$. Si estende alle risoluzioni la nomenclatura introdotta per i parallelismi: gli elementi B_j di una risoluzione si dicono *classi parallele*, e se due

blocchi b', b'' appartengono alla stessa classe B_j, si dice che sono paralleli e si scrive $b' \| b''$; si dice poi che una risoluzione $B = \cup_j B_j$ ha la *proprietà del parallelogramma* se, per ogni b_1, b_2, b_3 e B, $b_1 \| b_2$, $b_1 \neq b_2$ e $b_3 \subseteq b_1 \cup b_2$ implicano $b_3 \| (b_1 \cup b_2) \setminus b_3$. Si noti che affinché $S(t,m,n)$ sia risolubile, m deve dividere n, e che il numero delle classi parallele di una risoluzione è $\binom{n-1}{t-1}/\binom{m-1}{t-1}$. Infine, il gruppo degli automorfismi di una risoluzione è il gruppo delle permutazioni su Ω che mandano classi parallele in classi parallele.

Si considerino ora i sistemi $S(5,6,12)$ e $S(5,8,24)$:

i) Le 66 coppie di esadi complementari formano evidentemente l'unica possibile risoluzione di $S(5,6,12)$, che ovviamente soddisfa la proprieta del parallelogramma.

ii) Una risoluzione di $S(5,8,24)$ è necessariamente costituita da una partizione delle 759 ottadi in 253 trii. Benché già Todd (1966) accenni all'esistenza di una tale partizione, in relazione all'interpretazione geometrica dei sottogruppi di M_{24} isomorfi a $PSL(2,23)$, la risolubilità di $S(5,8,24)$ è esplicitamente esaminata per la prima volta da Kramer, Magliveras, Mesner (1980). i quali peraltro provano molto di più, e cioé che:

1) $S(5,8,24)$ ammette 13 risoluzioni mutuamente disgiunte (i.e. senza trii in comune), ciascuna delle quali ha un gruppo di automorfismi contenente C_{23};

2) $S(5,8,24)$ ammette 9 risoluzioni mutuamente disgiunte e non isomorfe, delle quali 6 hanno come gruppo di automorfismi

il gruppo affine $\langle a : x \to x+1, h : x \to 2x \pmod{23} \rangle$, e 3 hanno come gruppo di automorfismi il gruppo $\langle a,h,c : x \to -x^{-1} \pmod{23} \rangle \cong PSL(2,23)$. In due di queste ultime risoluzioni, lo stabilizzante di un trio è isomorfo a S_4, mentre nella terza è isomorfo a D_{12}.

In particolare, 2) conferma l'osservazione di Todd (1966). offrendo una soddisfacente interpretazione, nei termini della geometria di S(5,8,24), della classe di sottogruppi massimali di M_{24} isomorfi a PSL(2,23)(cfr.§7).

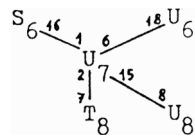
6). (L'azione di M_{24} sui sottoinsiemi di Ω)

L'azione di M_{24} su Ω = PG(1.23) induce in modo ovvio un'azione sull'insieme potenza 2^{Ω}. L'azione di M_{24} su 2^{Ω} è stata analizzata da Todd, il quale ha provato in particolare che M_{24} ha 49 orbite su 2^{Ω}. Conway (1971) presenta un modo semplice e suggestivo di determinare e descrivere queste 49 orbite, ponendo in relazione i sottoinsiemi di Ω di cardinalità r (r-*adi*) con le ottadi e le dodecadi contenute in C. A tale scopo, dopo avere osservato che, per la 5-transività di M_{24} su Ω, ci si può ridurre ad esaminare le orbite sulle r-adi quando $6 \leq r \leq 12$, conviene introdurre la seguente nomenclatura:

i) una r-ade si dice *speciale* (S_r) se contiene 0 è contenuta in un'ottade di C;

ii) una r-ade non speciale si dice *umbrale* (U_r) se è contenuta in una dodecade di C, *trasversale* (T_r) in caso contrario. (In base a queste definizioni, le ottadi e le dodecadi di

C, sono rispettivamente, ottadi speciali e dodecadi umbrali. Tuttavia l'aggettivo speciale, risp. umbrale, è stato nelle sezioni precedenti, e sarà nel seguito, generalmente sottinteso. Infine, la definizione di esade speciale è coerente con la terminologia usata in 1).) Nel caso delle dodecadi non umbrali, conviene raffinare la nomenclatura: una dodecade non umbralr può contenere i) una sola ottade di C. e in tal caso si dirà tout-court *speciale* (S_{12}); ii) tre ottadi di C, e in tal caso si dirà *extraspeciale* (S^+_{12}); iii) tutti 1 punti di una dodecade umbrale tranne uno, e in tal caso si dirà *penumbrale* (U_{12}); in tutti gli altri casi si dirà che la dodecade è *trasversale* (T_{12}). Ciò posto, si hanno per r=6 due orbite $\{S_6\}$. $\{U_6\}$; per r = 7 due orbite: $\{S_7\}$, $\{U_7\}$; per r=8 tre orbite: $\{S_8\}$, $\{U_8\}$, $\{T_8\}$; per r=9 tre orbite: $\{S_9\}$, $\{U_9\}$, $\{T_9\}$; per r = 10 tre orbitr: $\{S_{10}\}$, $\{U_{10}\}$, $\{T_{10}\}$; per r=11 tre orbite: $\{S_{11}\}$, $\{U_{11}\}$, $\{T_{11}\}$; per r = 12 cinque orbite: $\{S^+_{12}\}$, $\{S_{12}\}$, $\{U_{12}\}$, $\{U^-_{12}\}$, $\{T_{12}\}$. Conway (1971) (ma cfr. anche Choi (1967)) dà una rappresentazione diagrammatica delle orbite di M_{24} su 2^Ω, designando ogni orbita con un nodo, e congiungendo i nodi mediante spigoli che contrassegnano il numero dei modi in cui una r-ade di un'orbita si può mutare in una (r-1)-ade o in una (r+1)-ade di una certa altra orbita, rimuovendone un punto o aggiungendovi un punto del complemento. E.g., se si considera una 7-ade umbrale U_7, nel diagramma si ha la

Configurazione: 

, a significare che

i) vi è un punto di U_7 rimuovendo il quale si ottiene un'esade speciale S_6, mentre la rimozione di uno qualsiasi degli altri punti produce un'esade umbrale U_6; ii) in $\Omega \setminus U_7$ vi sono 15 punti ciascuno dei quali, aggiunto a U_7, dà un'ottade umbrale "8" e 2 punti che danno invece un'ottade trasversale T_8.

Una descrizione alternativa, in termini di "vettori di frequenza", della partizione di 2^Ω in orbite di M_{24} (e delle analoghe partizioni per i gruppi M_{23} e M_{22}), è data da Kramer, Magliveras. Mesner (1981):

Sia Γ un'orbita di M_{24} su 2^Ω, e sia $X \in 2^\Omega$, di cardinalità r. Il vettore di frequenza di X rispetto a Γ è il vettore $\underline{e}_{X,\Gamma} = (e_0, e_1, \ldots, e_r)$, ove $e_i = |\{Y \in \Gamma \mid |X \cap Y| = i\}|$, $0 \leq i \leq r$. Si noti che: i) se Δ è l'orbita di M_{24} che contiene X, per ogni $X' \in \Delta$ si ha $\underline{e}_{X,\Gamma} = \underline{e}_{X',\Gamma}$; ii) per la transitività di M_{24} su Ω, $\Sigma i \cdot e_i = |X| \cdot \lambda$, ove λ è il numero degli elementi di Γ contenenti un assegnato punto di Ω, e ciò implica che, se $|X| \neq |X'|$, $\underline{e}_{X,\Gamma} \neq \underline{e}_{X',\Gamma}$. In forza di i) e ii), se a orbite distinte di sottoinsiemi della stessa cardinalità corrispondono vettori di frequenza distinti, le orbite di M_{24} su 2^Ω sono completamente caratterizzate dai loro vettori di frequenza. Ciò accade se si sceglie come orbita di riferimento Γ l'orbita costituita dalle 759 ottadi di S(5,8,24): è allora possibile, con metodi esclusivamente computazionali, dare una rappresentazione diagrammatica delle orbite di M_{24} su 2^Ω (isomorfa a quella di Conway), indicinta dai vettori di frequenza. Dopo di ciò, è possibile stabilire una procedura per determinare, a partire dai vettori

di frequenza di M_{24}, la partizione di $2^{\Omega\setminus\{\infty\}}$ in orbite di $(M_{24})_\infty \simeq M_{23}$, e la partizione di $2^{\Omega\setminus\{\infty,0\}}$ in orbite di $(M_{24})_{\infty,0} \simeq M_{22}$ assumendo come orbita di riferimento per M_{23}, l'orbita costituita dai 253 blocchi della contrazione di S(5,8,24) in ∞, e come orbita di riferimento per M_{22} quella costituita dai blocchi del sistema precedente che non contengono 0. (In particolare, Kramer, Magliveras. Mesner (1981) tabulano un elenco completo di rappresentanti delle orbite di M_{24}, $(M_{24})_\infty$, $(M_{24})_{\infty,0}$ su 2^Ω, $2^{\Omega\setminus\{\infty\}}$, $2^{\Omega\setminus\{\infty,0\}}$, rispettivamente.)

L'informazione così raccolta sulle orbite di M_i (i=24,23,22) è utilizzata in Kramer, Magliveras, Mesner (1981) per determinare tutte le possibili quaterne di parametri t,m,n,λ, con $1< t< m \leq n/2$, per le quali esiste un t-(n,m,λ) disegno che ammette M_i come gruppo di automorfismi. Un t-disegno (Ψ,B) è però da intendersi qui in un'accezione più vasta, rispetto alla definizione datane in §3, poiché B è in generale una famiglia di sottoinsiemi (di cardinalità m) estratti da Y (i.e. vi possono essere blocchi ripetuti). Un t-disegno secondo la definizione di §3 si dice, in questo contesto, *semplice*. Adottando metodi introdotti da Kramer,Mesner (1976). Kramer, Magliveras. Mesner (1981) determinano molti nuovi t-disegni, e in particolare dei t-disegni non-semplici fino a t=ll. E.g.: l'unione di 6 copie di $\{S_{12}^+\}$, una copia di $\{T_{12}\}$, e 6 copie di $\{U_{12}\}$, è la famiglia dei blocchi di un 11-(24,12,6) disegno non-semplice, che ha M_{24} come gruppo di automorfismi.

(Cogliamo qui l'occasione di segnalare che recentemente S.S. Magliveras e D.W. Leavitt hanno provato che esistono o-disegni

semplici non banali. Essi hanno considerato il gruppo $P\Gamma L(2,2^5)$, 4-omogeneo sulla retta projettiva $PG(1,2^5)$, e hanno prodotto sei 6-(33,8,36) disegni semplici, non banali, a due a due non isomorfi (Magliveras. Leavitt (1982)). Successivamente, Kramer, Leavitt, Magliveras (1984) hanno anche prodotto due 6-(20,9,12) disegni semplici non isomorfi, aventi come gruppo di automorfismi il gruppo 3-omogeneo PSL(2,19) (essendo 20=19+1 il minimo valore di v=q+1 per il quale PSL(2,q) ammetta 6-disegni semplici) .)

ADDENDA:

1) Un congegno combinatorio che svolge per M_{12} un ruolo analogo a quello del MOG per M_{24}, ideato da J.H.Conway e R.T.Curtis, è descritto in Curtis (1982). Il congegno si chiama "Kitten", e può essere utilizzato per determinare l'esade di S(5,6,12) che contiene 5 punti assegnati, per produrre elementi di M_{12}, e per descrivere alcuni sottogruppi massimali. Il MOG e i suoi usi sono ulteriormente indagati in Conway (1982). Vi si descrive anche il cosiddetto MINIMOG (tabella 4 x 3 derivabile dal Kitten). Al MOG e al MINIMOG sono rispettivamente associati un codice di lunghezza 6 su GF(4) (l'"esacodice", atto a condurre calcoli nel codice binario esteso di Golay), e un codice di lunghezza 4 su GF(3) (il "tetracodice", atto a condurre calcoli nel codice ternario esteso di Golay).

2) Una nuova costruzione combinatoria di S(5,8,24), basata su una soggiacente "geometria affine", è presentata in Kadir,

Key (1984). Punto di partenza è la configurazione che si ottiene da PG(2,4) sopprimendo un punto e le rette ad esso incidenti: tale configurazione è un 1-(20,5,4) disegno, duale del piano affine AG(2,4). Sfruttando "a priori" le proprietà note di M_{24} e S(5,8,24), è possibile associare in modo univoco a un arbitrario piano affine duale Al, altri tre piani duali A_2, A_3, A_4, in modo che sull'insieme Ω costituito dai 20 punti di A_1 e dai 4 "nuovi" punti A_i $(1 \leq i < 4)$, si formi in modo naturale un sistema S(5,8,24). La costruzione permette poi un'analisi parziale di M_{24}.

§7. 1 SOTTOGRUPPI MASSIMALI DEI GRUPPI DI MATHIEU

La determinazione dei sottogruppi massimal i dei gruppi di Mathieu si deve essenzialmente alla scuola di D. Livingstone. 1 sottogruppi massimali di M_{24} sono stati determinati da Choi (1967). 1 sottogruppi massimali degli altri gruppi di Mathieu possono ricavarsi allora, considerandoli come sottogruppi di M_{24}.

Il primo decisivo contributo alla descrizione dei sottogruppi massimali di M_{24} si deve, ancora una volta, a Todd. Come si è accennato in §6, Todd (1966) elenca 8 classi di coniugio di sottogruppi massimali d i M_{24}. Di queste classi, 7 sono descritte in modo naturale mediante la geometria di S(5,8,24); la classe rimanente è costituita da sottogruppi isomorfi a PSL(2,23), con l'azione naturale su Ω = PG(1,23). (Un'interpretazione geometrica di PSL(2,23), mediante una risoluzione di S(5,8,24), è stata pero data da Kramer. Magliveras. Mesner (1980); cfr. §6,5)). Sfugge all'analisi di Todd una sola classe di sottogruppi massimali, isomorfi a PSL(2,7), la cui locazione in M_{24} è, come si vedrà, più riposta.

In Choi (1972A,1972B) le 9 classi di sottogruppi massimali di M_{24} sono determinate utilizzando una meticolosa analisi delle orbite di M_{24} nella sua azione sui sottoinsiemi di Ω. Choi (1972A) descrive gli stabilizzanti in M_{24} dei sottoinsiemi di Ω, e determina i sottogruppi di M_{24} che sono massimali fra i sottogruppi intransitivi: vi sono 9 classi di tali sottogruppi, 4 delle quali danno sottogruppi massimali di M_{24}. Choi

(19728) completa la descrizione dei sottogruppi massima1 i transitivi su Ω : vi sono una classe di sottogruppi primitivi, e 4 classi di sottogruppi imprimitivi su Ω.

1) Sottogruppi massimali intransitivi su Ω:

La laboriosa analisi di Choi risulta drasticamente semplificata se si osserva che ogni sottoinsieme X di Ω di cardinalità r (r-*ade*), o appartiene al sottospazio C di 2^{Ω} generato dalle ottadi di S(5.8.24) (cfr.§6), oppure è congruo modulo C a un'unica 1-ade (*monade*), o a un'unica 2-ade (*diade*), o a un'unica 3-ade (*triade*), o alle 4 *tetradi* di un unico sestetto (Conway (1971)). (Ciò è conseguenza del fatto che, se ad un sottoinsieme X di Ω, con $|X| \geq 5$, si somma un'ottade di C contenente 5 punti di X, si ottiene un sottoinsieme di cardinalità minore di $|X|$, congruo a X modulo C.)

Dall'osservazione precedente segue subito, infatti, che un sottogruppo intransitivo di M_{24} è contenuto in uno dei seguenti sottogruppi:

i) lo stabilizzante di una monade;
ii) lo stabilizzante di una diade;
iii) lo stabilizzante di una triade;
iv) lo stabilizzante di un sestetto (cfr. 3));
v) lo stabilizzante di un'ottade di C;
vi) lo stabilizzante di una dodecade di C (cfr. 3)).

Se ne deduce che vi sono esattamente 4 classi di sottogruppi massimali di M_{24}, intransitivi su Ω, isomorfi rispettivamente a :

a) M_{23}, lo stabilizzante di una monade;

b) $\mathrm{Aut}(M_{22}) = [M_{22}]C_2$, lo stabilizzante di una diade;

c) $P\Gamma L(3,4) = [M_{21}]S_3$, lo stabilizzante di una triade;

d) $AGL(4,2) \simeq \mathrm{Hol}(E_{24})$, lo stabilizzante di un'ottade.

Riguardo a d): Sia H lo stabilizzante di un'ottade 0 in M_{24}. Il sottogruppo K di M_{24}, costituito dagli elementi che fissano i punti di 0, è abeliano elementare di ordine 2^4, e opera come un gruppo regolare su $\Omega \setminus 0$ (Witt (1938A)). La transitività di M_{24} sulle ottadi di S(5,8,24) implica allora che H induce su 0 il gruppo alterno Ag, e $H = [K] \cdot A_8$. D'altra parte, sia $\gamma \in \Omega \setminus 0$. $H_\gamma = Ag$ opera per coniugio come un gruppo di automorfismi su $K \setminus \langle 1 \rangle$, e in modo equivalente opera su $\Omega \setminus (0 \cup \{\gamma\})$: in entrambe le azioni, H_γ opera come il gruppo generale lineare GL(4,2). In particolare, si conclude che H opera su $\Omega \setminus 0$ come il gruppo affine AGL(4,2), ed è quindi isomorfo all'olomorfo di un gruppo abeliano elementare E_{24}. (Si noti anche l'isomorfismo "eccezionale" $Ag \simeq GL(4,2)$.)

(Da d) segue in particolare che un 2-sottogruppo di Sylow di M_{24} è isomorfo a un L-sottogruppo di Sylow di GL(5,2). Una ricognizione diretta consente allora di riconoscere che un 2-sottogruppo di Sylow di M_{24} contiene esattamente due sottogruppi abeliani elementari di ordine 26, che saranno qui e nel seguito denotati con E_{26} e E'_{26}, aventi rispettivamente su Ω 3 orbite di lunghezza 8 (le ottadi di un trio) e 6 orbite di lunghezza 4 (le tetradi di un sestetto)).

2) Sottogruppi massimali primitivi su Ω:

M_{24} contiene una sola classe di sottogruppi propri, primitivi su Ω (che pertanto sono massimali in M_{24}). Tali sottogruppi sono isomorfi a PSL(2,23), e sono coniugati al sottogruppo $\langle x \to x+1, x \to -x^{-1} \pmod{23} \rangle$ con l'azione naturale su $\Omega = PG(1,23)$. Sono dunque sottogruppi 2-transitivi (e 3-omogenei) su Ω.

3) Sottogruppi massimali imprimitivi su Ω:

Vi sono 4 classi di sottogruppi massimali di M_{24}, imprimitivi su Ω, con blocchi d'imprimitività di lunghezza 12,8,4,3. Esse sono rispettivamente rappresentate dai seguenti sottogruppi:

a) G_1, *Lo stabilizzante* in M_{24} *di* un *duo* $\{\Delta,\Delta'\}$ di dodecadi complementari. $(M_{24})_\Delta = (M_{24})_{\Delta'} \simeq M_{12}$, e $G_1 = N_{M_{24}}((M_{24})_\Delta)$ è isomorfo ad $Aut(M_{12}) = [M_{12}]C_2$ (Witt (1938A), cfr.§3; Todd (1966)). Il **sistema** d'imprimitività è il duo, il gruppo indotto ha ordine 2, e il nucleo d'imprimitività è $(M_{24})_\Delta \simeq M_{12}$.

b) G_2, *lo stabilizzante di* un *trio* di ottadi mutuamente disgiunte: $G_2 = N_{M_{24}}(E_{26}) = [E_{26}](PSL(3,2) \times S_3)$. Il sistema di imprimitività è il trio, e il gruppo indotto sul trio è S_3. Il nucleo d'imprimitività è estensione spezzata fedele di E_{26} mediante PSL(3,2).

(Riguardo a G_2: Si osservi che le tetradi di un sestetto danno luogo a 15 trii. Poiché vi sono 1771 sestetti e 3795 trii, e $1771 \cdot 15 = 3795 \cdot 7$, si deduce che ogni trio possiede esattamente 7 "raffinamenti" in sestetti distinti. $E_{26} = O_2([E_{26}]PSL(3,2))$ è il sottogruppo costituito dagli elementi di G_2 che fissano ciascuna ottade del trio e ciascuno dei 7 sestetti che raffinano

il trio. PSL(3,2) è il gruppo indotto da G_2 sui 7 sestetti (modulo C, i sestetti formano un sottospazio 3-dimensionale di $2^{\Omega}/C$, i.e. un piano projettivo di ordine 2, sul quale PSL(3,2) opera in modo naturale). Infine, S_3 fissa i raffinamenti, permutando le ottadi del trio.)

c) G_3, *lostabilizzante.d* i *unsestett*$G_3 = N_{M_{24}}(E'_{26}) = ([E'_{26}]C_3)\cdot S_6$. Il sistema d'imprimitività è il sestetto, e il gruppo indotto da G_3 sulle tetradi del sestetto è S_6. Il nucleo d'imprimitività di G_3 è estensione spezzata fedele di E'_{26} mediante il gruppo ciclico C_3. (E'_{26} contiene 18 involuzioni di tipo 212, le cui trasposizioni si distribuiscono a coppie sulle tetradi del sestetto, e $45 = \binom{6}{2}\cdot 3$ involuzioni di tipo 1828, ciascuna delle quali fissa i punti di due tetradi del sestetto. C_3 è generato da un elemento di tipo 1636, che fissa esattamente un punto in ogni tetrade.)

d) $G_4 \simeq PSL(2,7)$ ($\simeq PSL(3.2)$).

Questa classe di sottogruppi massimali sfugge. come si è detto, a Todd (1966). La sua esistenza fu suggerita da D.Livingstone, e confermata da R.List, che produsse generatori espliciti per un PSL(2,7) massimale in M_{24} (cfr. Choi (1972B), e List(1977)). Precisamente: esistono in M_{24} un'involuzione x di tipo 212, e un elemento y di ordine 3 e tipo 38, per i quali $o(xy) = 7$ e $\langle x,y \rangle \simeq PSL(2,7)$ è massimale in M_{24}. $\langle x,y \rangle$ ha un sistema d'imprimitività su Ω, costituito da 8 blocchi di lunghezza 3, con nucleo d'imprimitività banale:

Un sottogruppo massimale isomorfo a PSL(2,7) ha una locazione piuttosto anomala in M_{24}. Esso è descritto da Conway (1971) come il centralizzante in M_{24} della permutazione s=(12,13,14)(21,7,8)(17,1,20)(2,19,15)(6,3,11)(∞,5,10)(16,0,9)(4,22,8)∈$S_{24}\setminus M_{24}$: gli 8 3-cicli di s formano un sistema d'imprimitività per PSL(2,7), che opera su di essi come sui punti di PG(1,7) (donde il nome di "octern group". i.e. stabilizzante d.i otto terne, dato a G_4). Questa caratterizzazione è pero estrinseca alla geometria di S(5,8,24). Non molto più soddisfacente è Curtis (1976), che descrive l'"octern group" come lo stabilizzante in M_{24} del sottospazio 4-dimensionale di C, costituito da Ø e dalle dodecadi che sono unione di terne. Finalmente Chawathe (1978) offre una spiegazione "intrinseca" dell'esistenza di PSL(2.7) massimali, fondata su una delicata analisi di proprietà riposte di S(5,8,24), già parzialmente osservate da Todd (1966). La descrizione di Chawdthe è, per sommi capi, la seguente:

I sottoinsiemi di Ω di cardinalità 6 (esadi) si suddividono in due orbite per l'azione di M_{24}: una costituita dalle. esadi speciali, l'altra dalle esadi umbrali (cfr.§6). Sia E un'esade umbrale. Ciascun punto α_i e E ($1 \leq i \leq 6$) determina tre punti $\varepsilon_i, \eta_i, \zeta_i$ tali che $(E\setminus\{\alpha_i\}) \cup \{\varepsilon_i, \eta_i, \zeta_i\}$ sia un'ottade di S(5,8,24): si ottiene in tal modo un sestetto $\{(\alpha_i, \varepsilon_i, \eta_i, \zeta_i)\}$, $1 \leq i \leq 6$. Vi sono 64 esadi umbrali che danno luogo allo stesso sestetto, e esattamente 18 di queste sono disgiunte da E. Un insieme di 4 esadi umbrali mutuamente disgiunte si dice *quartetto*: le 18 esadi disgiunte da E si possono suddividere in un unico modo in 6 terne, in modo che ciascuna di esse, insieme con E, dia

luogo a un *quartetto* (Todd (1966)). Una partizione di Ω in 8 terne si dirà un ottetto se i) l'unione di due terne è un'esade umbrale; ii) le 28 esadi così ottenute si possono disporre in 7 quartetti. M_{24} opera sugli ottetti suddividendoli in due orbite aventi rispettivamente lunghezza $2^6 \cdot 3 \cdot 5 \cdot 11 \cdot 23$ e $2^7 \cdot 3^2 \cdot 5 \cdot 11 \cdot 23$. Lo stabilizzante di un ottetto (i.e. il sottogruppo di M_{24} costituito dagli elementi che permutano le terne dell'ottetto) nella prima orbita, è il normalizzante in M_{24} di un elemento di ordine 3 e tipo 38; nella seconda orbita è un sottogruppo massimale, isomorfo a PSL(2,7). E.g., un ottetto della seconda orbita, ove si consideri il sistema S(5,8,24) prodotto da Carmichael (1931) e usato da Todd (1966), è il seguente: {0,1,14}, {∞,21,17}, {4,9,16}, {3,11,22}, {8,5,19}, {2,20,18}, {10,7,13}, {6,12,15}; lo stabilizzante dell'ottetto è il gruppo $\langle x,y \rangle$, ove x = (0,8)(1,5)(3,9)(4,22)(6,18)(7,21)(10, ∞)(11,16))(12,20)(13,17)(14,19)(2,15), e y = (8,5,19)(15,10,2)(9,16,4)(22,∞,0)(1,11,21)(18,6,13)(3,17,14)(20,12,7). L'ottetto è, come si vede, un sistema d'imprimitività per $\langle x,y \rangle \simeq$ PSL(2,7). I 7 quartetti cui l'ottetto dà luogo hanno poi la proprieta seguente: due quartetti distinti determinano, per differenza simmetrica delle loro esadi, le esadi di un unico terzo quartetto. I 7 quartetti sono pertanto interpretabili come i punti di un piano projettivo di ordine 2, e $\langle x,y \rangle$ opera in modo naturale come PSL(3.2) su tale piano projettivo.

Una descrizione dei sottogruppi massimali di M_{24} è contenuta in Conway (1971). In particolare, Conway i) determina i sottogruppi

massimali intransitivi su Ω ; ii) descrive i sottogruppi massimali (con l'eccezione di PSL(2,23) e PSL(2,7)) come stabilizzanti di una configurazione su Ω (una monade e il suo complemento, una diade e il suo complemento, una triade e il suo complemento, un'ottade e il suo complemento, un duo. un trio, un sestetto) ; iii) analizza il grado di transitivita di ciascun gruppo nella 'sua azione simultanea sui singoli elementi della configurazione. L'approccio di Conway consente tuttavia un'analisi solo parziale del caso imprimitivo.

Anche List (1977) riprende la questione della determinazione dei sottogruppi massimali di M_{24}, e presenta una versione molto più concisa di quella di Choi (1972A,1972B), basata sull'uso di metodi più sofisticati di teoria dei gruppi, atti a trattare il caso imprimitivo. In particolare, List prova che un sottogruppo massimale di M_{24} è necessariamente non-risolubile, e può quindi limitare l'analisi ai sottogruppi imprimitivi non-risolubili.

Curtis (1976) descrive invece esplicitamente i nove tipi di sottogruppi massimali di M_{24}, facendo uso delle tecniche combinatorie associate al MOG. Curtis (1977) prova poi che la lista di gruppi ottenuta è completa. La dimostrazione è relativamente concisa, e combina l'uso del MOG con l'analisi dell'azione di M_{24} su 2^{Ω} e con tecniche di teoria dei gruppi di permutazioni. Citiamo in particolare il seguente risultato, che semplifica lo studio dei sottogruppi imprimitivi: Sia H un sottogruppo transitivo di M_{24}, con un sistema di blocchi di lunghezza 1,2,3,4, o 6. Se il gruppo indotto da H è primitivo sui blocchi, è addirittura 2-transitivo sui blocchi.

Ci sembra utile, per esemplificare le tecniche MOG, riprendere qui con qualche variante alcune delle argomentazioni di Curtis (1976), volte a descrivere sottogruppi massimali di M_{24}.

Si considerino ad esempio:

i) *lo stabilizzante di un'ottade* 0.

L'azione di M_{24} sugli insiemi ordinati del tipo $\{\alpha_1, \alpha_2, \ldots, \alpha_6 | \alpha_7\}$, considerati in §6,3), mostra che M_{24} è transitivo sulle ottadi e $H = (M_{24})_{[0]}$ induce un gruppo sottilmente o-transitivo su 0, i.e. il gruppo alterno Ag. Il nucleo dell'azione di H su 0 è dunque un sottogruppo K di ordine 2^4, e non è difficile, scegliendo $0 = \Lambda_1$, esibire nel rettangolo $\Lambda_1 + \Lambda_2 + \Lambda_3$ 15 involuzioni di tipo $1^8 2^8$ appartenenti a K. Si conclude che K è abeliano elementare, e $H = E_{2^4} A_8$.

ii) *lo stabilizzante di un duo* $\{\Delta, \Delta'\}$.

Sia $E = \{\alpha_1, \ldots, \alpha_6\}$ un'esade speciale contenuta in A, e sia $0 = \{\alpha_1, \ldots, \alpha_6, \gamma, \delta\}$ l'ottade contenente E: allora $\Delta = 0 + Q$, ove Q è una delle 16 ottadi che intersecano 0 in $\{\gamma, \delta\}$. Scegliendo ad es. $0 = \Lambda_1$, e $\gamma = \infty$, $\delta = 14$, è facile determinare mediante il MOG le 16 ottadi che intersecano 0 in $\{\gamma, \delta\}$, i.e. le 16 dodecadi che contengono E, e riconoscere che il nucleo K dello stabilizzante di 0 opera transitivamente su di esse. Poiché M_{24} è transitivo sulle esadi speciali (cfr.§6,3)), si conclude che M_{24} è transitivo sulle dodecadi.

In modo simile si prova che lo stabilizzante della dodecade A è S-transitivo sui punti di A. Siano infatti $\beta_1, \ldots, \beta_5$ 5 punti di A, 0' l'ottade che li contiene, $E' = \{\beta_1, \ldots, \beta_5, \beta_6\} \subset 0'$

l'esade speciale da essi determinata in A: allora è $A = O'+Q'$, ed esiste in M_{24} un elemento g tale che sia $(\beta_i)^g = \alpha_i$, $1 \le i \le 6$. Si ha dunque: $A^g = (O'+Q')^g (O')^g + (Q')^g = O + (Q')^g$, con $O \cap (Q')^g = \{\gamma, \delta\}$. ed esiste $k \in K$ tale che sia $\Delta^{gk} = O^k + (Q')^{gk} = O+Q = \Delta$ Ora, $x = gk \in (M_{24})_{[\Delta]}$, e $(\beta_i)^x = \alpha_i$, c.v.d.

$(M_{24})_{[A]}$ è il gruppo di Mathieu M_{12}: la transitività di M_{24} sulle dodecadi implica che a) $|M_{12}| = |M_{24}|/2576 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, i.e. M_{12} è sottilmente 5-transitivo sui punti di A ; b) M_{12} ha indice 2 nella stabilizzante del duo $\{\Delta, \Delta'\}$.

Sia ora $A = K \cdot S_6$ il sottogruppo dello stabilizzante di O, costituito dagli elementi che fissano la coppia $\{\gamma, \delta\}$. Il sottogruppo di A, costituito dagli elementi che fissano Q, è isomorfo a S_6, e opera simultaneamente su $O \setminus \{\gamma, \delta\}$ e su $Q \setminus \{\gamma, \delta\}$. Tuttavia le due azioni non sono equivalenti: infatti, in caso contrario, esisterebbe in M_{24} un elemento $y \neq 1$ che fissa 8 punti di A , i.e. gli 8 punti di un'ottade umbrale; ma allora y fisserebbe i punti di un insieme del tipo $\{\alpha_1, \alpha_2, \ldots, \alpha_6 | \alpha_7\}$, assurdo. Si sono dunque ottenute le due azioni di S_6, scambiate fra loro da un automorfismo esterno, già considerate da Witt (1938A)(cfr.§3). Infine, poiché $A_{[Q]} \simeq S_6$ ha due orbite di lunghezza 6 su A , e un'orbita di lunghezza 2 su A', si riconosce che le azioni di M_{12} su A e A' sono inequivalenti.

iii) Lo *stabilizzante* di *un trio*.

Lo stabilizzante $H = E_{24} \cdot A_8$ di un'ottade O contiene un elemento di ordine 15 e tipo $3.5.1 \cdot 15$, che fissa un punto $\gamma \in \Omega \setminus O$, e permuta transitivamente i punti di $\Omega \setminus (O \cup \{\gamma\})$.

Tale elemento opera perciò sulle 30 ottadi disgiunte da 0, suddividendole in due orbite, una costituita dalle 15 ottadi che contengono γ, l'altra dalle rimanenti. Si conclude che H è transitivo sui 15 trii che contengono 0, e quindi M_{24} è transitivo sui 3795 trii. Si scelga allora il trio costituito dai mattoni Λ_1, Λ_2, Λ_3. Si ha subito che i 7 raffinamenti di questo trio sono i sestetti individuati dalle tetradi dello spazio P, introdotto in §6,3); ed è possibile, mediante il MOG, produrre tre permutazioni (una di tipo $1^6 3^6$, due di tipo $1^8 2^8$) che operano sui sestetti e generano un gruppo isomorfo a PSL(2,7). Poiché i sestetti danno luogo a un sottospazio 3-dimensionale di $2^\Omega/C$, si conclude che il gruppo indotto sui sestetti dallo stabilizzante del trio è $PSL(3,2) \simeq PSL(2,7)$. Le considerazioni precedenti conducono alla struttura $[E_{2^6}](PSL(3,2) \times S_3)$ per lo stabilizzante del trio (S_3 essendo il gruppo delle permutazioni di $\Lambda_1, \Lambda_2, \Lambda_3$ che fissano i sestetti).

iv) La *stabilizzante* di un *sestetto*.

M_{24} è transitivo sui 1771 sestetti: pertanto lo stabilizzante di un sestetto ha ordine $2^6 \cdot 3 \cdot 6!$. Si scelga il sestetto costituito dalle colonne del rettangolo $\Lambda_1 + \Lambda_2 + \Lambda_3$. Per provare che il gruppo indotto sulle tetradi è l'intero S_6, basta osservare che a) la permutazione (3,15)(20,18)(16,10)(7,2)(22,19)(1,9)(12,6)(21,5), suggerita dal MOG, opera come una trasposizione sulle tetradi; b) il sottogruppo di M_{24} costituito dagli elementi che fissano i punti di una tetrade, è transitivo sui punti rimanenti, e quindi lo stabilizzante di un sestetto è L-transitivo

sulle tetradi; c) in forza di a) e b), lo stabilizzante di un sestetto contiene tutte le trasposizioni sulle tetradi. Dopo di ciò, si possono rappresentare esplicitamente nel rettangolo $\Lambda_1 + \Lambda_2 + \Lambda_3$ tutte le involuzioni che fissano i punti di Λ_1 e preservano le altre 4 tetradi del sestetto: sono 45 involuzioni a due a due permutabili, che per ragioni d'ordine generano un sottogruppo di ordine 26. Si è così condotti alla struttura $([E'_{26}]C_3) \cdot S_6$ dello stabilizzante di un sestetto (ove $\cdot C_3$ è generato dalla permutazione (0,3,15)(8,20,18)(4,16,10)(13,7,2)(1,12,21)(9,5,6)).

Come si è detto all'inizio del paragrafo, i sottogruppi massimali degli altri gruppi di Mathieu possono essere determinati e descritti in modo suggestivo, considerandoli come sottogruppi di M_{24}. Noi ci limiteremo qui ad elencare brevemente, per ciascun gruppo, le classi di sottogruppi massimali, indicandone dove è significativa la provenienza dai corrispondenti sottogruppi di M_{24}.

M_{23}: i) l'unica classe di sottogruppi massimali transitivi è costituita dai normalizzanti dei 23-sottogruppi di Sylow, isomorfi al gruppo affine $\langle x \to x+1, x \to 2x \rangle$ di ordine $23 \cdot 11$.

ii) Vi sono 6 classi di sottogruppi intransitivi, rispettivamente isomorfi ai gruppi seguenti:

a) M_{22}, lo stabilizzante di un punto;

b) $[M_{21}]C_2$, lo stabilizzante di una coppia;

c) $[E_{24}]A_7$ (l'unica estensione spezzata fedele di E_{2^4} mediante A_7, sottogruppo di AGL(4,2))

d) $A_8 \simeq GL(4,2)$

(c) e d) provengono entrambi dallo stabilizzante di un'ottade in M_{24}, e hanno due orbite di lunghezza 7 e 16, 8 e 15 rispettivamente);

e) M_{11}, con due orbite di lunghezza 11 e 12 (dallo stabilizzante di un duo in M_{24});

f) $[E'_{2^4}](C_3 \times A_5)C_2$, con un'orbita di lunghezza 3, e 5 blocchi d'imprimitività sui punti rimanenti (dallo stabilizzante di un sestetto in M_{24}).

M_{22}: i) Non contiene sottogruppi propri transitivi.

ii) Ha 8 classi di sottogruppi massimali, rispettivamente isomorfi ai gruppi seguenti:

a) $M_{21} = PSL(3,4)$, lo stabilizzante di un punto;

b) $[ASL(2,4)]C_2$, lo stabilizzante di una coppia di punti, con un'orbita di lunghezza 2 e 5 blocchi d'imprimitività sui punti rimanenti (si può riguardare come estensione spezzata fedele di E'_{2^4} mediante S_5, proveniente dallo stabilizzante di un sestetto in M_{24});

c) $[E_{24}]A_6$ (l'unica estensione spezzata fedele di E_{24} mediante A_6, sottogruppo di AGL(4,2))

d) A_7 (vi sono due classi di A_7, scambiate fra loro da un automorfismo esterno di M_{22})

e) $AGL(3,2) \simeq Hol(E_{23})$, lo stabilizzante di un vettore non

nullo di V(4,2) in GL(4,2).

(I sottogruppi in c),d),e) provengono dallo stabilizzante di un'ottade 0 in M_{24}, quando si fissino rispettivamente due punti di 0, un punto di 0 e uno di $\Omega \setminus 0$, e due punti di $\Omega \setminus 0$. Hanno orbite di lunghezza 6 e 16, 7 e 15, 8 e 14 rispettivamente);

f) PSL(2,11), con due orbite di lunghezza 11;

g) M_{10}, con due orbite di lunghezza 10 e 12, e due blocchi d'imprimitività di lunghezza 6 sulla seconda orbita.

(I sottogruppi in f) e g) provengono dallo stabilizzante di un duo $\{\Delta,\Delta'\}$ in M_{24}, quando si fissino un punto di Δ e uno di Δ', e due punti di Δ, rispettivamente).

M_{12}: Conviene rappresentare M_{12} come lo stabilizzante della dodecade Δ nel duo $\{\Delta,\Delta'\}$. Vi sono 11 classi di sottogruppi massimali in M_{12}:

i) Vi è una classe di sottogruppi isomorfi a PSL(2,11), a-transitivi sia su Δ che su Δ'.

ii) a) Fissando un punto di $\Delta(\Delta')$ si ottiene una classe di sottogruppi isomorfi a M_{11}, 3-transitivi su $A'(A)$.

b) Fissando (come insieme) una coppia di punti di $\Delta(\Delta')$ si ottiene una classe di sottogruppi isomorfi a $Aut(S_6)$ $(= M_{10} \cdot C_2)$, con due orbite di lunghezza 2 e 10 su $\Delta(\Delta')$, e un sistema di due blocchi d'imprimitività di lunghezza 6 su $A'(A)$.

c) Fissando (come insieme) una terna di punti di $A(A')$ si ottiene una classe di sottogruppi isomorfi a $Hol(E_{3^2})$ $(= M_9 \cdot S_3)$, con due orbite di lunghezza 3 e 9 su $\Delta(\Delta')$, e un sistema di 4 blocchi d'imprimitività di lunghezza 3 su $\Delta'(\Delta)$.

Le due classi che si ottengono in ciascuno dei punti a),b),c) sono scambiate fra loro da un automorfismo esterno di M_{12}, realizzato da un'involuzione di M_{24} che scambia fra loro A e Δ'.

d) Fissando (come insieme) una quaterna di punti di $\Delta(\Delta')$ si ottiene la classe dei centralizzanti di un'involuzione centrale in M_{12}, isomorfi all'olomorfo del gruppo dei quaternioni Q_8 $(= M_8 \cdot S_4)$. L'azione su A e A' è la stessa, con due orbite di lunghezza 4 e 8.

iii) Vi sono infine 3 classi di sottogruppi imprimitivi, con la stessa azione su A e A', isomorfi ai gruppi seguenti:

a) $C_2 \times S_5$. E' la classe dei centralizzanti di una involuzione non-centrale in M_{12}, con due naturali sistemi d'imprimitività: uno costituito da 6 blocchi di lunghezza 2, l'altro da 2 blocchi di lunghezza 6.

b) $A_4 \times S_3$, con due naturali sistemi d'imprimitività: uno costituito da 4 blocchi di lunghezza 3, l'altro da 3 blocchi di lunghezza 4.

c) $[E_{2^4}](E_{2^3} \cdot S_3)$, il normalizzante di un sottogruppo abeliano elementare di ordine 2^4, normale in un 2-sottogruppo di Sylow di M_{12}, con un sistema d'imprimitività costituito da 3 blocchi di lunghezza 4.

(Notiamo infine che M_{12} contiene, come è chiaro, una seconda classe di sottogruppi (non massimali) isomorfi a PSL(2.11): ciascuno di essi è contenuto in un unico sottogruppo di ciascuna delle due classi di sottogruppi massimali isomorfi a M_{11}. Per entrambe le classi di PSL(2,11), è $N_{\mathrm{Aut}(M_{12})}(\mathrm{PSL}(2,11)) \simeq \simeq \mathrm{PGL}(2,11)$, massimale in $\mathrm{Aut}(M_{12})$.)

M_{11}: Conviene rappresentare M_{11} come lo stabilizzante di un punto δ e A nel gruppo$(M_{24})_{[\Delta]}$. Vi sono 5 classi di sottogruppi massimali in M_{11}:

a) una classe di sottogruppi isomorfi a PSL(2,11), che si ottengono fissando un punto $\delta' \in \Delta'$, e sono 2-transitivi su $\Delta \setminus \{\delta\}$ e $\Delta' \setminus \{\delta'\}$ (cfr.f) in M_{22} e ii), a) in M_{12});

b) una classe di sottogruppi isomorfi a M_{10}, che si ottengono da ii),b) in M_{12} fissando un punto $\delta_1 \in \Delta \setminus \{\delta\}$ (cfr. anche g) in M_{22});

c) una classe di sottogruppi isomorfi all'estensione spezzata $[E_{3^2}]\,\mathrm{Syl}_2(M_{11}) = M_9 \cdot C_2 \subset \mathrm{Hol}(E_{3^2})$, che si ot-

tengono da ii),c) in M_{12} fissando un punto nell'orbita di lunghezza 3 su A ;

d) una classe di sottogruppi isomorfi $GL(2,3) = [Q_8]S_3$ ($= [M_8]S_3$), che si ottengono da ii),d) in M_{12} fissando un punto nell'orbita di lunghezza 4 su A: è la classe dei centralizzanti di un'involuzione in M_{11};

e) una classe di sottogruppi isomorfi a S_5 con la seguente partizione in orbite di $A'U\Delta'$: 1+5+6|2+10 (da iii),a) in M_{12}).

(In ciò che precede si è omessa, per ragioni di brevità, una descrizione diretta dei sottogruppi massimali di ciascun gruppo M_i (i=11,12,22,23), in funzione dei blocchi del corrispondente sistema di Steiner. La si lascia per esercizio al lettore.)

Concludiamo questa sezione ricordando la "survey" di Greenberg (1973), di cui è parte fondamentale una descrizione minuziosa di tutti i sottogruppi dei gruppi di Mathieu. I 5 gruppi di Mathieu sono trattati separatamente, le dimostrazioni sono omesse. Sfortunatamente la trattazione è piuttosto ripetitiva e laboriosa, e non esente da errori anche gravi, come l'asserzione $M_{11} \not\subset M_{23}$ (già presente in Garbe. Mennicke (1964)).

ADDENDUM:

PSL(2,7), considerato come sottogruppo massimale di M_{24}, è oggetto di ulteriori riflessioni in Collins (1984), In particolare, Collins prova che M_{24} contiene esattamente due classi di S_4 "regolari" (i.e. generati da elementi a,b con o(a) = 2,

$o(b) = 3$ e $o(ab) = 4$, e a, b, ab privi di punti fissi su Ω), con rappresentanti S, S' in un fissato sottogruppo $L \simeq PSL(2,23)$; e che si può scegliere un sottogruppo $M \simeq PSL(2,7)$ massimale in M_{24}, tale che sia $L \cap M = S$ o S'. Su tali basi, Collins propone una potenziale costruzione alternativa di M_{24}.

§8. CARATTERIZZAZIONI GRUPPALI DEI GRUPPI DI MATHIEU

In questo paragrafo descriveremo varie caratterizzazioni dei gruppi di Mathieu, considerati come gruppi semplici. Tutte, al di là dell'interesse intrinseco, traggono motivazioni dal vasto programma della classificazione dei gruppi semplici finiti. Abbiamo scelto un punto di vista "storico", anche se le caratterizzazioni che menzioneremo possono a volte considerarsi, a posteriori, casi particolari 0 corollari di caratterizzazioni meno specifiche, aventi un più ampio spettro d'azione. D'altra parte, la dimostrazione di teoremi di classificazione molto generali riposa ordinariamente proprio sull'uso sistematico di un gran numero di caratterizzazioni specifiche.

A) Centralizzanti di involuzioni

Queste caratterizzazioni si situano nel solco del "programma di Brauer". Se G è un gruppo semplice di ordine pari, e z è una involuzione di G, si ha $|G| \leq (|C_G(z)|^2)!$ (Brauer,Fowler (1955)): da ciò segue che, se H è un gruppo finito, esiste al più un numero finito di gruppi semplici in cui il centralizzante di una involuzione sia isomorfo a H. Richard Brauer formulò su tale base il progetto di caratterizzare gruppi semplici mediante la struttura dei centralizzanti di involuzioni (cfr. Brauer (1954)).

Teoremi di questo tipo hanno giocato un ruolo cruciale nella caratterizzazione di gruppi semplici noti, nella scoperta di nuovi gruppi sporadici, e nella strategia generale della classificazione dei gruppi semplici (cfr. Collins, ed. (1980), Gorenstein

(1982)). Il teorema di caratterizzazione di M_{11} (Brauer (1954)) riportato qui sotto, se ne può considerare un capostipite. Nel seguito, non si farà quasi cenno delle dimostrazioni, in genere molto complesse, e tipicamente affidate a tecniche di teoria delle rappresentazioni (in particolare di teoria modulare, o "di Brauer"). di analisi locale, e di teoria della fusione.

M_{11}:

Mll ha una sola classe di involuzioni, di tipo $1^3 2^4$. Il centralizzante di un'involuzione è isomorfo a GL(2,3), estensione spezzata di Q_8 mediante S_3.

Nel 1954, al Congresso internazionale di Amsterdam, R. Brauer annunciò il seguente:

TEOREMA (Brauer (1954)). Sia G un gruppo finito di ordine pari, z un'involuzione di G, e si supponga che sia: i) $G = G'$; ii) $C_G(z) \simeq GL(2,q)$; $C,(z) = C_G(x)$, per ogni $x \in Z(C_G(z)) \setminus \{1\}$. Se $q \equiv -1(4)$, $q \not\equiv 1(3)$, e $q \neq 3$. allora $G \simeq PSL(3,q)$; se $q=3$, allora $G \simeq PSL(3,3)$ oppure $G \simeq M_{11}$.

Questo risultato è corollario del pih generale:

TEOREMA (Brauer (1966)). Sia G un gruppo finito di ordine pari, e z un' involuzione di C. Se G è privo di sottogruppi di indice 2, e $C_G(z) \simeq GL(2,q)/Z_d$, con $q \equiv -1(4)$ e Z_d sottogruppo centrale di ordine dispari d, allora: i) $G \simeq PGL(3,q)$, $PSL(3,q)$, o $SL(3,q)$; ii) $G \simeq PSL(3,q) \times C_3$, con $q \equiv 1(3)$. $q \not\equiv 1(9)$; iii) $q = 3$ e $G \simeq M_{11}$. (In particolare, se G è semplice, $G \simeq PSL(3,q)$, oppure $G \simeq M_{11}$.)

(Le precedenti caratterizzazioni possono considerarsi casi

speciali del "teorema dell'involuzione classica", che caratterizza i gruppi di Chevalley in caratteristica dispari, e gioca un ruolo cruciale nella determinazione dei gruppi semplici "of component type", e in special modo nella soluzione dei problemi delle "forme standard" (cfr. ad es. Seitz (1980)). Il gruppo M_{11} è l'unica eccezione sporadica che compare nel teorema sopraddetto, che possiamo enunciare nella forma seguente:

TEOREMA (dell'involuzione classica, Aschbacher (1977A)). Sia G un gruppo semplice, e z un'involuzione di G. Se $C_G(z)$ contiene un sottogruppo subnormale L isomorfo a SL(2,q), q dispari, e $z \in L$, allora G è un gruppo di Chevalley sul campo GF(q) (con l'eccezione di PSL(2,q) e di ${}^2G_2(q)$) oppure G è isomorfo a M_{11}. (Nel caso di un gruppo G di Chevalley, il sottogruppo $L = \langle X_r, X_{-r} \rangle$ generato da due sottogruppi radicali X_r, X_{-r} relativi a una coppia di radici lunghe fra loro opposte, è isomorfo a SL(2,q), e l'unica involuzione z di L soddisfa le condizioni del Teorema. L è anzi normale in $C_G(z)$, salvo nel caso ortogonale.))

Si noti che GL(2,3) può anche riguardarsi come estensione non spezzata di C_2 mediante S_4. Held (1968A,1968B,1969A) ha classificato i gruppi semplici con le seguenti proprietà: a) il centro di un 2-sottogruppo di Sylow è ciclico; b) il centralizzante di un' involuzione centrale è estensione di un gruppo abeliano elementare E_{2^r}, $r \leq 4$, mediante il gruppo simmetrico S_4. Sono i gruppi seguenti: A_8, A_9, A_{10}, PSL(3.3). M_{11}, M_{12}, M_{22}. Se r=1, l'estensione è non spezzata, e si ha il seguente:

TEOREMA (Held (19688)). Sia G un gruppo semplice finito, z un'involuzione centrale di G. Se: i) $Z(Syl_2G)$ è ciclico; ii) $CG(z)$ è estensione di C_2 mediante S_4, allora $G \simeq PSL(3,3)$ oppure $G \simeq M_{11}$.

M_{12}:

M_{12} ha due classi di involuzioni: una classe di involuzioni centrali, di tipo $1^4 2^4$, e una classe di involuzioni non-centrali, di tipo 2^6.

Il centralizzante di un'involuzione centrale in M_{12} è isomorfo all'olomorfo del gruppo dei quaternioni Q_8, estensione spezzata di Q_8 mediante S_4. Si ha il seguente teorema (che può considerarsi un corollario di Brauer. Fong (1966). cfr. la sezione B) di questo paragrafo):

TEOREMA (Wong W.J. (1964B)). Sia G un gruppo finito, z un'involuzione di G, e si supponga che: i) $C_G(z)$ sia isomorfo al centralizzante di un' involuzione centrale di M_{12}: ii) G contenga al più due classi di involuzioni. Allora G è isomorfo a M_{12}, oppure G è estensione non spezzata di E_{23} mediante PSL(3,2). (Tale estensione è unica, a meno d'isomorfismi, ed è esplicitamente rappresentata come un gruppo di trasformazioni non-lineari di V(4,2)).

Si noti che l'olomorfo di Q_8 può anche riguardarsi come estenzione non spezzata di E_{23} mediante S_4. In proposito, Held (1968B) contiene il seguente:

TEOREMA. Sia G un gruppo semplice finito, z un'involuzione

centrale di G. Se i) $Z(Syl_2 G)$ è ciclico; ii) $C_G(z)$ è estensione di E_{23} mediante S_4, allora l'estensione è spezzata, e $G \simeq A_8, A_9$, oppure l'estensione non è spezzata e $G \simeq M_{12}$.
(Il risultato dipende da Wong W.J. (19648) e Brauer. Fong (1966)).

Il centralizzante di un'involuzione non-centrale di M_{12} è isomorfo a $C_2 \times S_5$. Si noti che $S_5 \simeq PGL(2,5) \simeq PGL(2,4)$, ove σ è l'automorfismo di PGL(2,4) indotto dall'automorfismo di Frobenius di GF(4). Thwaithes (1973) contiene (corollario di un risultato più generale) il seguente:

TEOREMA. Sia G un gruppo semplice finito, e z un'involuzione di G. Se $C_G(z) = \langle z \rangle \times PGL(2,4) \langle \sigma \rangle$, allora $G \simeq M_{12}$.

Sussiste anche il seguente:

TEOREMA (Sitnikov (1974)). Sia G un gruppo semplice finito, e z un'involuzione di G. Se $C_G(z) = \langle z \rangle \times PGL(2,q)$, q dispari, allora $q = 5$ e $G \simeq M_{12}$.

M_{22}:

M_{22} ha una sola classe di involuzioni, di tipo $1^6 2^8$. Il centralizzante di un'involuzione è estensione spezzata di E_{24} mediante S_4, ed è isomorfo al centralizzante di un'involuzione di E_{24} nel sottogruppo massimale $[E_{24}]A_6$ (stabilizzante di un blocco del sistema S(3,6,22)). Anche nel gruppo alterno A_{10} il centralizzante di un'involuzione centrale è estensione spezzata di E_{24} mediante S_4: le strutture delle due estensioni sono pero diverse. (A_{10} è caratterizzato dal centralizzante di un'involuzione centrale, cfr. Held (1969A)).

Sussiste il seguente:

TEOREMA (Janko (1968A), Held (1968A,1969A)). Sia G un gruppo semplice finito, e z un'involuzione centrale di G. Se: i) $Z(Syl_2G)$ è ciclico; ii) CG(z) è estensione di E_{24} mediante S_4, allora l'estensione è spezzata, e G è isomorfo ad A_{10} oppure a M_{22}.
(Il risultato è provato, nell'ipotesi che l'estensione $E_{24}S_4$ sia spezzata, indipendentemente da Janko (1968A) e da Held (1969A). Held (1968A) prova che l'estensione è necessariamente spezzata.)

M_{23}:

M_{23} ha una sola classe di involuzioni, di tipo 1728. Il centralizzante di un'involuzione è estensione spezzata .di E_{24} mediante GL(3,2), ed è isomorfo al centralizzante di un'involuzione di E_{24} nel sottogruppo massimale $[E_{24}]A_7$ (stabilizzante di un blocco del sistema S(4,7,23)). Inversamente, sussiste il seguente :

TEOREMA (Janko (1968B)). Sia G un gruppo semplice finito, e z una involuzione centrale di G. Se i) $Z(Syl_2G)$ è ciclico; ii) $C_G(z)$ è estensione di E_{24} mediante GL(3,2), allora l'estensione è spezzata, e G è isomorfo a M_{23}.

Il risultato è generalizzabile nel seguente:

TEOREMA (Dempwolff (1972)). Sia G un gruppo semplice finito, e. z un'involuzione centrale di G. Se $C_G(z)$ è estensione spezzata di E_{2^n} mediante GL(n-1,2), allora n=2 e $G \simeq A_5$, oppure n=4 e $G \simeq M_{23}$.

M_{24}:

M_{24} ha due classi di involuzioni: una classe di involuzioni

centrali. di tipo $1^8 2^8$, e una classe di involuzioni non-centrali. di tipo 2^{12}.

1) Un'involuzione z di tipo $1^8 2^8$ fissa i punti di un'ottade 0 del sistema S(5,8,24). Il centralizzante di z in M_{24} è contenuto nello stabilizzante di 0: pertanto, è isomorfo al centralizzante di un'involuzione di E_{24} in Hol (E_{24}) $\simeq$ AGL(4,2) (cfr.§7), ed è facile riconoscere che è estensione spezzata di E_{24} mediante Hol(E_{23}) $\simeq$ AGL(3,2) (le strutture, precedentemente descritte, dei centralizzanti di involuzioni in M_{23} e in M_{22} ne conseguono immediatamente). Si osservi inoltre che il sottogruppo $O_2(C_{M_{24}}(z)) = [E_{24}]E_{23}$ è un gruppo extraspeciale 2^{1+6} con centro $\langle z \rangle$, e può anche riguardarsi come prodotto dei sottogruppi $E_1 = E_{24}$ e $E_2 = \langle z \rangle \times E_{23}$, entrambi normali in $C_{M_{24}}(z)$.

La stessa struttura di $C_{M_{24}}(z)$ ha anche il centralizzante di una trasvezione nel gruppo projettivo PSL(5,2) ($\simeq$ GL(5,2)). E proprio nell'intento di caratterizzare i gruppi semplici M_{24} e PSL(5,2) mediante un tale centralizzante d'involuzione, Held (1969B) fu condotto a scoprire un nuovo gruppo semplice, il gruppo sporadico He di ordine $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$, che ha due classi di involuzioni, e nel quale appunto il centralizzante di un'involuzione centrale è isomorfo al centralizzante di un'involuzione centrale di M_{24} e PSL(5,2).

Vari autori hanno contribuito a mettere in luce il legame fra M_{24} e He. Il risultato seminale è in Held (1969B):

TEOREMA (Held (1969B), G.Higman, J.G.McKay). Sia G un gruppo semplice finito, z un'involuzione di G. H il centralizzante di z in

in G, Ho il centralizzante di un'invcluzione di E_{24} in Hol(E_{24}). Se $H \simeq H_o$, si hanno tre possibilità per G: i) $G \simeq PSL(5,2)$; ii) $G \simeq M_{24}$; iii) $G \simeq He$.

Un cenno alla dimostrazione: Si considera $O_2(H) = 2_+^{1+6} = E_1E_2$, con E_1, E_2 sottogruppi normali di H, abeliani elementari di ordine 2^4. L'analisi della fusione delle involuzioni porta a due possibilità per $N_G(E_i)$, i=1,2: o $N_G(E_i) = H$, oppure $N_G(E_i)/E_i \simeq GL(4,2)$. Se ne deducono tre possibilità per G: i) se $N_G(E_i)/E_i \simeq GL(4,2)$, i = 1.2. si ha $G \simeq PSL(5.2)$; ii) se $N_G(E_i)/E_i \simeq GL(4,2)$ e $N_G(E_j) = H$, $i \neq j = 1,2$, si ha $G \simeq M_{24}$; iii) se $N_G(E_i) = H$, i = 1.2, si ha $G \sim$ He. Held (1969B) determina ordine, classi d i coniugio, centralizzanti degli elementi, normalizzanti dei. sottogruppi di Sylow di G nel caso iii). Esistenza e unicità di G sono state accertate da G.Higman e J.McKay, con una costruzione esplicita che fa ricorso all'uso di un computer. (Presentazioni per He sono state prodotte da McKay (1974) e da Cannon,Havas (1974). 1 sottogruppi massimali di He sono stati determinati da Butler (1981)).

Si può fare una richiesta più debole su $C_G(z)$, espressa dal seguente :

TEOREMA (Held,Schoenwaelder (1970)). Sia G un gruppo semplice finito, e z un'involuzione centrale di G. Se $C_G(z)$ è estensione di un gruppo extraspeciale 2^{1+6} mediante GL(3,2), allora $G \simeq PSL(5,2), M_{24}, He$.

(Si prova che $O_2(C_G(z)) = 2^{1+6}$ è di tipo +, e che $C_G(z)/O_2(C_G(z))$ opera in modo completamente riducibile sullo spazio $2^{1+6}/2$. Ne segue che l'estensione è spezzata, e ci si riconduce a Held

(1969B) .)

Il Teorema precedente ammette come conseguenza che $PSL(5,2)$, M_{24} e He sono i soli gruppi semplici contenenti un'involuzione il cui centralizzante è un gruppo perfetto, estensione di 2^{1+6} mediante $GL(3,2)$. Una variazione su questo tema è il seguente risultato, la cui dimostrazione si riconduce in ultima analisi a Held, Schoenwaelder (1970):

TEOREMA (Striko (1976)). Sia G un gruppo semplice finito, z un'involuzione di G, $H = C_G(z)$. Se i) H è perfetto; ii) H contiene un sottogruppo normale $V = 2^{1+6}$; iii) $C_H(V) \subseteq V$; allora $G \simeq PSL(5,2)$, M_{24}, He.

Altra variazione è la seguente:

TEOREMA (Schoenwaelder (19748)). Sia G un gruppo finito, z un'involuzione di G, $H = C_G(z)$. Se H/O(H) è isomorfo a H_o (il centralizzante di un'involuzione di E_{24} in $Hol(E_{24})$), allora G/O(G) è isomorfo a uno dei gruppi seguenti: H_o, $Hol(E_{24})$, $PSL(5,2)$, M_{24}, He.

Ancora, Ademaj (1978) prova il seguente:

TEOREMA. Sia G un gruppo semplice finito, z un'involuzione centrale di G, $H = C_G(z)$. Se i) $O_2(H) = 2^{1+2n}$; ii) $H/O_2(H) \simeq PSL(n,2)$; allora $G \simeq PSL(n+2,2)$, oppure $n=3$ e $G \simeq M_{24}$, He. (Cfr. anche Dempwolff (1974)).

Una drastica generalizzazione dei risultati precedenti fu ottenuta da U. Dempwolff e S.K. Wong nell'ambito di un'analisi generale dei gruppi finiti in cui il centralizzante di un'involuzione contiene sottogruppi normali extraspeciali

e abeliani (Dempwolff, Wong S.K. (1977.1978)). analisi connessa al cosiddetto "problema extraspeciale", di cui si farà cenno in §13,D)). Vale precisamente il seguente:

TEOREMA (Dempwolff.Wong S.K. (1978)). Sia G un gruppo semplice finito, e z un'involuzione di G. Se $F^*(C_G(z))$ è un gruppo extraspeciale $P = 2^{1+2n}$, $n \geq 3$, si hanno due possibilità: i) CG(z) opera in modo irriducibile sullo spazio $P/\langle z \rangle$; ii) $G \simeq PSL(n+2,2)$, oppure $n=3$ e $G \simeq M_{24}$, He.

Nelle ipotesi del Teorema precedente, è possibile precisare: se $n=3$, allora $G \simeq PSL(5,2)$, $PSU(5,2)$, M_{24}, He, Sz (il gruppo sporadico di Suzuki) (cfr. Smith S.D. (1979)).

Menzioniamo infine un risultato che coinvolge anche M_{23} e i gruppi di Janko J_2, J_3, e dipende da Held, Schoenwaelder (1970), oltre che da risultati di Janko:

TEOREMA (Beisiegel(1974)). Sia G un gruppo semplice finito, e z un'involuzione centrale di G. Se i) $Z(Syl_2G)$ è ciclico; ii) $C_G(z)$ contiene un L-sottogruppo normale V di ordine $\leq 2^7$; iii) $C_G(z)/V$ è semplice con 2-sottogruppi di Sylow diedrali; allora $G \simeq M_{23}, M_{24}, PSL(5,2)$, He, J_2, J_3.

2) Si consideri un'involuzione t di tipo 2^{12}, contenuta nello stabilizzante di un sestetto $G_3 = ([F_{2^6}]G_3) \cdot S_6$ (cfr.§7). Vi sono 31878 involuzioni di tipo 2^{12} in M_{24}, e poiché G_3 permuta transitivamente le 18 involuzioni di tipo 2^{12} contenute in F_{2^6}, segue che $|C_{M_{24}}(t)| = |C_{G_3}(t)|$. Ciò implica che il centralizzante di un'involuzione non-centrale t in M_{24} è contenuto nello stabilizzante di un sestetto, ed è estensione non spezzata

di F'_6 (= $O_2(C_{M_{24}}(t))$ mediante S_5.

Si ha il seguente:

TEOREMA (Stroth (1975A)). Sia G un gruppo semplice finito, e z un'involuzione di G. Se CG(z) è isomorfo al centralizzante di un'involuzione non-centrale di M_{24}, allora $G \simeq M_{24}$.

Stroth dimostra che $Syl_2G \simeq Syl_2M_{24}$, e applica Schoenwaelder (1974A) (cfr. la sezione B)). Il risultato è parte di un'analisi pih ampia, motivata dal fatte che il centralizzante di un'involuzione non-centrale nel gruppo di Suzuki Sz è estensione spezzata di E_{2^2} mediante $PSL(3,4)\cdot C_2$, e quindi è "simile" al centralizzante di un'involuzione non-centrale in He, che è estensione non spezzata di E_{2^2} mediante $PSL(3,4)\cdot C_2$. Stroth (1975A, 1975B) dimostra essenzialmente che, nel caso di M_{24} e di PSL(5,2), non si possono invece presentare altri gruppi semplici con centralizzanti "simili". (D'altra parte, Sz è pienamente caratteri2 zato mediante il centralizzante anzidetto da Reifart (1975).)

3) Si ha infine il seguente, complessivo:

TEOREMA (Held (1973), Deckers (1974)). Sia G un gruppo semplice finito, e z un'involuzione di G. Se $C_G(z)$ è isomorfo al centralizzante di una (qualsiasi) involuzione di He, allora $G \simeq PSL(5,2), M_{24}, He$.

(Poiché, in forza di Held (1969B), si può supporre $C_G(z) \simeq C_{He}(t)$, con t involuzione non-centrale di He, il risultato è in effetti una caratterizzazione di He mediante il centralizzante di un'involuzione non-centrale. Tale caratterizzazione è ottenuta da Deckers (1974) nell'ipotesi che sia $|Syl_2G \leq 2^{10}$, utilizzando

Schoenwaelder (1974A); Held (1973) tratta il caso $|Syl_2 G| > 2^{10}$, escludendone la possibilità.)

Concludiamo questa sezione con qualche ulteriore osservazione:

a) Esaminando la struttura dei centralizzanti di involuzioni nei gruppi di Mathieu. si riconosce che sono tutti "core-free" (i.e. per ogni involuzione z in M_i (i=11,12,22,23,24), $O(C_{M_i}(z)) = \{1\}$), e, con l'eccezione del centralizzante di un'involuzione non-centrale in M_{12}, isomorfo a $C_2 \times S_5$, sono 2-costretti.

Ricordiamo qui che i gruppi semplici finiti si suddividono, alla luce del programma di classificazione di Gorenstein-Aschbacher, in due classi: quella dei gruppi detti "of component-type", e quella dei gruppi "Of noncomponent-type" (cfr. ad es. Collins (1980), Gorenstein (1982)). Appartengono alla prima classe i gruppi semplici G nei quali esiste un'involuzione z, tale che $C_G(z)/O(C_G(z))$ sia dotato di una componente, i.e. di un sottogruppo subnormale quasisemplice. ciò che equivale ad asserire che CG(z) non è 2-costretto. Fra i gruppi di Mathieu, M_{12} è dunque l'unico "of component-type" (e la componente S_5 del centralizzante di un'involuzione non-centrale è "standard" nel senso di Aschbacher (1976A): cfr. la sezione E)).

b) I gruppi di Mathieu M_{11}, M_{12}, M_{24} sono gruppi "di tipo GF(2)".

Ricordiamo in proposito che un gruppo **semplice** finito G si dice "di tipo GF(2)" se contiene un'involuzione z, tale che $F^*(C_G(z))$ sia un 2-gruppo privo di sottogruppi caratteristici

abeliani non-ciclici (un 2-gruppo cosiffatto si dice "di tipo simplettico". ed è prodotto centrale di un gruppo extraspeciale e di un gruppo ciclico, diedrale, quasidiedrale o quaternionale). I gruppi "di tipo GF(2)" sono stati classificati con il contributo di vari autori (cfr. Aschbacher (1976B, 1977B), Smith S.D. (1979,1980A,1980B), Timmesfeld (1978)). e sono essenzialmente gruppi di Chevalley sul campo GF(2), salvo alcune eccezioni di rango basso, e ben 16 gruppi sporadici. Il caso più interessante si presenta quando $F^*(C_G(z))$ è extraspeciale (ciò che accade in particolare per i gruppi M_{11}, M_{12} e M_{24}). Per cenni ulteriori su questo argomento, cfr. §13,D).

c) Per ragioni di completezza, conviene notare che:

i) $Aut(M_{12})$ contiene tre classi di involuzioni: oltre alle due classi di involuzioni contenute in M_{12}, vi è una classe di involuzioni contenute in $Aut(M_{12}) \setminus M_{12}$, con centralizzante in M_{12} isomorfo a $C_2 \times A_5$ (a tale classe appartengono le involuzioni del sottogruppo massimale PGL(2.11) non contenute in PSL(2,11)).

ii) $Aut(M_{22})$ contiene tre classi di involuzioni: oltre alla classe di involuzioni di M_{22}, vi sono due classi di involuzioni contenute in $Aut(M_{22}) \setminus M_{22}$, con centralizzanti rispettivamente isomorfi all'olomorfo di E_{2^4}, e a un'estensione spezzata di E_{2^4} mediante $Hol(C_5)$ (con $[E_{2^4}, g] = E_{2^4}$, $1 \neq g \in C_5$).

d) Concludiamo questa sezione rammentando, senza entrare in dettagli, che la classificazione dei gruppi semplici ha anche richiesto "caratterizzazioni dispari". Sussistono in particolare dei teoremi di caratterizzazione mediante la struttura dei centralizzanti di elementi di ordine 3, concernenti

M_{22}, M_{23} e M_{24} (cfr. O'Nan (1976A), Durakov (1979)).

B) Struttura dei 2-sottogruppi di Sylow

Per ciascuno dei gruppi di Mathieu descriveremo la struttura dei l-sottogruppi di Sylow, e i teoremi di caratterizzazione corrispondenti. Non deve sorprendere che queste caratterizzazioni siano intimamente legate, per i risultati e per le tecniche impiegate, a quelle mediante i centralizzanti di involuzioni.

M_{11}:

Un 2-sottogruppo di Sylow di Mll è quasidiedrale di ordine 24, i.e. $Syl_2M_{11} = \langle x,y | x^8 = y^2 = 1, y^{-1}xy = x^3 \rangle$. Identica struttura ha un 2-sottogruppo di Sylow di PSL(3,3).

Si noti che $Z(Syl_2M_{11}) = \langle x4 \rangle$, e $C_{M_{11}}(x^4) \simeq GL(2,3)$ possiede un 2-complemento ciclico di ordine 3. Wong W.J.(1964A) ha provato il seguente:

TEOREMA. Sia G un gruppo semplice finito, e sia $Syl_2G = \langle x,y | x^{2a} = y^2 = 1, y^{-1}xy = x^{2^{a-1}+\varepsilon}, \varepsilon = \pm 1, a \geq 3 \rangle$. Allora $\varepsilon = -1$, cioé Syl_2G è quasidiedrale, e se $C_G(x^{2^{a-1}})$ possiede un 2-complemento abeliano, $G \simeq PSL(3,3)$ oppure $G \simeq M_{11}$.

Più in generale, Wong W. J. (1964A) dimostra che, se G è un gruppo finito con 2-sottogruppi di Sylow quasidiedrali, e $C_G(Z(Syl_2G))$ possiede un 2-complemento abeliano, allora $G/O(G) \simeq Syl_2G$, $GL(2,3)$, $PSL(3,3)$, M_{11}, o H(q) (ove H(q) è il sottogruppo di $P\Gamma L(2,q)$, $q = p^{2m}$, p dispari, costituito dalle permutazioni sulla retta projettiva $PG(1,q)=GF) \cup \{\infty\}$,

così definite: $x \to (ax^\gamma + b)/(cx^\gamma + d)$, con $\gamma = 1$ o $\gamma = p^m$ secondo che $ad-bc$ sia o non sia un quadrato in $GF(q)^*$. In particolare, $H(9) = M_{10}$ (cfr. §2)). Per analoghi risultati, sotto ipotesi leggermente diverse, cfr. anche Mazurov (1966.1967). (I gruppi semplici finiti con 2-sottogruppi di Sylow quasidiedrali sono stati completamente classificati in un famoso lavoro di Alperin, Brauer. Gorenstein (1970). Il Teorema precedente si può pertanto considerare un caso speciale del seguente:

TEOREMA (Alperin. Brauer. Gorenstein (1970)). Sia G un gruppo semplice finito, con 2-sottogruppi di Sylow quasidiedrali. e sia z un'involuzione di G. Allora: i) $C_G(z) \simeq GL(2,q)/Z_d$, ove $q \equiv -1(4)$ e Z_d è un sottogruppo centrale di $GL(2,q)$ di ordine dispari d. Segue da Brauer (1966) che G è isomorfo a $PSL(3,q)$ o a M_{11}; ii) $C_G(z) \simeq GU(2,q)/Z_d$, ove $q \equiv 1(4)$ e Z_d è un sottogruppo centrale di $GU(2,q)$ di ordine dispari d, e G è isomorfo a $PSU(3,q)$.)

M_{12}:

Il centralizzante di un'involuzione centrale in M_{12} è isomorfo all'olomorfo di Q_8: pertanto, Syl_2M_{12} è la naturale estensione spezzata di Q_8 mediante Dg. (L'olomorfo di Q_8 può anche riguardarsi come estensione spezzata di $Q_8 * Q_8 = 2_+^{1+4}$ mediante S_3. Ne segue che un 2-sottogruppo di Sylow di M_{12} ammette anche la presentazione: $Syl_2M_{12} = \langle x,y,z,t,u \mid x^4 = y^4 = z^4 = t^4 = [x,z] = [x,t] = [y,z] = [y,t] = 1, x^2 = y^2 = z^2 = t2 = [x,y] = [z,t], u^{-1}xu = x^{-1}, u^{-1}yu = xy^{-1}, u^{-1}zu = z^{-1}, u^{-1}tu = zt^{-1} \rangle$. Da questa si può dedurre anche la presentazione seguente: $Syl_2M_{12} = \langle a,b,c,d \mid a^4 = b^4 =$

$= c^2 = d^2 = [a,b] = [c,d] = 1,\ c^{-1}ac = a^{-1}bc = b^{-1}, d^{-1}ad = b>.$)

Hanno 2-sottogruppi di Sylow isomorfi a quelli di M_{12} anche i gruppi semplici $G_2(q)$, per $q \equiv 3,5(8)$, e $D_4^2(q)$ ($= P\Omega^-(8,q)$), per $q \equiv 3$, S(8), e il gruppo $T = E_{23} GL(3,2)$, l'unica estensione non spezzata di E_{23} mediante $GL(3,2)$. Si noti che i gruppi $G_2(q)$ e $D_4^2(q)$ contengono una sola classe di involuzioni, mentre T contiene, al pari di M_{12}, due classi di involuzioni.

Una prima parziale caratterizzazione, in funzione della struttura di Syl_2M_{12}, si deve a Brauer,Fong (1966). M_{12} contiene un elemento s di ordine 8, autocentralizzante e coniugato a s^3, s^5 e s^7 (e pertanto autocentralizzante e coniugato a s^3, s^5 e s^7 in un 2-sottogruppo di Sylow di M_{12}). Orbene, vale il seguente :

TEOREMA (Brauer,Fong (1966)). Sia G un gruppo finito di ordine $2^6 \cdot m$, m dispari. Si supponga che G contenga un elemento s di ordine 8, autocentralizzante in un l-sottogruppo di Sylow S di G, e coniugato a s^3, s^5 e s^7 in S. Si hanno allora le seguenti possibilità : i) G ha un sottogruppo di indice 2; ii) G ha una sola classe di involuzioni iii) $G/O(G) \simeq T$, oppure $G/O(G) \simeq M_{12}$.

(La dimostrazione si basa essenzialmente su tecniche di teoria modulare. In ultima analisi, M_{12} è identificato mediante l'ordine, in forza di Stanton (1951) (cfr. la sezione D)).

Segue in particolare dal Teorema precedente che, se G è un gruppo semplice finito, con $Syl_2G \simeq Syl_2M_{12}$, e G ha più

di una classe di involuzioni, allora G è isomorfo a M_{12}. Nel caso in cui G contenga una sola classe di involuzioni, il risultato definitivo si deve a **Gorenstein,Harada** (1971B). previa uso essenziale di un risultato di Harris (1971). Si ha dunque il seguente complessivo:

TEOREMA (Harris (1971), Gorenstein. **Harada** (1971B)). Sia G un gruppo finito privo di sottogruppi di indice 2. con G=G', O(G) = Z(G) = 1. Se $Syl_2G \simeq Syl_2M_{12}$, allora G è isomorfo a uno dei gruppi seguenti: $T; M_{12}; G_2(q), q \equiv 3,5(8); {}^2D_4(q), q \equiv 3,5(8)$.

M_{22}, M_{23}:

M_{22} e M_{23} hanno 2-sottogruppi di Sylow isomorfi, di ordine 2^7. La struttura del centralizzante di un'involuzione mostra che Syl_2M_{22} è estensione spezzata di E_{24} mediante D_8. (Per una presentazione, cfr. **Garbe,** Mennicke (1964), o Gorenstein, **Harada** (1971A).)

Hanno 2-sottogruppi di Sylow isomorfi a quelli di M_{22} e M_{23} anche i gruppi seguenti: $C_2 \cdot A_8$ (il ricoprimento di A_8); PSL(4,q), per $q \equiv 5(8)$; PSU(4,q), per $q \equiv 3(8)$; e il gruppo sporadico di McLaughlin Mc. (Mc è stato costruito da J.McLaughlin (cfr.Mc-**Laughlin** (1969)) come estensione transitiva di rango 3 di PSU(4,3). Mc ha una sola classe di involuzioni, i cui centralizzanti sono isomorfi a $C_2 \cdot A_8$, ed è pienamente caratterizzato dalla struttura di tali centralizzanti (cfr. **Janko,** Wong S.K.(1972))).

Si ha il seguente:

TEOREMA (Phan 1969, 1970, 1971) **Gorenstein,** Harada, (1971A), **Mason** D.R. (1973)). Sia G un gruppo semplice finito, e si supponga

$Syl_2G \simeq Syl_2M_{22}$. Allora G è isomorfo a uno dei gruppi seguenti: M_{22}; M_{23}; il gruppo di McLaughlin Mc; $PSL(4,q)$, $q \equiv 5(8)$; $PSU(4,q)$, $q \equiv 3(8)$.

M_{24} :

M_{24} ha 2-sottogruppi di Sylow di ordine 2^{10}, isomorfi ai 2-sottogruppi di Sylow di $PSL(5,2)$ e di He. La struttura di Syl_2M_{24} è dettagliatamente descritta in Schoenwaelder (1974A) (per una presentazione cfr. anche Garbe. Mennicke (1964)).

Si ha il seguente:

TEOREMA (Schoenwaelder (1974A,1974B)). Sia G un gruppo finito, privo di sottogruppi di indice 2, e sia $Syl_2G \simeq Syl_2M_{24}$. Allora G/O(G) è isomorfo a uno dei gruppi seguenti: $G_o = Hol(E_{24})$; H_o, il centralizzante di un'involuzione di E_{24} in G_o; $PSL(5,2)$; M_{24}; He.

(Le ipotesi su G implicano che, se $H=C_G(z)$, con z involuzione centrale di G, allora $H/O(H) \simeq H_o$. Il risultato segue pertanto dal teorema di caratterizzazione di Schoenwaelder (1974B), citato in A).)

H. Sandlöbes e U. Schoenwaelder hanno poi completamente determinato i gruppi finiti "core-free" con 2-sottogruppi di Sylow isomorfi a quelli di M_{24}. Si ha il seguente:

TEOREMA (Sandlöbes, Schoenwaelder (1979)). Sia G un gruppo finito, con O(G) = 1. e si supponga $Syl_2G \simeq Syl_2M_{24}$. Allora G è isomorfo a uno dei 13 gruppi seguenti: G_o, l'olomorfo di $E_{24} = \langle z,a,b,c \rangle$; $H_o=C_{G_o}(z)$; $H_1=N_{H_o}(\langle z,a \rangle)$; Syl_2M_{24}; lo stabilizzante di un trio in M_{24}; 4 sottogruppi dello stabilizzante di un

trio, descritti esplicitamente mediante generatori; lo stabilizzante di un sestetto in M_{24}; M_{24}; PSL(5,2); He.

(Un cenno alla dimostrazione: Se z è un'involuzione centrale di G, $C_G(z)/O(C_G(z))$ risulta isomorfo a H_o, H_1, o Syl_2M_{24}. Syl_2M_{24} contiene due sottogruppi abeliani elementari di ordine 2^6: E_{2^6}, e E'_{2^6} (cfr. §7). La dimostrazione si basa sull'analisi della fusione in G delle involuzioni di $E_{2^6} \cap E'_{2^6}$: per ciascuna delle possibili strutture di $C_G(z)/O(C_G(z))$ si hanno varie possibilità di fusione, che portano alla determinazione dei vari casi.)

Concludiamo questa sezione con alcune osservazioni:

a) I Z-sottogruppi di Sylow dei gruppi di Mathieu hanno in comune le seguenti proprietà: i) hanno centro di ordine 2; ii) sono autonormalizzanti nei gruppi rispettivi.

b) M_{11} ha Z-rango 2, M_{12} ha Z-rango 3, M_{22} e M_{23} hanno 2-rango 4, M_{24} ha Z-rango 6.

c) Ogni sezione di M_{11}, M_{12}, M_{22}, M_{23} ha l-rango al più 4.

(I gruppi semplici in cui ogni sezione ha 2-rango al pih 4, o, equivalentemente, in cui ogni Z-sottogruppo è generabile da 4 elementi, sono stati classificati in un celebre, ponderoso lavoro di Gorenstein. Harada (1974). In particolare, una tappa cruciale nella dimostrazione del "Main Theorem" di Gorenstein, Harada (1974), è una caratterizzazione di M_{12}, i cui connotati sono però troppo tecnici per essere qui riportati.)

C) Altre caratterizzazioni Z-locali.

Alcune caratterizzazioni dei gruppi di Mathieu in termini di sottogruppi 2-locali sono state ottenute nel più generale contesto dello studio dei gruppi semplici contenenti 2-sottogruppi autocentralizzanti di ordine piccolo:

Si consideri un gruppo semplice finito G. contenente un 2-sottogruppo abeliano elementare E di ordine 2^4, autocentralizzante in G. Allora $N_G(E)/E$ è isomorfo a un sottogruppo di GL(4,2), e i contributi di vari autori consentono di affermare che, quando $N_G(E)/E$ è non-risolubile, la struttura di G è nota (cfr. il conciso rapporto di Stroth(1980)). In particolare, si hanno i seguenti risultati:

1) TEOREMA. Se $N_G(E)/E \simeq GL(4,2)$, allora $G \simeq M_{24}$, PSL(5,2), A_i (i=16,17,18,19), Co_3.

(Se l'estensione $N_G(E) = E \cdot GL(4,2)$ è non spezzata, G è isomorfo al terzo gruppo di Conway Co3 (O'Nan,Solomon (1976)); se l'estensione è spezzata, si ottengono i gruppi rimanenti (Harada (1978), e Harada.Yamaki (1979). sulla base di precedenti risultati di Kierman (1975) e Yamaki (1975)).

2) TEOREMA. Se $N_G(E)/E \simeq Hol(E_{23})$, allora $G \simeq M_{24}$,He. (Stroth (1977B)).

(In M_{24} e in He il centralizzante H di un'involuzione centrale contiene un sottogruppo abeliano elementare E, tale che sia $H = N_G(E)$ (Held (1969B); cfr. A): nel caso di M_{24}, E è il sottogruppo $E_2 = \langle z \rangle \times E_{23}$). In particolare, $N_G(E)/E$ è isomorfo allo stabilizzante di un vettore non nullo di V(4.2) in GL(4,2), i,e. all'olomorfo di E_{23}.)

3) TEOREMA. Se $N_G(E)/E \simeq A_5$, $S_5, A_6, A_7, A_5 \times C_3$ o $(A_5 \times C_3)C_2$, allora ogni sezione di G ha Z-rango al più 4 (Harada (1975A)).

(La struttura di G è determinata, in forza di Gorenstein, Harada (1974). Compaiono qui i gruppi M_{22}, M_{23}, che contengono come sottogruppi massimali le estensioni spezzate $[E_{24}]A_6, [E_{24}]A_7$, soddisfacenti le ipotesi richieste. In particolare, se $N_G(E)/E \simeq A_7$, si ha $G \simeq M_{23}$, Mc, Ly (il gruppo di Lyons).)

I teoremi precedenti coprono, di fatto, tutti i sottogruppi non-risolubili di $GL(4,2)$, eccetto $PSL(2.7)$ e S_6. Anche in questi ultimi due casi, G è noto (cfr. Stroth (1977A) e Stroth (1977C)).

Nel caso, infine, in cui $N_G(E)/E$ sia risolubile, si hanno risultati definitivi quando $O_2(N_G(E)/E) = 1$: allora, ogni sezione di G ha L-rango al più 4 (cfr. Stroth (1977A), Stroth (1980)).

D) Caratterizzazioni mediante l'ordine

Come conseguenza della classificazione dei gruppi semplici finiti, è possibile enunciare il seguente:

TEOREMA. Un gruppo semplice finito è caratterizzato, nella classe dei gruppi semplici finiti, dal suo ordine, se si eccettuano le coincidenze: 1) $|PSp(2n,q)| = |P\Omega(2n+1,q)|$, per $n \geq 3$ e q dispari; 2) $|PSL(3,4)| = |A_8|$.

(Le coincidenze sono classicamente note (cfr. Dickson (1901). Nell'ambito dei gruppi classici, il risultato. si deve a Artin (1955); è stato aggiornato alla classe di tutti i gruppi semplici noti da D.N.Teague.)

Per molti gruppi semplici, si hanno tuttavia caratterizzazioni mediante 1 'ordine che prescindono dalla classificazione. In particolare, i gruppi di Mathieu sono stati così caratterizzati da Stanton. Parrott, e Bryce.

Stanton (1951) prova che, se G è un gruppo semplice, e $|G|=|M_{24}|$, G e M_{24} hanno la stessa tavola dei caratteri. Analogo risultato per M_{12} s i trova già in Brauer (1943). D'altra parte, M_{24} e M_{12} risultano determinati dalle loro tavole dei caratteri: si conclude che M_{24} e M_{12} sono unici del loro ordine.

1 metodi di Stanton sono braueriani, i.e. di teoria modulare dei caratteri. In gran parte analòghi sono i metodi usati da Parrott (1970) per M_{11} e M_{22}. Nel caso di M_{11}, l'ordine determina la struttura di un L-sottogruppo di Sylow: in virtù di Wong W.J. (1964A) (cfr. B)) si conclude che M_{11} è unico del suo ordine. Nel caso di M_{22} si inferisce dall'ordine che il centralizzante di un'involuzione centrale è estensione di E_{24} mediante S_4: in virtù di Held (1968A) si conclude che M_{22} è unico del suo ordine.

Il caso di M_{23} è trattato da Bryce (1971). I metodi sono ancora braueriani, e consentono di determinare la struttura del centralizzante di un'involuzione: M_{23} è allora determinato dal suo ordine, in virtù di Janko (1968B).

E) 1 gruppi di Mathieu come sottogruppi standard

Nello studio dei gruppi semplici "of componont type", secondo il programma di Gorenstein-Aschbacher, si è condotti (in virtù di un fondamentale teorema di Aschbacher-Foote. e della natura

induttiva del processo di classificazione) a dover determinare i gruppi semplici che contengono una "componente standard" (nel senso che preciseremo fra poco) isomorfa a un gruppo quasisemplice noto (cfr. ad es. Collins (1980)). La soluzione definitiva di questi cosiddetti "problemi delle forme standard" è stata una delle ultime tappe del processo di classificazione dei gruppi semplici, e vi hanno contribuito numerosi autori (per questi, e per un resoconto della strategia che è stata seguita, cfr. ad es. Seitz (1980)).

In questa sezione riportiamo concisamente, per ragioni di completezza, i teoremi che si riferiscono a componenti standard isomorfe ai gruppi di Mathieu, benché non si tratti, come è chiaro, di risultati volti specificamente a caratterizzare da un punto di vista gruppale i gruppi di Mathieu.

Ricordiamo innanzitutto la nozione di sottogruppo "strettamente immerso", introdotta da Aschbacher (1975): un sottogruppo K di un gruppo finito G si dice *strettamente immerso* (tightly embedded) in G. se $|K|$ è pari e $|K \cap K^g|$ è dispari per ogni $g \in G \setminus N_G(K)$.

(Il concetto di sottogruppo strettamente immerso si è rivelato estremamente efficace nella descrizione della struttura dei gruppi semplici. Basti considerare il seguente risultato, intimamente legato al teorema dell'involuzione classica (cfr.A)):

TEOREMA (Aschbacher (1977A)). Sia G un gruppo semplice finito, e si supponga che G contenga un sottogruppo K, strettamente immerso in G e con Z-sottogruppi di Sylow quaternionali. Allora G è un gruppo di Chevalley su GF(q), q dispari, oppure G è

isomorfo a M_{11} o a M_{12}.)

Un sottogruppo A di un gruppo finito G si dice *standard* se soddisfa le condizioni seguenti (Aschbacher (1975)): i) A è quasisemplice; ii) $[A,A^g] \neq 1$ per ogni $g \in G$; iii) $K = CG(A)$ è strettamente immerso in G; iv) $N_G(K) = N_G(A)$. (Segue dalla definizione che A è una componente del centralizzante di ogni involuzione di K.)

Sia ora G un gruppo semplice "of component type", i.e. si supponga che G contenga un'involuzione z, tale che $C_G(z)/O(C_G(z))$ abbia una componente A. Per abuso di linguaggio, si dirà che A è una componente di G; se poi A è un sottogruppo standard di G, si dirà che A è una *componente standard* di G. L'importanza del concetto di sottogruppo standard risiede nel fatto che:
1) se G è un gruppo semplice "of component type", allora G contiene una componente standard (salvo alcune note eccezioni, fra i gruppi di Chevalley con rango (di Lie) basso) (In ciò consiste il "Component Theorem" di Aschbacher-Foote, dimostrato sotto l'ipotesi della validità della cosiddetta B-congettura di Thompson da Achbacher (1975). Foote (1976).)
2) Per ogni gruppo quasisemplice noto H, è stato tecnicamente possibile, sotto opportune ipotesi aggiuntive legate alla natura induttiva del teorema generale di classificazione dei gruppi semplici, determinare i gruppi finiti contenenti una componente standard A, con A/Z(A) isomorfo a H.

A proposito di 2), la situazione generale che si presenta è la seguente: Se G è un gruppo finito, con O(G) = 1, A è un sottogruppo standard di G, e L(G) è il sottogruppo generato

dalle componenti di G. si hanno tre possibilità: 1) A è normale in G; ii) $L(G) = X \times X^z$, ove $X \simeq A$ è semplice, z è un'involuzione. e $\langle z \rangle = C_G(A)$; iii) $A \subseteq L(G)$ e $L(G)$ è semplice.

Esaminando le configurazioni possibili, si è sovente condotti a provare la non-esistenza di gruppi semplici contenenti una componente standard di tipo assegnato. Ciò accade, ad esempio, nel caso dei grandi gruppi di Mathieu, per i quali si hanno i risultati seguenti:

a) Sia G un gruppo finito, con O(G) = 1. e sia $A \simeq M_{24}$ una componente standard di G. Allora $L(G) \simeq M_{24}$, oppure $L(G) \simeq M_{24} \times M_{24}$. (Egawa (1981). J.Koch).

b) Sia G un gruppo finito, con O(G) = 1, e sia $A \simeq M_{23}$ una componente standard di G. Allora $\langle A^G \rangle = A$, oppure $\langle A^G \rangle \simeq A \times A$. (Finkelstein (1976)).

c) Sia G un gruppo finito, con O(G) = 1, e sia A una componente standard di G, con $|Z(A)|$ dispari e $A/Z(A) \simeq M_{22}$. Allora A è semplice, e $\langle A^G \rangle = A$. oppure $\langle A^G \rangle \simeq A \times A$. (Finkelstein (1977A)) (c) risolve il caso $A \simeq M_{22}$ ed esclude il caso $A \simeq C_3 \cdot M_{22}$. Poiché il moltiplicatore di Schur di M_{22} è ciclico di ordine 12 (cfr. 511). si presentano anche i casi in cui $|Z(A)| = 2,4,6,12$. Anche tali casi sono stati investigati, escludendo l'esistenza di gruppi con una componente standard cosiffatta (da Harada, e usando le tecniche di Finkelstein (1977B)).)

Nel caso di M_{11} e di M_{12}, si hanno i risultati seguenti:

d) Sia G un gruppo finito, con F*(G) semplice, e sia $A \simeq M_{11}$ una componente standard di G. Allora $F^*(G) \simeq Mc$ (e $G \simeq Aut(Mc)$).

(cfr. Seitz (1980); non siamo stati in grado di individuare una referenza bibliografica precisa. Si noti che $Aut(Mc) = [Mc]C_2$, e, se z è un'involuzione in $Aut(Mc) \setminus Mc$. il centralizzante di z in Mc è un sottogruppo massimale di Mc, isomorfo a M_{11}.)

e) Sia G un gruppo finito, con F*(G) semplice, e sia A una componente standard di G, con $A/Z(A) \simeq M_{12}$. Allora A è semplice, e $F^*(G) \simeq Co_3$, Sz (e $G \simeq Co_3$, Aut(Sz)). (Finkelstein. Solomon (1979))

(In Co3 il centralizzante di un'involuzione non-centrale è isomorfo a $C_2 \times M_{12}$. M_{12} è standard in Co_3; Co3 è stato caratterizzato mediante la struttura del centralizzante sopraddetto da Yoshida (1974) (cfr. §13). In $Aut(Sz) = [Sz]C_2$ vi è una classe di involuzioni, con centralizzanti isomorfi a $Aut(M_{12})$, e M_{12} standard in Aut (Sz).)

F) A conclusione di questo paragrafo, menzioniamo alcuni interessanti risultati in teoria di Galois:

Matzat (1979B) ha provato che M_{11} è il gruppo di Galois di un polinomio sul campo numerico Q(m). Più precisamente, Matzat ha dimostrato che esiste un'estensione di Galois del campo Q(m)(t) con gruppo di Galois M_{11}; di qui, specializzando t con opportuni elementi di $Q(\sqrt{-11})$, si ottengono delle estensioni di Galois di $Q(\sqrt{-11})$ con gruppo di Galois. Mll. (Ad esempio, posto $\theta = +\sqrt{-11}$, $\alpha = -33+12\theta$, $\beta = -(1/3)(253+98\theta)$, $\gamma = -11(107+34\theta)$, il polinomio $f(x) = (x^2+\alpha)^4(x^3+11x^2+\beta x+\gamma) - \delta$ ha gruppo di Galois M_{11} se $\delta \equiv 1 (\mathrm{mod}\,(1/2)(3+\theta)(6-\theta))$.) Le tecniche usate da Matzat (sviluppate in Matzat (1979A)) consentono anche di provare,

tranne che nel caso di M_{11} e M_{12}, che i gruppi di permutazioni primitivi non-risolubili di grado minore di 16, sono gruppi di Galois di polinomi sul campo razionale Q. Recentemente Matzat ha anche dimostrato (in Matzat (1983)) che M_{12} è il gruppo di Galois di un polinomio su $Q(\sqrt{-5})$, e $Aut(M_{12})$ è il gruppo di Galois di un polinomio su Q. (Matzat (1983) esamina più in generale i gruppi semplici sporadici di ordine $<10^6$, provando ad es. che $J_2(Aut(J_2))$ è il gruppo di Galois di un polinomio su $\mathbb{Q}(\sqrt{5})(\mathbb{Q})$. I risultati sono provati combinando le tecniche di Matzat (1979A) con le informazioni contenute nelle tavole dei caratteri dei gruppi in questione.)

Non è noto se M_{11} e M_{12} siano gruppi di Galois di polinomi su $\mathbb{Q}$. Nulla poi ci risulta sia stato ottenuto riguardo ai grandi gruppi di Mathieu.

§ 9. 1 GRUPPI DI MATHIEU COME GRUPPI DI PERMUTAZIONI ALTAMENTE TRANSITIVI.

1) Si assuma la classificazione dei gruppi semplici finiti, o più esattamente la conoscenza, che da quella deriva, di tutti i gruppi 2-transitivi. Allora si può enunciare il teorema seguente, che caratterizza pienamente i gruppi di Mathieu come gruppi multiplamente transitivi:

TEOREMA. Sia G un gruppo di permutazioni k-transitivo su un insieme finito Ω, con $k \geq 4$. Si supponga $G \neq AC$: allora $k < 6$. e si hanno le seguenti possibilità:

i) $k = 4, |\Omega| = 11$. $G = M_{11}$

ii) $k = 4, |\Omega| = 23$, $G = M_{23}$

ii) $k = 5, |\Omega| = 12$, $G = M_{12}$

iv) $k = 5, |\Omega| = 24$, $G = M_{24}$.

In tutti i casi G è un gruppo di permutazioni univocamente determinato che opera in modo "naturale" su Ω, salvo che in iii): M_{12} ha infatti (cfr. §3.) due distinte rappresentazioni di permutazione "naturali" come gruppo S-transitivo di grado 12.

Non sembra possibile, al momento attuale, ottenere il teorema precedente prescindendo dall'ispezione dell 'elenco di tutti i gruppi 2-transitivi. L'intenso sforzo di ricerca sviluppato negli ultimi decenni si è però concretizzato in numerosi risultati parziali di grande interesse intrinseco (a volte con significativo impatto sullo stesso progetto della classificazione dei gruppi semplici). Rimandando alle "surveys di Shult (1981) e Cameron

(1981) per l'analisi generale dei gruppi Z-transitivi, in questo paragrafo illustreremo solo i risultati più strettamente legati al contesto dei gruppi altamente transitivi.

Il primo risultato è classico, e si deve a C.Jordan:

TEOREMA (Jordan (1872)). Sia G un gruppo di permutazioni sottilmente k-transitivo su Ω, con $k \geq 4$. Allora: i) k=4, e $G=S_4, S_5, A_6, M_{11}$; ii) k=5, e $G=S_5, S_6, A_7, M_{12}$; iii) $k \leq 6$, e $G = S_k, S_{k+1}, A_{k+2}$. (In tutti i casi, G opera in modo naturale su Ω).

La dimostrazione conduce a una effettiva costruzione di M_{11} e M_{12}. Si prova anzitutto che, se k=4 e $|\Omega| > 7$, necessariamente $|\Omega| = 11$. M_{11} è identificato mediante una sequenza di estensioni transitive: se $\Omega = GF(11) = \{0,1,\ldots,10\}$, lo stabilizzante di 3 punti di Ω, ad es. $G_{0,9,10}$, è necessariamente isomorfo al gruppo dei quaternioni Q_8; $G_{9,10}$ è allora un gruppo di Frobenius di ordine 9.8, e a meno di equivalenza si può supporre $G_{9,10} = \langle a,b,u,v \rangle$, ove $a = (1,3,2,6)(4,5,8,7)$, $b = (1,4,2,8)(3,7,6,5)$, $u = (0,1,2)(3,4,5)(6,7,8)$, $v = (0,3,6)(1,4,7)(2,5,8)$, e $G_{0,9,10} = \langle a,b \rangle$. Dopo di ciò, aggiungendo la permutazione $x = (0,9)(3,4)(5,7)(6,8)$, univocamente determinata a meno d'equivalenza, si ottiene G_{10}; e infine si ottiene G aggiungendo a $G_{10} = \langle a,b,u,v,x \rangle$ la permutazione $y = (0,10)(3,5)(4,8)(6,7)$, anch'essa univocamente determinata a meno d'equivalenza. Se k=5, e $|\Omega| > 7$, allora necessariamente $|\Omega| = 12$. Se $\Omega = GF(11) \cup \{\infty\}$, G si ottiene aggiungendo a $M_{11} = G_\infty$ la permutazione $z = (0,\infty)(3,6)(4,5)(7,8)$. In particolare dunque, il procedimento porge

generatoriesplicitiper M_{11} e M_{12}.

Come è ben noto, i gruppi di permutazioni sottilmente 3-transitivi sono stati completamente determinati in un classico teorema di Zassenhaus (1936) (cfr. anche Tits (1949), Huppert (1962)): essi sono i) i gruppi projettivi $PGL(2,q)$ nella loro azione naturale su $PG(1,q)$; ii) i gruppi H(q) menzionati in §8.,B). Gorenstein.Hughes (1961) hanno considerato gruppi k-transitivi, con $k \geq 3$, in cui lo stabilizzante di k+l punti è l'identità. Si ha in particolare il seguente:

TEOREMA. Sia G k-transitivo su Ω, ma non sottilmente k-transitivo su Ω, con $k \geq 3$. Se per. ogni $\Delta \subseteq \Omega$, con $|\Delta|=k+1$, è $G_\Delta = 1$, allora: i) k=3 e $G=S_5, A_6, P\Gamma L(2,2^p)$ (p primo), M_{11}; ii) k=4 e $G=S_6$, A_7, M_{12}; iii) $k \geq 5$ e $G = A_{k+3}$, S_{k+2} (tutti i gruppi G nelle loro azioni usuali).

(Menzioniamo qui anche un risultato di Corbas (1965): Sia G S-transitivo su Ω, lo stabilizzante di 4 punti abbia ordine ≤ 2, e solo l'identità fissi 5 punti. Se esistono 4 punti $\alpha, \beta, \gamma, \delta \in \Omega$ tali che sia $1 \neq G_{\alpha,\beta,\gamma,\delta} \neq G_{\alpha,\beta,\gamma} \neq 1$, allora $|\Omega| = 12$, e $G = M_{11}$.)

Il teorema di Jordan (1872) è stato generalizzato da M.Hall, argomentando secondo le stesse linee:

TEOREMA (Hall (1954)). Sia G un gruppo di permutazioni. 4-transitivo su Ω. Se lo stabilizzante in G di 4 punti di Ω ha ordine dispari, allora $G = S_4, S_5, A_6, A_7, M_{11}$ (tutti nelle loro azioni usuali).

Una generalizzazione del teorema di Jordan è da considerarsi

anche il seguente:

TEOREMA (Suzuki (1966)). Sia G un gruppo di permutazioni 4-transitivo su Ω, e sia $\Gamma \subseteq \Omega$, $|\Gamma|=2$. Se G_Γ contiene un sottogruppo normale, regolare su $\Omega \setminus \Gamma$, $G=S_4, S_5, S_6, A_6, M_{11}$.

Ne discende il:

COROLLARIO. Sia G $(k+2)$-transitivo su Ω, con $k \geq 2$, e $G \not\supseteq A_\Omega$.

Se lo stabilizzante di k punti contiene un sottogruppo normale, regolare sui punti rimanenti, allora $k=2,3$ e $G=M_{11}, M_{12}$. (Per $k=3$, il risultato è provato anche da Nagao (1966)).

Il teorema di Hall (1954) è servito a sua volta da punto di partenza per vaste generalizzazioni, in direzioni diverse ma strettamente collegate. Vi ha contribuito in massima misura la scuola giapponese, con risultati tanto più pregevoli in quanto generalmente ottenuti applicando in modo ingegnoso metodi elementari di teoria dei gruppi di permutazioni.

Nei seguenti punti' 1) e 2). salvo avviso contrario, G è un gruppo 4-transitivo su Ω, e $H=G_\Delta$, con $\Delta \subseteq \Omega$, $|\Delta|=4$.

1) Notevoli risultati sono stati ottenuti considerando i 2-sottogruppi di Sylow di H. Se $P \in \mathrm{Syl}_2 H$, $\Phi = \mathrm{Fix}\{P\}$, $N_G(P)$ opera su Φ come un gruppo 4-transitivo (per il classico "lemma di Jordan-Witt", cfr. Witt (1938A)), soddisfacente alle ipotesi di Hall (1954). Pertanto $N_G(P)$ opera su Φ come $S_4, S_5, A_6, A_7, M_{11}$ nelle loro azioni naturali: in particolare $|\Phi| = 4,5,6,7,11$.

Naturalmente, il caso $P=1$ è quello trattato da Hall (1954). Oyama (1969,1970) ha provato che, se $|\Phi|=6,11$, allora $P=1$

e $G=A_6, M_{11}$, rispettivamente. Pertanto, se $P\neq 1$, $|\Phi|=4,5,7$.
Oyama (1973) ha poi provato che, se $|\Phi|=7$, allora $G=A_7$, oppure $G=M_{23}$ (e $|P|$ è rispettivamente 1 0 2^4). Restano così insoluti i casi $P \neq 1, |\Phi| = 4,5$.

Si osservi che, posto $\Sigma = Fix\{H\}$, è ovviamente $\Sigma \subseteq \Phi$, e $N_G(H)$ opera su Σ come un gruppo sottilmente 4-transitivo, cioé come S_4, S_5, A_6, M_{11} nelle loro azioni 'naturali. Nagao (1965) ha provato che, se $N_G(H)^{\Sigma} = S_5, A_6, M_{11}$, allora $N_G(H)^{\Sigma} = G$. In particolare. se $G\neq S_5, A_6, M_{11}$, $\Sigma = A$ ha cardinalità 4. Percib. più esattamente, restano insoluti i casi in cui $P\neq 1, |\Sigma|=4$, $|\Phi|=4,5$.

Vari risultati presuppongono condizioni sulla struttura e/o sull'azione di P. Sia $P\neq 1$:

a) se P è semiregolare su $\Omega \setminus \Phi$, allora P è regolare su $\Omega \setminus \Phi$, e $G=S_6, S_7, A_8, A_9, M_{12}, M_{23}$ (Nagao,Oyama (1965), Oyama (1968)).

b) se P è abeliano, allora P è regolare su $\Omega\setminus\Phi$, e $G = S_6, S_7, A_8, A_9, M_{23}$ (Noda.Oyama (1969), Oyama (1971)).

c) se P è transitivo su $\Omega\setminus\Phi$, allora $G=S_{2^k+4}, S_{2^k+5}$ $(k \geq 1)$; A_{2^k+4}, A_{2^k+5} $(k \geq 2)$; M_{12}; M_{23} (Oyama (1974)).

d) se $\Omega|$ è pari e $\Phi = Fix\{Z(P)\}$, allora $G=S_n$, $n \geq 6$; A_n, $n \geq 8$ e $n \equiv 0(4)$; M_{12} (Oyama (1974)).

e) se $\Omega|$ è pari, e per ogni $\alpha \in \Omega \setminus \Phi$, $P_\alpha = 1$ oppure $P_\alpha \neq 1$ è semiregolare su $\Omega \setminus Fix\{P_\alpha\}$: allora $G=S_6, S_8, A_8, A_{10}, M_{12}, M_{24}$ (Oyama (1974)).

2) Altri risultati sono legati a particolari condizioni sull'ordine o sulla struttura di H, o sull'azione di H su $\Omega \setminus \Delta$.

Un primo risultato, che pone restrizioni su $|\Omega|$, risale a Parker (1959): Se $G \not\supseteq A_\Omega$, allora per ogni primo dispari che divide $|H|$ si ha $|\Omega| = 4(p+1)$, oppure' $|\Omega| \geq 5p$.

Oyama (1976) ha provato che, se $3 \nmid |H|$, $G = S_4, S_5, S_6, A_6, M_{11}, M_{12}$ (Se $|H|$ è dispari, Hall (1954) implica $G = S_4, S_5, A_6, M_{11}$; se $|H|$ è pari, $G = S_6, M_{12}$).

Yoshizawa (1977) ha poi provato che, se H è un gruppo di Frobenius, $G = S_7, A_8, M_{23}$.

Sempre Yoshizawa (1978A), ispirandosi a tecniche di Oyama (1976), ha dimostrato il seguente:

TEOREMA.. Sia G 5-transitivo su Ω, $\Gamma \subseteq \Omega$, $|\Gamma| = 5$. Se G_Γ ha un 2-sottogruppo di Sylow normale $\neq 1$, allora $G = S_7, A_9, M_{24}$. (Un risultato più debole era già stato ottenuto da Noda (1967) nell'ambito dello studio dei gruppi o-transitivi: cioè che, se G è o-transitivo su Ω, $G = S_7$ o A_9).

[Cogliamo qui l'occasione di ricordare, senza entrare in dettagli, che sulla struttura dei gruppi o-transitivi (problema banalizzato dal Teorema enunciato all'inizio di questo paragrafo) esiste una letteratura abbastanza vasta, soprattutto di scuola giapponese.

La non-esistenza di gruppi 6-transitivi non banali è stata legata alla "congettura di Schreier", secondo la quale, se G è un gruppo semplice finito, Aut G/Inn G è risolubile (ciò che è facilmente verificabile, sulla base della classificazione dei gruppi semplici). Vale il seguente:

TEOREMA (Wielandt (1960), Nagao (1966), Suzuki (1966), O'Nan (1975)). Se G è un gruppo a.-transitivo su Ω, e la congettura di Schreier è valida per i fattori di composizione dei sottogruppi propri di G, G contiene A_Ω.

Si hanno inoltre numerosi risultati di natura parziale sui gruppi o-transitivi, e più in generale sui gruppi 2p-, (2p+1)-, 0 SP-transitivi. con p primo dispari: cfr. Noda (1967), Bannai (1973,1974,1975,1976A,1976B), Miyamoto (1974). Yoshizawa (1978B,1979A,1979B,1980). Si tratta, ad esempio, di risultati legati al comportamento dello stabilizzante di 2p punti in un gruppo 2p-transitivo, analoghi a quelli legati al comportamento di H in un gruppo 4-transitivo. E a titolo esemplificativo citiamo il

TEOREMA (Bannai *(1976A). **Se G** è 2p-transitivo **su** Ω,* con p dispari, e se G_Γ, $|\Gamma| = 2p$, è un p'-gruppo, allora $G \supseteq A_\Omega$. (Miyamoto (1974) prova il risultato analogo per G 3p-transitivo su Ω).]

Si consideri ora l'azione di H su $\Omega \setminus \Delta$. Se H ha un'orbita di lunghezza 1 su $\Omega \setminus A$, allora, in virtù di Nagao (1965). $G = S_5, A_6, M_{11}$. Oyama (1978) ha provato che, se H ha un'orbita di lunghezza 2 su $\Omega \setminus \Delta$, $G = S_6$.

Conviene menzionare anche risultati di carattere più generale dimostrati da E.Bannai. Bannai (1972, 1975) ha provato che, se G è un gruppo k-transitivo su Ω, $G \not\supseteq A_\Omega$, e G_Δ $(\Delta \subseteq \Omega, |\Delta| = k)$ ha un'orbita di lunghezza m su $\Omega \setminus \Delta$, allora k è limitato da una funzione dipendente solo da m. Più precisamente, tenendo

anche conto di Oyama (1978): se $m \leq 2$, allora $k < 6$. in virtù di Nagao (1965). del fatto che M_{11} non ammette due successive estensioni transitive, e di Oyama (1978) (e in tal caso, se $k = 4$, $G = M_{11}$; se $k = 5$, $G = M_{12}$). Se $m > 2$, allora $k < p$; ove p è il più piccolo numero primo strettamente maggiore di m.

3) Seguendo Buekenhout (1972A), diremo che un gruppo di permutazioni G su Ω, di ordine pari, è un (k.r)-gruppo se i) G è k-transitivo su Ω, $k \geq 1$; ii) r è il massimo numero di punti di Ω fissati da un'involuzione di G. (Si noti che $|\Omega| \equiv r(2)$, e che un'estensione transitiva di un (k.r)-gruppo è un (k+1,r+1)-gruppo, e viceversa).

Si può allora enunciare il teorema di Hall (1954) nel modo seguente: se G è un (4,r)-gruppo, con $r \leq 3$, $G = S_4, S_5, A_6, A_7, M_{11}$. In questa ottica, una prima, fondamentale generalizzazione si deve a Nagao (1968), il quale ha provato che, se G è un (4,r)-gruppo, con $r \leq 5$, allora $G = S_i$, (i=4,5,6,7); A_i, (i=6,7,8, 9); $M_{11}; M_{12}$. (In particolare, se r=4,5 G è 5-transitivo su Ω).

Oyama (1968.1974) ha generalizzato i risultati di Hall e Nagao nel modo seguente:

TEOREMA. Sia G un (4,r)-gruppo, e sia Π un sottoinsieme di Ω di cardinalità r. Se $G_{[\Pi]} = N_G(G_\Pi)$ opera su Π come il gruppo simmetrico 0 il gruppo alterno su Π, i.e. $G^{\Pi}_{[\Pi]} \geq A^{\Pi}_{\Pi}$, allora $G = S_i$, $i \geq 4$; A_i, $i \geq 6$; M_i, i=11,12,23,24 (nelle rappresentazioni usuali).

(Si noti che, nelle ipotesi del Teorema, $G^{\Pi}_{[\Pi]} \supseteq A_{\Pi}$ equivale a $N_G(Q)^{\Pi} \supseteq A_{\Pi}$, con $Q = Syl_2 G_{\Pi}$, poiché $G_{[\Pi]} = G_{\Pi} \cdot N_G(Q)$).

Hiramine (1977) ha esteso a sua volta il risultato di Oyama. provando che, se G è un (4,r)-gruppo, Π è un sottoinsieme di Ω di cardinalità r, e $G_{[\Pi]}$ opera su Π come un gruppo 4-transitivo "noto" (i.e. S_r, A_r, o un gruppo di Mathieu M_r, r = 11,12,23,24), allora G è un gruppo 4-transitivo "noto".

In altra direzione, il teorema di Oyama ha trovato una radicale generalizzazione in un risultato di Rowlinson (1977), che indebolisce l'ipotesi di 4-transitività fino a richiedere solo la semplice transitivita, e classifica completamente gli (l.r)-gruppi semplici con la proprietà $N_G(G_{\Pi})^{\Pi} \supseteq A_{\Pi}$.

Per la loro importanza intrinseca, oltre che per meglio intendere il risultato di Rowlinson. conviene fare qualche cenno ai risultati acquisiti sui (k.r)-gruppi. Salvo che in alcuni casi di particolare interesse, non daremo elenchi dei (k,r)-gruppi per i valori studiati di k e r, rimandando per questi ai lavori via via citati. Notiamo inoltre che la maggior parte dei risultati conseguiti differiscono per un aspetto sostanziale da quelli ottenuti dalla scuola giapponese nel contesto dei gruppi 4-transitivi. poiché presuppongono in genere profondi teoremi di caratterizzazione dei gruppi semplici finiti, in funzione dell'ordine e/o della struttura dei 2-sottogruppi di Sylow.

Gli (l.l)-gruppi (i.e. i gruppi transitivi in cui ogni involuzione fissa esattamente un punto) sono stati determinati da

Bender (1971), in un lavoro oggi celebre per l'impatto che il concetto in esso formulato, quello di sottogruppo "fortemente immerso" ("strongly embedded subgroup") ha avuro sulla strategia della classificazione dei gruppi semplici. Gli (l,l)-gruppi sono infatti precisamente i gruppi finiti G che contengono un sottogruppo fortemente immerso. i.e. un sottogruppo proprio M, con $|M|$ pari e $|M \cap M^g|$ dispari per ogni $g \in G \setminus M$. Gli (l,l)-gruppi semplici, oggi noti come "gruppi di Bender", sono i seguenti: $PSL(2,2^n)$; i gruppi di Suzuki $Sz(2^{2n+1})$.

Bender (1968) aveva precedentemente classificato i (2,0)-gruppi, mentre i (2,2)-gruppi erano stati classificati da Hering (1968), e i (2,3)-gruppi da King (1969).

Fondandosi sul risultato di Bender (1971), Buekenhout (1972A) ha determinato tutti gli (1,3)-gruppi, e dopo di ciò ne ha determinato le estensioni transitive, i.e. i (2,4)-gruppi.

Più precisamente: i (2,4)-gruppi sono stati classificati da Noda (1971), nel caso in cui $8 \nmid |\Omega|$; Buekenhout (1972B) ha completato la classificazione nel caso In cui $8 \nmid |\Omega|$. In particolare i (2,4)-gruppi semplici sono M_{12} nelle sue azioni usuali come gruppo S-transitivo di grado 12. M_{11} nella sua azione S-transitiva di grado 12, $PSU(3,3)$ nella sua azione sui 28 punti di un unital, e A_8 nella sua azione usuale.

Buekenhout (19728) ha anche provato che, se G è un k;k+2)-gruppo con $k \geq 3$, allora $G = S_{k+4}$; A_{k+6}; $P\Gamma L(2,2^4)$ 0 un suo sottogruppo di indice 2 (tutti nelle azioni suali).

Rowlinson (1972,1973) ha classificato i gruppi semplici contenenti una sola Classe di involuzioni, che sono rappresentabili come (1,r)-gruppi con $1 \leq r \leq 7$ (in particolare, per $r=2$ gli argomenti

usati sono validi anche nel caso vi sia più di una classe di involuzioni, e sono quindi determinati tutti gli (1,2)-gruppi semplici). In una serie di lavori, Buekenhout e Rowlinson hanno poi studiato gli (1,4)-gruppi, centrando l'analisi sul tipo delle involuzioni e sulla struttura dei 2-sottogruppi di Sylow (Rowlinson (1974). Buekenhout, Rowlinson (1974), Buekenhout, Rowlinson (1976)). In particolare hanno determinato gli (1,4)-gruppi semplici: se G è un gruppo semplice rappresentabile come (1,4)-gruppo, ogni sezione di G ha L-rango ≤ 4; inoltre $|Syl_2G| \leq 2^8$, oppure ogni sezione di G ha 2-rango ≤ 2. Allora gli (1,4)-gruppi semplici sono facilmente elencabili sulla base di Gorenstein, Harada (1974). e del fatto che i gruppi semplici con $|Syl_2G| \leq 2^{10}$ sono noti (Beisiegel (1977). Stingl (1976)).

Anche gli (1.x-)-gruppi semplici con r=5,6,7 sono "noti", nel senso che sono da ricercarsi fra i gruppi semplici in cui ogni sezione ha 2-rango ≤ 4, oppure $|Syl_2G| \leq 29$, oppure contengono un sottogruppo fortemente immerso (cfr. Rowlinson (1976)). In particolare, Hiramine (1978) ha provato che un (1.5) -gruppo semplice contiene una sola classe di involuzioni, oppure ogni sua sezione ha 2-rango ≤ 4 e $|Syl_2G| \leq 2^8$; e usando Rowlinson (1972. 1973) ha dato un elenco completo degli (1,5)-gruppi semplici. (Come conseguenza di questo risultato, e dei risultati precedenti sul (2,r)-gruppi, r $\leq$ 4, Hiraminr è poi in grado di classificare i (2,5)-gruppi).

Possiamo ora enunciare il risultato di Rowlinson (1977) che generalizza Oyama (1974):

TEOREMA. Sia G un (l,r)-gruppo semplice, con $r \geq 5$, e sia Π un sottoinsieme di Ω di cardinalità r. Se $G^{\Pi}_{[\Pi]} \supseteq A_{\Pi}$, allora G è uno dei gruppi seguenti:

i) $M_{21}, M_{22}, M_{23}, M_{24}$ nelle loro azioni usuali (r=5,6,7,8);

ii) A_{r+4};

iii) J_1, il primo gruppo di Janko, rappresentato sui laterali del normalizzante di un l-sottogruppo di Sylow (r=5);

iv) Mc, il gruppo di McLaughlin, rappresentato sui laterali del ricoprimento $C_2 \cdot A_7$ (r=8).

(Rowlinson può supporre $r \geq 5$, in forza dei risultati già noti sugli (l,r)-gruppi con $r \leq 4$.)

Nelle ipotesi drl Teorema, G_{Π} è strettamente immerso in G. (Si ricordi (cfr. §8,E)) che un sottogruppo proprio K di un gruppo G si dice strettamente immerso in G, se $|K|$ è pari e $|K \cap K^g|$ è dispari per ogni $g \in G \setminus N_G(K)$. Si tratta, quindi, di una generalizzazione del concetto di sottogruppo fortemente immerso). Rowlinson può così applicare i fondamentali risultati di Aschbacher (1975,1976A) sui gruppi contcncnt i sottogruppi strettamente immersi, e ottenere condizioni Z-locali su G sufficienti a determinare G in forza di noti teoremi di classificazione.

II) (Un problema di Mathieu). Si consideri il gruppo projettivo PSL(2,p), p numero primo, nella sua azione naturale su Ω = PG(1,p); e sia G un gruppo di permutazioni su Ω, tale che sia $PSL(2,p) < G \leq A_{\Omega}$. Il problema di determinare tutti i gruppi G rosiffatti fu proposto da Mathieu (1873). Gli rsrmpi noti

UNIVERSITÀ DEGLI STUDI DIP.TO DI MATEM. LECCE

non banali sono: i) $PSL(2,7) < AGL(3,2) < A_8$; ii) $PSL(2,11) < M_{12} < A_{12}$; iii) $PSL(2,23) < M_{24} < A_{24}$.

Neumann (1976) ha provato che, se $p > 7$, G è necessariamente 4-transitivo su Ω. (E Bhattacharya (1981) ha censito i gruppi $PSL(2,p)$, $7 \leq p \leq 113$, provando che, eccetto per $p=7,11,23$ e eventualmente $p=101$, $PSL(2,p)$ è massimale in A_{p+1}). Naturalmente, se si assume che tutti i gruppi 4-transitivi siano noti, il risultato di Neumann comporta che, se $p>7$ e $PSL(2,p) < G < A_\Omega$, allora $p=11$ e $G=M_{12}$, oppure $p=23$ e $G=M_{24}$.

La massimalità di $PSL(2,p)$ in A_{p+1}, per $p > 23$, può essere anche dedotta come corollario della seguente famosa congettura (la cui validità è conseguenza della classificazione dei gruppi l-transitivi):

Congettura: Sia G un gruppo di permutazioni non risolubile, 2-transitivo su un insieme Ω, e contenente un ciclo di lunghezza $n = |\Omega|$. Se $G \neq A_\Omega$, si hanno i casi seguenti:

i) $n=11$, e $G=PSL(2,11)$; ii) $n=11$, e $G=M_{11}$; iii) $n=23$, e $G=M_{23}$; iv) $|\Omega| = (q^n-1)/(q-1)$, e G è un gruppo di collineazioni di $PG(n-1,q)$ contenente $PSL(n,q)$.

(In i), $PSL(2,11)$ opera su Ω in una delle azioni 2-transitive, corrispondenti alle due classi di sottogruppi coniugati isomorfi ad A_5; in ii), iii), iv) G opera in modo "naturale" su Ω: in particolare, in iv) G opera sull'insieme dei punti (o sull'insieme degli iperpiani, se $n>2$) di $PG(n-1,q)$).

III) Uno dei filoni fondamentali dell'indagine dei gruppi G, 2-transitivi su un insieme Ω, consiste nell'analisi della

struttura normale dello stabilizzante G_α ($\alpha \in \Omega$). (Cfr. Shult (1981) per un'illuminante "survey"). In tale contesto si situano le seguenti caratterizzazioni di M_{11} e M_{22}:

TEOREMA (Hiramine (1979A)) Sia G un gruppo di permutazioni 2-transitivo su un insieme Ω, con $|\Omega|$ pari, e si supponga che G_α contenga un sottogruppo normale isomorfo a PSL(2,q), per qualche q dispari. Allora G ha un sottogruppo normale regolare, oppure: i) $\Omega = 6$, q=5, e $G=A_6, S_6$; ii) $|\Omega|=12$, q=11, e $G=M_{11}$ (nella sua azione 3-transitiva sui laterali di PSL(2,11)).

TEOREMA (Hiramine (1979B)). Sia G un gruppo di permutazioni 2-transitivo su un insieme Ω, con $|\Omega|$ pari, e si supponga che G_α contenga un sottogruppo normale isomorfo a $PSL(3,2^n)$, per qualche n. Allora G ha un sottogruppo normale regolare. oppure: $|\Omega|=22$, n=2, e $G=M_{22}$, o $Aut(M_{22})$.

IV) Menzioniamo, infine, una caratterizzazione permutazionale di M_{11} e M_{12}, che appare di natura piuttosto tecnica, e si riconduce alla determinazione della struttura dei 2-sottogruppi di Sylow.

TEOREMA(Fomin (1979)). Sia G un gruppo semplice finito, transitivo su un insieme Ω. Si supponga che esista un sottoinsieme A di Ω, di cardinalità $k \geq 2$, per il quale sia $G_\Delta \neq 1$, e che per ogni sottoinsieme Γ di Ω di cardinalità k+1 sia $G_\Gamma = 1$. Se i) $|G_\Delta$ è pari: ii) $N_G(G_\Delta)/G_\Delta \simeq S_k$; iii) GA è contenuto propriamente nello stabilizzante di certi k-l punti di Ω; iv) per ogni $\Pi \subseteq \text{Fix}\{G_\Delta\}$, $|\Pi| = k$, si ha $G_\Pi = G_\Delta$: allora

k < 4, e G è equivalente come gruppo di permutazioni su Ω a uno dei gruppi seguenti:

a) PSL(2,q), $q \equiv 1(4)$, nell'azione naturale su PG(1,q);

b) A_5 nella sua azione sulle coppie non ordinate (α,β) $(\alpha \neq \beta \in \{1,2,3,4,5\})$;

c) PSL(2,11), in una delle 2 azioni 2-transitive di grado 11;

d) M_{11}, nella sua azione naturale come gruppo 4-transitivo di grado 11. o nella sua azione 3-transitiva di grado 12 (sui laterali di PSL(2,11));

e) M_{12}, in una delle due rappresentazioni naturali di grado 12.

(Tutti i gruppi elencati soddisfano le ipotesi del Teorema. In particolare, in d) k=3,4; in e) k=4).

§10. GENERATORI E RELAZIONI

Generatori per i gruppi di Mathieu si ottengono sia nelle costruzioni di tali gruppi come estensioni transitive (Witt (1938A), cfr. §2.), che nelle loro caratterizzazioni come gruppi multiplamente transitivi (Jordan (1872), Hall (1959), cfr. §9). Generatori ottenuti per tale via sono riportati nella maggior parte dei libri di teoria dei gruppi (e.g. Hall (1959). Scott (1964). Zappa (1970). Robinson (1982)). E' possibile derivarne presentazioni astratte dei gruppi di Mathieu, che sono state esplicitamente calcolate da Todd (1970). Queste e altre presentazioni mediante generatori e relazioni, sono il contenuto di questo paragrafo. Esse sono generalmente ottenute usando il metodo di enumerazione dei laterali (di un sottogruppo in un gruppo) di Todd-Coxeter (cfr. ad es. Coxeter, Moser (1972), cap. 2).

M_{11}:

Sia $\Omega = \{0,1,\ldots,10\} = GF(11)$. Mathieu (1873) dà i seguenti generatori per M_{11}:

$$a = (0,1,2,3,4,5,6,7,8,9,10)$$
$$b = (4,5,3,9)(10,7,2,6)$$

e osserva che $\langle a,b^2 \rangle = PSL(2,11)$, in una "non usuale" rappresentazione di grado 11. (Questi generatori sono riprodotti in Carmichael (1937)).

Fryer (1955) dà generatori leggermente diversi: $M_{11} =$

$\langle a, b_1, b_2 \rangle$, con bl = (4,5,3,9)(10,8,6,2), b_2 = (1,4,5,9,3)(10,7,6, 2,8). In effetti, a e bl bastano a generare Mll, poiché $b_2 = a^2 b_1^2 a^8 b_1^2 a^2 b_1^2$.

Coxeter. Moser (1957), p.98, ne ricavano una presentazione astratta per M_{11}:

$$M_{11} = \langle x, y, z \mid x^{11} = y^5 = z^4 = (x^4 z^2)^3 = (xyz)^3 = 1,$$
$$y^{-1} xy = x^4, z^{-1} yz = y^2 \rangle.$$

(Le relazioni sono soddisfatte per $x=a$, $y=b_2$, $z = b_1$.)

Moser (1959) dà una presentazione un poco diversa:

$$M_{11} = \langle x, y, z \mid x^{11} = y^5 = z^4 = (xz)^3 = (x^{-1} zy)^3 = 1,$$
$$y^{-1} xy = x^4, z^{-1} yz = y^2 \rangle.$$

(Le relazioni sono soddisfatte per $x=a$, $y=b_2$, $z=b$.)

Garbe.Mennicke (1964) danno una presentazione con 2 generatori:

$$M_{11} = \langle x, y \mid x^{11} = y^4 = (xy^2)^3 = (x^4 y^2 x^{-5} y^2)^2 = 1,$$
$$(x^{-4} y^{-1})^3 = x^{-1} yx^{-2} y, x^{-5} y^2 x^2 y = (x^3 y^{-1} xy)^{-1} \rangle.$$

(Le relazioni sono soddisfatte per $x=a$, $y=b$.)

Una prrsrnt az ione con 3 generatori e 6 relazioni molto semplici è infine data da Coxeter, Moser (1972):

$$M_{11} = \langle x, y, z \mid x^{11} = y^5 = z^4 = (xz)^3 = 1, y^{-1} xy = x^4, z^{-1} yz = y^2 \rangle.$$

(Le relazioni sono soddisfatte per $x=a$, $y=b_2$, z = (1,5,4,3). (2,6,10,7), e il sottogruppo $\langle x, y, z^2 \rangle = \langle x, z^2 \rangle$ è isomorfo

a PSL(2,11).)

M_{12}:

Sia $\Omega = \{0,1,\ldots,10\} \cup \{\infty\} = GF(11) \cup \{\infty\} = PG(1,11)$. **Mathieu** (1873) dà i seguenti generatori per M_{12} (riprodotti in **Carmichael** (1937)):

$$a,b,c = (0,\infty)(1,10)(2,5)(3,7)(4,8)(6,9).$$

Tali generatori si possono rappresentare come trasformazioni razionali su Ω nella forma seguente:

$$a : x \to x + 1;\ b : x \to 4x^2 - 3x^7;\ c : x \to -x^{-1}.$$

$\langle a,b^2,c\rangle$ è M_{11} nella sua rappresentazione 3-transitiva di grado 12. (Altri generatori per tale M_{11} sono dati, ad es., in Hall (1980); cfr. §5). $\langle a,c\rangle$ è PSL(2,11) nella sua azione naturale su PG(1,11): M_{12} si ottiene dunque aggiungendo a PSL(2,11) la permutazione b.

Essenzialmente la stessa generazione si ha in de **Séguier** (1904): ad $\langle a,c\rangle$ si aggiunge la permutazione b_1.

Moser (1959) ricava da a,b,c una presentazione astratta per M_{12}:

$$M_{12} = \langle x,y,z,t \mid x^{11} = y^5 = z^4 = t^2 = (xz^2)^3 = (x^{-1}zy)^3 = (tx)^3$$
$$= 1, y^{-1}xy = x^4,\ z^{-1}yz = y^2,\ y = tz^{-1}tz,$$
$$tx^2z^{-1}x^4t = x^{-1}z^2x^3z^2x^4zx^5 \rangle .$$

(Le relazioni sono soddisfatte per $x=a$, $y=b_2=b^2a^2b^2a^6b^2a^2$.

z=b,t=c.)

Garbe,Mennicke (1964) danno un'altra presentazione:

$$M_{12} = \langle x,y,z \mid x^{11} = y^4 = z^2 = (xy^2)^3 = (x^4y^2x^{-5}y^2)^2 = (x^{-1}zy)^3 =$$

$$= (xz)^3 = 1,\ (x^{-4}y^{-1})^3 = x^{-1}yx^{-2}y,\ x^{-5}y^2x^2y = (x^3y^{-1}xy)^{-1},$$

$$(x^{-1}yx^2y)^2 = zyz.\ (xyzx^{-4})^2 = x^2y^2zy \rangle .$$

(Le relazioni sono soddisfatte per x=a, y=b, z=c.)

Le due presentazioni precedenti sono dedotte da presentazioni corrispondenti di M_{11}. Leech (1969) da invece un'elegante presentazione di M_{12}, indipendente da M_{11}, e ricavata avendo in mente x = a, y=(∞,0)(1,10)(3,9)(5,8):

$$M_{12} = \langle x,y \mid x^{11} = y^2 = (xy)^3 = (x^3y)^6 = (x^3yx^6y)^3 = (x^4y)^{10}$$

$$= (x^2yx^{-2}yx^3y)^4 = 1 \rangle .$$

Si osservi che $\langle x,y \rangle = \langle x,xy \rangle$ implica che M_{12} è generato da un'involuzione e da un elemento di ordine 3. Ciò è del resto già provato in Whitelaw (1966): considerando M_{12} come gruppo degli automorfismi della configurazione di Coxeter in PG(5,3), vi si danno i seguenti generatori per M_{12}: f = = (0,6)(1,7)(2,8)(3,9)(4,10)(5,∞), g = (0,6,1)(3,7,∞)(4,8,9). Leech nota che, al contrario, M_{11} non può essere generato da un'involuzione e un elemento di ordine 3.

Anche Conway (1971) dà una nitida presentazione di M_{12}. Si considerano le trasformazioni $a : x \to x + 1$; $b_2 : x \to 4x$; $c : x \to -x^{-1}$. Esse generano PSL(2.11) su Ω = PG(1,11), e danno luogo alla presentazione: $PSL(2,11) = \langle x,y,z \mid x^{11} = y^5 = z^2 = y^{-1}xyx^{-3} =$

$= (yz)^2 = (xz)^3 = 1 >$. Si ottiene M_{12} aggiungendo ad a, b_2, c la permutazione $d = (1,9)(2,6)(4,5)(7,8)$. a, b_2, c, d soddisfano le relazioni della presentazione:

$$M_{12} = <x,y,z,t \mid x^{11} = y^5 = z^2 = t^2 = Y^{-1}xyX^3 = (xz)^3 = (xt)^3 = (yz)^2 = (yt)^2 = (tzy)^2 = 1 >.$$

(Si noti che $<x,y,z>$ e $<x,y,t>$ sono rnt ramb i isomorfi a PSL(2,11), ma sono distinti in M_{12}: $<x,y,z>$ è massimale, $<x,y,t>$ è contenuto in $(M_{12})_\infty = M_{11}$. Cfr.§7.)

Eliminando y mediante la relazione $(tzy)^2 = 1$ (equivalente a $(zt)^2 = y^2$), si ha la presentazione più semplice:

$$M_{12} = <x,z,t \mid x^{11} = z^2 = t^2 = (xz)^3 = (xt)^3 = (zt)^{10} = (zt)^{-2}x(zt)^2x^2 = 1 > .$$

Todd (1970) dà una presentazione di M_{12}, derivata dalla costruzione di M_{12} come gruppo sottilmente 5-transitivo:

Si considerano le permutazioni:

$$A = (3,4,5,10)(6,8,9,7)$$
$$B = (3,6,5,9)(4,7,10,8)$$
$$C = (2,5)(4,7)(6,8)(9,10)$$
$$D = (1,2)(4,10)(6,7)(8,9)$$
$$E = (0,1)(4,7)(6,9)(8,10)$$
$$F = (\infty,0)(4,10)(6,8)(7,9)$$

A,B,C,D,E,F soddisfano le relazioni:

i) $A^4 = B^4 = 1$, $A^2 = B^2$, $A^{-1}BA = B^{-1}$

ii) $C^2 = 1$, $A^{-1}CA = (BC)^2$, $B^{-1}CB = (AC)^2$

iii) $D^2 = 1$, $D^{-1}AD = A\text{-}1$, $D^{-1}BD = AB$, $(CD)^3 = 1$

iv) $E^2 = 1$, $E^{-1}AE = AB$, $E^{-1}BE = B^{-1}$, $CE = EC$, $(DE)^3 = 1$

v) $F^2 = 1$, $F^{-1}AF = A\text{-}1$, $F^{-1}BF = BA$, $CF = FC$, $DF = FD$, $(EF)^3 = 1$.

Queste relazioni definiscono una presentazione astratta di M_{12}: $\langle A,B \rangle$ è il gruppo dei quaternioni Q_8; $\langle A,B,C \rangle$ è un gruppo di Frobenius di ordine 9.8, 2-transitivo sui 9 laterali di $\langle A,B \rangle$; mediante l'enumerazione dei laterali, si verifica che $\langle A,B,C,D \rangle$, $\langle A,B,C,D,E \rangle$, $\langle A,B.C,D,E,F \rangle$ hanno ordine 10.9.8, 11.10.9.8, 12.11.10.9.8, e risultano quindi 3-,4-,5-transitivi di grado 10,11,12 rispettivamente. $\langle A,B,C,D,E,F \rangle$ è dunque M_{12}, $\langle A,B,C,D,E \rangle$ è M_{11}, e $\langle A,B,C,D \rangle$ è M_{10}.

M_{22}, M_{23}, M_{24} :

Sia $\Omega = GF(23) \cup \{\infty\} = PG(1,23)$. Mathieu (1873) (e Carmichael (1937)) dà i seguenti generatori per M_{24}:

a = (0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22)

b = (2,16,9,6,8)(4,3,12,13,18)(10,11,22,7,17)(20,15,14,19,21)

c = $(0,\infty)$(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)(18,14).

Tali generatori si possono rappresentare come trasformazioni razionali su Ω nella forma seguente:

$$a : x \to x + 1;\ b : x \to -3x^{15} + 4x^4;\ c : x \to -x^{-1}.$$

$\langle a,b \rangle = (M_{24})_\infty = M_{23}$. (Agli stessi generatori, più un generatore sovrabbondante di ordine 11, perviene Janko (1968B) nel caratterizzare M_{23} mediante il centralizzante di un'involuzione).

$\langle a,c \rangle$ è $PSL(2,23)$ nella sua azione naturale su $PG(1,23)$: M_{24}

si ottiene dunque aggiungendo a PSL(2,23) la permutazione b. (Questa è la generazione di de Séguier (1904).)

Molto simile è la generazione proposta in Conway (1971): M_{24} si ottiene aggiungendo a $\langle a,c \rangle = PSL(2,23)$ la permutazione

$d = (14,17,11,19,22)(20,10,7,5,21)(18,4,2,6,1)(8,16,13,9,12)$,

cioé la trasformazione $x \to 9^{\varepsilon}x^3$, ove $\varepsilon = -1$ se x è un quadrato in GF(23), $\varepsilon = 1$ in caso contrario.

Todd (1970) dà una presentazione di M_{24}, derivata dalla costruzione di M_{24} come sequenza di estensioni transitive.

Si considerino le permutazioni:

A = (4,15)(6,18)(7,8)(9,13)(10,16)(11,21)(12,19)(20,22)

B = (4,10)(6,11)(7,12)(8,19)(9,22)(13,20)(15,16)(18,21)

C = (4,20)(6,8)(7,18)(9,16)(10,13)(11,19)(12,21)(15,22)

D = (4,8)(6,20)(7,15)(9,21)(10,19)(11,13)(12,16)(18,22)

T = (5,17,14)(6,18,15)(7,12,10)(8,9,21)(11,20,19)(13,16,22)

G = (3,4)(5,22)(6,18)(7,12)(8,21)(11,19)(13,14)(16,17)

H = (2,3)(6,18)(9,21)(10,12)(11,13)(14,17)(16,19)(20,22)

I = (1,2)(6,15)(7,10)(8,11)(9,19)(14,17)(16,22)(20,21)

J = (0,1)(5,17)(6,8)(7,12)(9,15)(11,19)(16,22)(18,21)

K = (∞,0)(6,10)(7,15)(9,21)(12,18)(14,17)(16,22)(19,20)

Esse soddisfano le relazioni:

i) $A^2 = B^2 = C^2 = D^2 = 1$, $B^{-1}AB = C^{-1}AC = D^{-1}AD = A$, $C^{-1}BC = D^{-1}BD = B$, $D^{-1}CD = C$

ii) $T^3 = 1$, $T^{-1}AT = CD$, $T^{-1}BT = AD$, $T^{-1}CT = BD$, $T^{-1}DT = ABC$

iii) $G^2 = (GA)^3 = (GB)^3 = (GC)^3 = (GT)^2 = 1$

iv) $H^2 = 1$, $H^{-1}AH = A$, $H^{-1}BH = ABD$, $H^{-1}CH = AC$, $H^{-1}DH = D$,
$H^{-1}TH = T^{-1}$, $(GH)^3 = 1$

v) $I^2 = 1$, $I^{-1}AI = CD$, $I^{-1}BI = AD$, $I^{-1}CI = ABCD$. $I^{-1}DI = BCD$,
$I^{-1}TI = T^{-1}$, $I^{-1}GI = TG$, $(HI)^3 = 1$

vi) $J^2 = 1$, $J^{-1}AJ = ABC$, $J^{-1}BJ = B$, $J^{-1}CJ = C$, $J^{-1}DJ = CD$,
$J^{-1}TJ = T^{-1}$, $J^{-1}GJ = G$, $J^{-1}HJ = TH$, $(IJ)^3 = 1$

v.ii) $K^2 = 1$, $K^{-1}AK = AD$, $K^{-1}BK = CD$. $K^{-1}CK = BD$, $K^{-1}DK = D$.
$K^{-1}TK = T^{-1}$, $K^{-1}GK = TG$, $K^{-1}HK = H$. $K^{-1}IK = I$, $(JK)^3 = 1$.

Queste relazioni definiscono una presentazione astratta di M_{24}: $< A,B,C,D,T >$ è un gruppo di ordine 48. prodotto semidiretto di $<A,B,C,D> = E_{24}$ per $<T>$; $< A,B,C,D,T,G>$ è un gruppo di ordine 20.48. transitivo sui laterali di $< A,B,C,D,T>$. Mediante l'enumerazione dei laterali si trova che $<A,B,C,D,T,G,H>$, $< A,B,C,D,T,G,H,I>$, $< A,B,C,D,T,G,H,I,J>$, $< A,B,C,D,T,G,H,I,J,K>$ hanno ordine 21.20.48, 22.21.20.48, 23.22.21.20.48, 24.23.22.21.20.48, e sono quindi 2-,3-,4-, S-transitivi di grado 21,22,23,24 rispettivamente. Si conclude che essi sono isomorfi a M_{21}, M_{22}, M_{23}, M_{24}, rispettivamente.

Garbe. Mennicke (1964) danno i seguenti generatori per M_{22}:

$u = (1,4,7,21,3,13,17)(5,16,20,19,9,15,12)(6,8,11,10,14,22,18)$

$v = (2,21,10,11,3)(4,17,19,14,7)(5,6,18,22,20)(8,12,15,9,13)$.

(Si noti che $u,v \in < a,b > = M_{23}$, e $< u,v > = (M_{23})_0$).

v e $w = (uv^{-1}u)^2$ generano M_{21} $(=(M_{23})_{0,16})$. u,v,w soddisfano le relazioni della presentazione:

$$M_{22} = \langle x,y,z \quad x^7 = y^5 = z^3 = (xy)^2 = (zy)^4 = (zx)^4 = (y^{-1}zy^{-1}z^{-1}yz)^3 = 1,\ z = (xy^{-1}x)^2,\ (zy^2z)y^{-2}(zy^2z)^{-1}y^2 = yzy^{-1}z^{-1},\ x^{-2}yx^3 = y^2z^{-1}yzy^{-2}zy^2, x^2y^2x^{-3}yx^2y^{-1}x^2 = y^2z^{-1}yzy^{-1}z^{-1}yzy^2 \rangle .$$

Generatori per M_{22} sono determinati anche da Janko (1968A) nel caratterizzare M_{22} mediante il centralizzante di un'involuzione:

$M_{22} = \langle \ell,m,n \rangle$, con

$\ell = (1,2,3,4,5,6,7,8,9,10,11)(12,13,14,15,16,17,18,19,20,21,22)$

$m = (1,4,5,9,3)(2,8,10,7,6)(12,15,16,20,14)(13,19,21,18,17)$

$n = (11,22)(8,14)(4,5,3,9)(13,18,17,19)(2,16,10,15)(7,20,6,12).$

Jónsson, McKay (1976) danno una bella presentazione di M_{22}:

Si consideri la presentazione di $PSL(2,11)$, $PSL(2,11) = \langle x,y,z | x^{11} = y^5 = z^2 = Y^{-1}xyx^{-3} = (yz)^2 = (xz)^3 = 1 \rangle$ (Conway (1971)).

Posto $z = t^2$, si ottiene la srguente presentazione di M_{22}:

$$M_{22} = \langle x,y,t \quad x^{11} = y^5 = t^4 = Y^{-1}xy\bar{x}^3 = t^{-1}yty^{-2} = (xt^2)^3 = (x^5t)^5 = (x^3t)^6 = 1 \rangle .$$

($\langle x,y,t^2 \rangle$ è un sottogruppo massimale di M_{22} (cfr.§7); risulta inoltre $\langle xt, yt \rangle \cong PSL(3,4)$.)

La presentazione di Jónsson,McKay (1976) è associata alla generazione di M_{24} mediante a,c,d (Conway (1971)). Invero, se si considerano la trasformazione $h : x \to 2x \in \langle a,c \rangle$, i.e. la permutazione (1,2,4,8,16,9,18,13,3,6,12)(5,10,20,17,11,22,21,19,15,7,14), e la permutazione i=(1,18,2,4)(3,15)(5,9)(7,16,21,8)(10,12,20,13)(11,17,22,14), le relazioni sono soddisfatte per

$x=h$, $y=d$, $t=i$. Per questa scelta dei generatori, $M_{22} = \langle h,d,i \rangle = (M_{24})_{0,\infty}$ e $M_{21} = \langle hi,di \rangle = (M_{24})_{0,\infty,17}$; inoltre c coniuga h,d,i in h^{-1},d,i, realizzando un automorfismo esterno di M_{22}.

Si noti infine che la permutazione $(1,3,11,18,9,8,6)(2,4,5,14,13,10,15,22,19,21,20,16,7,12)$ coniuga h,d,i in ℓ,m^{-1},n.

Concludiamo questo paragrafo con la discussione di due questioni di minimalità:

1) Si congettura da lungo tempo, ed è ragionevole supporre, che ogni gruppo semplice finito non-abeliano sia generabile da due elementi. Ciò è noto per tutti i gruppi semplici, eccetto alcuni gruppi sporadici (e.g. il gruppo di Fischer-Griess F_1). Steinberg (1962) ha trattato il caso dei gruppi di Chevalley, chiedendosi anche se, per uno dei generatori possa sempre scegliersi un'involuzione. Ciò è senz'altro vero per i gruppi di Mathieu, e è stato verificato per ogni gruppo semplice di ordine $< 10^6$ da Cannon, McKay, Young (1979) e McKay, Young (1979).

Per i gruppi M_{11}, M_{12}, M_{22}, e M_{23}, il risultato risale a Brahana (1930) (cfr. anche, per M_{12}, Whitelaw (1966) e Leech (1969)).

Brahana (1930) da i seguenti generatori:

$M_{11} = \langle r_1, r_2 \rangle$. con $r_1 = (0,2)(1,3)(4,6)(5,7)$, $r_2 = (0,2,4,8,10)(3,7,9,5,6)$;

$M12 = \langle r_1, r_3 \rangle$, con $r_3 = (0,1,3,8,7,5,9,2,4,10,\infty)$;

$M_{22} = \langle s_1, s_2 \rangle$, con $s_1 = (0,7)(1,2)(3,4)(5,11)(8,13)(9,17)(10,12)(16,20)$, $s_2 = (0,16,8,12,4,7,17,19,20,21,22)(1,2,10,11,9,3,13,14,6,5,15)$;

$M_{23} = \langle s_2, s_3 \rangle$, con $s_3 = (1,16)(3,10)(4,13)(5,7)(6,15)(8,17)(9,12)$ (18.19).

(Per M_{24}, cfr. più avanti, al punto 2)).

Dato un gruppo G, e posto $X = \{x \in G \mid \langle x, y \rangle = G$. per almeno un $y \in G\}$, e $k = k(G) = \min_{x \in X} \{o(x))$, una (k,m,n)-*presentazione minimale* .di G è una presentazione del tipo:

$$G = \langle x, y \mid x^k = y^m = (xy)^n = 1,\ r_i(x,y) = 1,\ i \in I \rangle$$

dove m è minimale (rispetto a x).

Facendo uso di un elaboratore elettronico, **Cannon,McKay,Young** (1979) e **McKay,Young** (1979) hanno tabulato sistemi completi di. (2,m,n)-presentazioni minimali per i gruppi semplici non-abeliani di ordine $< 10^6$, e per ciascuna presentazione hanno prodotto coppie di permutazioni generatrici. In particolare hanno ottenuto: i) due (2,4,11)-presentazioni minimali per M_{11}; ii) una (2,3,10)-presentazione e due (2,3,11)-presentazioni minimali per M_{12}; iii) sei (2,4,11)-presentazioni minimali per M_{22}.

Ci limitiamo qui a riportarne alcune:

$M_{11} = \langle x, y \mid x^2 = y^4 = (xy)^{11} = 1,\ (xy^2)^6 = (xy)^2(xy^{-1})^2 xyxy^{-1} x\ y^2 xyxy^{-1} = 1 \rangle$

(e.g. $x = (0,9)(1,7)(2,10)(4,6)$, $y = (0,3,6,5)(1,10,9,8)$)

$M_{12} = \langle x, y \mid x^2 = y^3 = (xy)^{11} = 1,\ (xy^{-1}xy)^6 = ((xy)^2(xy^{-1})^2)^5 = ((xy)^4 xy^{-1} xyxy^{-1})^3 = 1 \rangle$

(e.g. x=f, y=g (Whitelaw (1966))

$M_{12} = \langle x, y \mid x^2 = y^3 = (xy)^{10} = 1.\ (xy^{-1}xy)^6 = ((xy)^4 xy^{-1} xyxy^{-1})^3 = 1 \rangle$

(e.g. $x = (1,10)(2,\infty)(3,7)(6,8)$, $y = (0,8,\infty)(1,6,10)(2,7,9)(3,4,5)$)

Nel caso di M_{22}, le presentazioni sono tabulate in modo incompleto. Una coppia minimale di (2,4,11)-generatori è, a d esempio, la seguente: x=(0,12)(2,17)(3,21)(4,18)(5,10)(6,8)(9,11)(13,14), Y = (0,5,4,19)(1,11,18,13)(2,15,9,16)(3,14)(6,20,7,12)(17.21).

2) Poiché due involuzioni il cui prodotto ha ordine finito generano un gruppo diedrale, il numero minimo di involuzioni sufficienti a generare un gruppo semplice finito non-abeliano è $\geq$ 3. Tale numero è esattamente 3 per i gruppi di Mathieu.

Il risultato è facilmente deducibile dall'esame dei sottogruppi massimali. Ma è anche immediatamente derivabile nel caso di M_{11}, considerando ad esempio i generatori di Brahana (1930) e osservando che ι_2 è contenuto in un sottogruppo diedrale di ordine 10, e nel caso di M_{12}, considerando ad esempio i generatori di Whitelaw (1966) e osservando che M_{12} contiene un'involuzione che inverte g.

Nel caso di M_{24}, si può considerare. nel sottogruppo <a,c>= PSL(2,23), i l sottogruppo diedrale D generato da c e da h. Se a D si aggiunge 1 'involuzione j = (16,22)(11,5)(1,13)(14,20)(0,8)(9,4)(15,18)(2,21)(10,6)(7,19)(17,12)(3,∞), s i ottiene un sottogruppo H = <c,h,j> transitivo su Ω, e di ordine divisibile per 7.11 (o(hj) = 21). Dall'esame dei sottogruppi massima1 i segue subito < c,h,j > = M_{24}: poiché < c,h,j > = < c,ch,j >, e ch è un'involuzione, si conclude che M_{24} è generato da 3 involuzioni. Argomentando in modo simile, si riconosce che anche M_{23} e M_{22} sono generati da 3 involuzioni. Ad esempio: le involuzioni

$(ad)^3 = (2,3)(4,15)(21,13)(14,17)(7,8)(16,12)(11,9)(10,19)$,
$(da^5)^4 = (14,7)(22,10)(19,12)(4,13)(1,8)(0,21)(5,2)(3,11)$, e
$((ad)^3)^{ah} = (6,8)(10,9)(21,5)(7,13)(16,18)(11,3)(1,20)(22,17)$
generano un sottogruppo di M_{24} transitivo su $\Omega \setminus \{\infty\}$. Segue che tale sottogruppo necessariamente coincide con $(M_{24})_\infty = M_{23}$.

Similmente $\langle (ad)^3, (da^5)^4, (ad)^{3d} \rangle = (M_{24})_{\infty,18} = M_{22}$.

Si osservi infine che $\langle hj, j \rangle$ è transitivo su Ω e ha ordine divisibile per 3.7.11. Si conclude che $\langle hj, j \rangle = M_{24}$, e $k(M_{24}) = 2$ (cfr. 1)).

ADDENDUM:

(A) La congettura menzionata in 1) è stata recentemente verificata per tutti i gruppi semplici finiti da Aschbacher. Guralnick(1984). La congettura vale in senso forte per i gruppi di Chevalley di rango 1, per i gruppi alterni, e per i gruppi sporadici. Si ha cioé il seguente:

TEOREMA. Se G è un gruppo semplice di Chevalley di rango 1, un gruppo alterno (di rango $n \geq 5$), o un gruppo sporadico, si ha $G = \langle z, t \rangle$, per qualche involuzione z e per qualche $t \in G$.

(B) Dalla Volta (1984) ha provato che ogni gruppo semplice sporadico è generabile mediante 3 involuzioni (che possono scegliersi, nella maggior parte dei casi, fra loro coniugate). (Per alcuni gruppi, tale risultato è anche deducibile da Aschbacher, Guralnick (1984). E' parimenti noto che, per varie classi di gruppi semplici di Chevalley e per i gruppi alterni, 3 è il minimo numero di involuzioni gene-

ratrici (Wagner (1978); Gillio, Tamburini (1982)). Sembra lecito congetturare che l'unica eccezione fra i gruppi semplici sia costituita dal gruppo unitario PSU(3,3), per generare il quale occorrono 4 involuzioni.

§11. CARATTERI E MODULI

A) 1 caratteri complessi dei gruppi di Mathieu sono stati calcolati da Frobenius (1904). Le corrispondenti tavole dei caratteri sono riportate, ad esempio. da Todd (1966).

James (1973) ha determinato i caratteri modulari dei gruppi di Mathieu, computando. per ogni significativo primo p, le matrici di decomposizione e le matrici di Cartan. (Hort imer (1980) ha studiato la decomposizione delle rappresentazioni di permutazione modulari dei gruppi L-transitivi. Nel caso dei gruppi di Mathieu, i risultati ottenuti sono impliciti in James (1973).)

In particolare, si osserva che: a) le rappresentazioni di permutazione "naturali" dei gruppi M_i (i=11,12,22,23,24) danno luogo a rappresentazioni complesse irriducibili di grado minimo i-l; b) il grado minimo di una rappresentazione 2-modulare non banale è 10 per M_{11}, 10 per M_{12}, 10 per M_{22} (con due rappresentazioni mutuamente duali) , 11 per M_{23} (con due rappresentazioni mutuamente duali), 11 per M_{24} (con due rappresentazioni mutuamente duali); c) il grado minimo di una rappresentazione 3-modulare non banale è 5 per M_{11} (con due rappresentazioni mutuamente duali) , 10 per M_{12} (con due rappresentazioni autoduali), 21 per M_{22}, 22 per M_{23}, 22 per M_{24}.

Varie rappresentazioni particolari dei gruppi di Mathieu (e.g. alcune delle 13 rappresentazioni a-modulari irriducibili ammesse da M_{24}) sono oggetto di studio corrente, sia per il loro interesse intrinseco, sia perché appaiono come costituenti

di rilevanti rappresentazioni di altri gruppi sporadici. Non esiste tuttavia, al momento attuale, una descrizione globale "ragionevole" degli M_i-moduli irriducibili (e.g. una descrizione che proceda dalla "geometria" di M_{24} e ne derivi le rappresentazioni di M_{24} e degli altri gruppi di Mathieu). D'altra parte, alcune fra le rappresentazioni che compaiono in b) e c) sono state ampiamente studiate da un punto di vista geometrico-combinatorio: ciò vale per le rappresentazioni Z-modulari dei grandi gruppi di Mathieu, naturalmente associate al codice binario esteso di Golay C, e per le rappresentazioni 3-modulari di M_{11} e M_{12} associate al codice ternario di Golay (cfr. §5 e §6). In particolare, il codice C, considerato come M_{24}-modulo, il modulo duale C*, e i moduli irriducibili da questi derivati, hanno un ruolo fondamentale nell'analisi di alcuni gruppi sporadici (cfr. §13). Per questo, ne diamo una descrizione più dettagliata nella sezione seguente.

B) MODULI ASSOCIATI ALL'AZIONE DI M_{24} SU 2^{Ω}

1) L'azione di M_{24} su $\Omega = \{0,1,\ldots,22,\infty\}$ induce in modo naturale un gruppo di automorfismi dello spazio vettoriale 2^{Ω}, che preservano il sottospazio C (cfr.§6). C è un M_{24}-modulo di dimensione 12 su GF(2), che si decompone ovviamente in 5 orbite di M_{24}, di lunghezze 1,1,759,759,2576. C non è irriducibile, poiché contiene il sottospazio invariante $<\Omega>$. Il modulo quoziente $V = C/<\Omega>$ è però irriducibile, e realizza una delle due rappresentazioni di grado minimo 11 su GF(2). Le ottadi e le dodecadi di C rappresentano sottospazi 1-dimensiona-

li di V, mentre i trii (=3 ottadi) e i sestetti (= 15 ottadi unione di tetradi) rappresentano rispettivamente sottospazi 2-dimensionali e 4-dimensionali di V. M_{24} ha due orbite su $V \setminus \{\underline{0}\}$. una di lunghezza 759 (le ottadi e i loro complementi), l'altra di lunghezza 1288 (le coppie di dodecadi complementari). M_{23} opera in modo naturale sul sottospazio di C costituito dagli elementi che non contengono ∞ , realizzando un modulo irriducibile di grado minimo 11. Analogamente, M_{22} opera sul sottospazio di C costituito dagli elementi che non contengono 0 e ∞ , realizzando un modulo irriducibile di grado minimo 10.

2) M_{24} opera sullo spazio quoziente $2^{\Omega}/C$, realizzando il modulo C^*, duale di C. Si consideri infatti l'applicazione $f : 2^{\Omega} \to C^*$, definita ponendo, per ogni $X \in 2^{\Omega}$ e per ogni Y e C, $(Y)(X^f)=0$ se $|X \cap Y|$ è pari, = 1 se $|X \cap Y|$ è dispari. f è un omomorfismo di 2^{Ω} su C^*, con nucleo C, che commuta con gli elementi di M_{24}. Si deduce che $2^{\Omega}/C$, per l'azione $(C+X)g=C+Xg (X \in 2^{\Omega}, g \in M_{24})$, è un M_{24}-modulo isomorfo a C^*. Si è già osservato (cfr. §7) che ogni sottoinsieme di Ω, non appartenente a C, è congruo modulo C a una unica monade, a un'unica diade, a un'unica triade, o alle 4 tetradi di un unico sestetto. Poiché M_{24} è transitivo sulle 24 monadi, sulle 276 diadi, sulle 2024 triadi e sui 1771 sestetti, si conclude che il modulo duale C^* si decompone in 5 orbite di M_{24}, di lunghezze 1,24,276,2024,1771. C^* non è irriducibile: i sestetti rappresentano infatti sottospazi 1-dimensionali di C^*, e generano un sottospazio di C^* di dimensione 11. Tale sottospazio realizza

un M_{24}-modulo irriducibile su GF(2), duale di $V=C/<\Omega>$. Si riconosce allora che M_{24} ha due orbite su $v^* \setminus \{0\}$, una di lunghezza 1771 (i sestetti), l'altra di lunghezza 276 (le diadi).

I sottospazi $<C,\{\infty\}>$ e $<C,\{\infty\},\{0\}>$ di 2^Ω sono invariant i per l'azione di $M_{23} = (M_{24})_\infty$ e $M_{22} = (M_{24})_{0,\infty}$ su 2^Ω, rispettivamente. M_{23} opera allora sullo spazio quoziente $2^\Omega/<C,\{\infty\}>$, realizzando un modulo irriducibile di dimensione 11 su GF(2), mentre M_{22} opera sullo spazio $2^\Omega/<C,\{\infty\},\{0\}>$, realizzando un modulo irriducibile di dimensione 10 su GF(2). Questi moduli sono i duali dei moduli irriducibili considerati in 1).

3) I GF(2)-moduli considerati in 1) e in 2) intervengono in modo determinante nella descrizione di alcuni gruppi sporadici associati ai gruppi di Mathieu. In particolare: C interviene nel gruppo di Leech L, C* nel gruppo di Fischer F_{24}, V nel gruppo di Conway Col. V* nel gruppo di Fischer F'_{24} e nel gruppo di Janko J_4 (cfr.§13). Per queste ragioni i moduli irriducibili V e V* sono talvolta indicati con il nome di "modulo di Conway" e di "modulo di Fischer", rispettivamente.

C) I moltiplicatori di Schur dei gruppi semplici finiti sono stati determinati, con il contributo di vari autori (cfr. ad esempio la breve "survey" di Griess (1980)). In particolare: a) M_{11}, M_{23}, M_{24} hanno moltiplicatore banale (Burgoyne, Fong (1966)); b) M_{12} ha moltiplicatore di ordine 2 (Burgoyne.Fong (1966)) (e il ricoprimento $C_2 \cdot M_{12}$ è sottogruppo di SL(6,3), cfr.§5); c) M_{22} ha moltiplicatore ciclico di ordine 12 (Mazet (1979)).

Burgoyne, Fong (1966) utilizzavano tecniche di teoria modulare dei caratteri, e davano anche, nel caso di M_{22}, il moltiplicatore C_6. La rettifica di Mazet (1979) è ripresa in Mazet (1982). che contiene un'esposizione molto chiara ed elegante del calcolo dei moltiplicatori dei gruppi di Mathieu. Mazet (1982) intreccia metodi coomologici con l'uso della geometria dei sistemi di Steiner, ricorrendo soltanto alla teoria dei caratteri ordinari. In particolare, ne.1 caso di M_{22}, servono a Mazet: i) l'osservazione che ogni estensione centrale di M_{21} (= PSL(3.4)) mediante C_3 si . prolunga a M_{22}, e dunque il ricoprimento SL(3,4) si prolunga a un ricoprimento $C_3 \cdot M_{22}$; ii) la costruzione esplicita di un ricoprimento $C_4 \cdot M_{22}$.

A proposito di ii): Mazet considera il sottogruppo $S=(M_{22})_E$, stabilizzante in M_{22} di un blocco E di S(3,6,22), estensione spezzata di E mediante A_6, e via l'azione di A_6 sull'algebra di Clifford di $\mathbb{R}^E$ costruisce dapprima un ricoprimento $C_4 \cdot S$. che dimostra poi essere prolungabile a un ricoprimento di M_{22}.

(L'esistenza di un ricoprimento $C_4 \cdot M_{22}$ era già stata notata da W.Feit, che l'aveva dedotta dall'esame della tavola dei caratteri di un'estensione centrale $C_2 \cdot M_{22}$. Indipendentemente, anche R.Griess aveva provato che un ricoprimento $C_4 \cdot M_{22}$ è realizzabile nel gruppo Spin(210.R). per sollevamento di una rappresentazione ortogonale 210-dimensionale di $C_2 \cdot M_{22}$. Notiamo inoltre che Jónsson,McKay (1976) hanno prodotto generatori per il ricoprimento $C_3 \cdot M_{22}$, considerato come sottogruppo del gruppo unitario SU(6,2). Ciò è ottenuto individuando nel reticolo

di Leech (cfr.§13) una configurazione di "punti". "rette" e "piani" che realizza una geometria unitaria PGU(6,2), in modo che M_{22} è il sottogruppo di PSU(6,2) che permuta certi 22 piani della configurazione.)

Si noti che M_{22} ha un moltiplicatore di Schur "eccezionale", fra i 26 gruppi sporadici. Di questi. 13 hanno moltiplicatore banale, 6 hanno moltiplicatore di ordine 2. 4 di ordine 3, e solo 2 (Sz e F_{22}) hanno moltiplicatore ciclico di ordine 6. Anche M_{21} ha un moltiplicatore "eccezionale". isomorfo a $C_3 x C_4 x C_4$ (inusualmente grande è la p-parte del moltiplicatore, per un gruppo di Chevalley in caratteristica p: nel nostro caso, $C_4 x C_4$). Mazet (1982) include il calcolo di tale moltiplicatore, la cui determinazione risale a N.Burgoyne e J.G.Thompson.

Lo studio delle rappresentazioni projettive di M_{12} e M_{22} è, a nostra conoscenza, incompleto. Humphreys (1980) ha però calcolato i caratteri projettivi di M_{12} e di $Aut(M_{12})$ (anche $Aut(M_{12})$ ha moltiplicatore di Schur di ordine 2). e i corrispondenti caratteri p-modulari per p = 2,3,5,7. Infine, i caratteri projettivi associati ai vari ricoprimenti di M_{22} (e di M_{21}) sono reperibili in Humphreys (1983).

D) Benard (1979) ha calcolato gli indici di Schur dei gruppi, sporadici di ordine fino a un bilione. In particolare, gli indici di Schur delle rappresentazioni dei gruppi di Mathieu sono tutti uguali a 1.

§12. GEOMETRIE DI BUEKENHOUT E GRUPPI DI MATHIEU

1) La teoria dei *buildings* sviluppata da Tits (1974) consente una caratterizzazione geometrica unitaria dei gruppi di Chevalley (e in generale dei gruppi algebrici semisemplici). E' impossibile per ragioni di spazio, richiamare qui il tessuto, di concetti e risultati necessari a una trattazione coerente dell'argomento. Rimandando perciò a Tits (1974), ricordiamo soltanto che un *building* $\mathcal{B} = (X, \mathcal{A})$ è una coppia costituita da un *complesso* (a camere) X e da un insieme $\mathcal{A}$ di sottocomplessi di X, detti *appartamenti* di $\mathcal{B}$, soddisfacenti alle condizioni seguenti: i) *X è spesso* (thick), i.e. ogni elemento di codimensione 1 è contenuto in almeno 3 *camere* (= elementi massimali di X); ii) gli appartamenti sono complessi (a camere) *sottili* (thin), i.e. ogni elemento di codimensione 1 è contenuto in esattamente 2 camere: iii) due elementi qualsiasi di X sono contenuti in un appartamento; iv) se x, x' e X sono entrambi contenuti in due appartamenti A, A', esiste un isomorfismo di A su A' che lascia invarianti x, x' e tutte le loro facce. Se non vale la condizione i), si dice che $\mathcal{B}$ è un *building debole* (in particolare, un appartamento è un building debole, sottile). Gli appartamenti di un building $\mathcal{B}$ sono *complessi di Coxeter* fra loro isomorfi, il cui *diagramma di Coxeter* è univocamente determinato da $\mathcal{B}$. Tale diagramma è dunque il *diagramma di* $\mathcal{B}$: è costituito da n nodi 0,1,. . . ,n-1 (ove n è il *rango* di $\mathcal{B}$) congiunti da spigoli $\overset{i}{\circ}\!\!-\!\!\overset{m_{ij}}{-}\!\!\overset{j}{\circ}$ con peso $m_{ij} \in \mathbb{N} \cup \{\infty\}$ (lo spigolo vuoto se $m_{ij}=0$). Il tipo del diagramma di $\mathcal{B}$, i.e. la partizione in tipi degli elementi di un (qualsiasi)

appartamento di $\mathcal{B}$, determina canonicamente una partizione in tipi degli elementi di $\mathcal{B}$, parametrizzata dai nodi del diagramma, che è il tipo *di* $\mathcal{B}$. In particolare, $\mathcal{B}$ si dice di *tipo finito* (o *sferico*) se il gruppo di Coxeter corrispondente al diagramma di $\mathcal{B}$ è finito; e $\mathcal{B}$ si dice di tipo *indecomponibile* se il suo diagramma è indecomponibile (i.e. non vuoto e connesso).

Se G è un gruppo di Chevalley, la struttura di coppia BN di G determina in modo naturale un building associato a G. Precisamente: G opera per coniugio come un gruppo di automorfismi *speciali* (i.e. automorfismi che preservano i tipi degli elementi) del building $\mathcal{B}_G = (X_G, \mathcal{A}_G)$, ove XG è l'insieme dei *sottogruppi parabolici* di G (i.e. sottogruppi contenenti sottogruppi di Borel) parzialmente ordinato rispetto alla relazione opposta dell'inclusione insiemistica, e gli elementi di $\mathcal{A}_G$ sono gli insiemi dei sottogruppi parabolici contenenti un assegnato toro massimale. Il diagramma di $\mathcal{B}_G$ è il diagramma di Coxeter del gruppo di Weyl di G. I *vertici* (i.e. gli elementi di rango 1) di $\mathcal{B}_G$ sono i *sottogruppi parabolici massimali* di G: la loro partizione in tipi coincide con la partizione in classi di sottogruppi coniugati, parametrizzate dalle radici fondamentali di G. In particolare, lo stabilizzante in G di un vertice di $\mathcal{B}_G$ è un sottogruppo parabolico massimale di G.

Tits (1974) ha classificato i buildings di tipo finito e indecomponibile, e ha in particolare provato che, se $\mathcal{B}$ è un *building finito* di tipo indecomponibile e di rango $n \geq 3$, allora $\mathcal{B} = \mathcal{B}_G$ per un opportuno gruppo di Chevalley G.

2) Un approccio assiomatico alla teoria dei buildings basato su "proprieta loca1 i", alternativo a quello precedentemente descritto, è presentato in Tits (1979) (cfr. anche Tits (1978C)). Tale approccio riprende impostazioni precedenti dello stesso Tits (cfr. Tits (1956.1959)). e è espresso in termini di "geometrie" definite "localmente" e di diagrammi per tali geometrie.

Ispirandosi alla teoria "locale" di Tits, Buekenhout (1979A. 19799) ha sviluppato una teoria generale delle geometrie e dei diagrammi, mediante la quale sembrano potersi descrivere anche i gruppi semplici sporadici. Di questa teoria, perfezionata in Buekenhout (1979C, 1979D, 1981A, 19819). Pasini (1980, 1983A, 19839). Biliotti, Pasini (1982). daremo solo le nozioni necessarie a intenderne le applicazioni ai gruppi sporadici, e in particolare ai gruppi di Mathieu.

Sia S un insieme dotato di una partizione: $S = \cup_{i\in\Delta} S_i$, indiciata da un insieme finito Δ di cardinalita n, e di una relazione binaria riflessiva e simmetrica 1 (*incidenza*). (In particolare, $S=\emptyset$ se n=O). Un insieme F di elementi a due a due incidenti di S è una *bandiera*, e l'insieme $J = \{ j\in\Delta | S_j \cap F\neq\emptyset \}$ è il *tipo* della bandiera F (per abuso di linguaggio, un elemento di S_i si dice di tipo i). $|J|$ è il *rango* di F. Una bandiera massimale. i .e. di tipo A , si dice anche *camera* ; il rango n di una camera è il *rango* di S. Per ogni $i \in \Delta\setminus J$, sia $S_{i,F}$ l'insieme degli elementi di S_i incidenti con tutti gli elementi di una bandiera F di tipo J: l'insieme $Res(F) = \cup_{i\in\Delta\setminus J} S_{i F}$, con l'incidenza ottenuta per restrizione a Res(F) dell'incidenza 1 definita su S, è il *residuo* di F. Per ogni i A , la i-

ombra di una bandiera F è l'insieme degli elementi di S_i incidenti con tutti gli elementi di F (in particolare la i-ombra di una bandiera $\{x\}$, $x \in S$, è l'insieme degli elementi di S_i incidenti con x).

Seguendo Buekenhout (1979A). diremo che $\Gamma = (S,I)$ è una *geometria* (o una *struttura* d'incidenza) su Δ, se sono soddisfatti gli assiomi seguenti: i) per ogni $i \in \Delta$, due elementi di S_i sono incidenti se e solo se coincidono: ii) ogni bandiera non massimale è contenuta in almeno 2 bandiere massimali (camere): iii) per ogni $i \neq j \in \Delta$, il grafo della restrizione di 1 all'insieme $S_i \cup S_j$ è connesso, e la stessa proprietà vale in Res(F), per ogni bandiera F; iv) (proprietà d'intersezione) per ogni $i \in \Delta$, $x \in S_i$ e per ogni bandiera F. l'intersezione delle i-ombre di $\{x\}$ e di F è vuota, oppure esiste una bandiera F' tale che $F \cup F'$ e $\{x\} \cup F'$ sono bandiere, e l'intersezione delle i-ombre di $\{x\}$ e F è la i-ombra di F'. Inoltre, la stessa proprietà vale in Res(F), per ogni bandiera **F. (Tits** (1979) dà una definizione essenzialmente equivalente di geometria, basata sul concetto di *sistema di camere*).

Una geometria $\Gamma' = (S',I')$ su Δ' è una *sottogeometria* di Γ se $\Delta' \subset \Delta$, $S' = \bigcup_{i \in \Delta'} S_i'$, $S_i' \subseteq S_i$, e $I' \subseteq I$. Se I' è la restrizione di I a S', Γ' si dice *indotta* da Γ. In particolare, se F è una bandiera di tipo J di Γ, Res(F) è una sottogeometria indotta da Γ su $\Delta \setminus J$.

Se $\Gamma = (S,I)$ è una geometria di rango 2 su $A = (0.1)$. conviene chiamare punti gli elementi di S_0, *rette* gli elementi di S_1.

Particolari geometrie di rango 2 sono: a) i *piani parziali*,

i.e. geometrie in cui esistono almeno un punto e una retta, due punti distinti sono incidenti con al più una retta, e due rette distinte sono incidenti con al più un punto; b) i *2-goni generalizzati*, i.e. geometrie in cui ogni punto è incidente con ogni retta.

Se Γ è una geometria su un insieme A, e F è una bandiera di tipo $A \setminus \{i,j\}$, $i \neq j \in \Delta$, Res(F) è una geometria di rango 2 su $\{i,j\}$, e risulta essere un *2-gono generalizzato* o un piano *parziale* (cfr. Buekenhout (1981B)).

Importanti classi di piani parziali sono: 1) i piani *lineari*: piani parziali in cui due punti distinti sono incidenti con una unica retta; 2) i *cerchi*: piani lineari in cui una retta è incidente con esattamente due punti; 3) i *piani proiettivi generalizzati*: piani lineari in cui due rette distinte sono incidenti con un unico punto; i *piani affini*: piani lineari in cui, per ogni punto x non incidente con una retta r, esiste un'unica retta r' incidente con x, e tale che r e r' non hanno punti incidenti in comune; gli *m-goni generalizzati* ($m > 2$). Un m-gono *generalizzato* ($m > 2$) è un piano parziale in cui, dati due elementi x,y, esiste una sequenza $x=x_0, x_1, \ldots, x_t=y$, con x_i e x_{i+1} incidenti, $x_i \neq x_{i+2}$, $t \leq m$; e inoltre, se $t < m$, la sequenza è unica. (In particolare, un 3-gono generalizzato è un piano proiettivo generalizzato). Si dice che un m-gono generalizzato ha *parametri* (s,u) se ogni retta è incidente con l+s punti, e ogni punto è incidente con l+u rette.

Siano $\Gamma_1 = (S_1, I_1)$, $\Gamma_2 = (S_2, I_2)$ due geometrie su un insieme A. Un *isomorfismo* (*speciale*) di Γ_1 su Γ_2 è una bijezione $f: S_1 \to S_2$

che preserva l'incidenza e' i tipi, cioé è tale che xI_1y implica $f(x)I_2f(y)$, e $x\in(S_1)_i$ implica $f(x)\in(S_2)_i$.

Gli *automorfismi* di una geometria Γ su A formano un gruppo $Aut(\Gamma)$. $Aut(\Gamma)$ induce un gruppo di trasformazioni sulle camere (bandiere massimali) di Γ: se $Aut(\Gamma)$ opera transitivamente sulle camere, si dice che è *transitivo sulle bandiere*; in tal caso anche Aut(Res(F)) è transitivo sulle bandiere, per ogni bandiera F di Γ.

Sia Γ una geometria su A. Si può dare a A la struttura di un grafo (non orientato) $\Delta(\Gamma)$, congiungendo $i\neq j\in\Delta$ se, per *almeno* una bandiera F di tipo $A\setminus\{i,j\}$. Res(F) non è un 2-gono generalizzato. $\Delta(\Gamma)$ è il *diagramma fondamentale* di Γ. Γ Si dice *pura* (Pasini (1980)) se, quando $i,j\in\Delta$ sono congiunti da uno spigolo di $\Delta(\Gamma)$, per *ogni* bandiera F di tipo $\Delta\setminus\{i,j\}$ Res(F) non è un 2-gono generalizzato. Buekenhout (1979A, 1979B, 1979D) e Pasini (1980) hanno sviluppato una soddisfacente teoria delle *geometrie pure*.

Un *diagramma (speciale)* su Δ è una coppia (Δ,δ), ove δ è una funzione che ad ogni coppia ordinata (i,j), $i=j\in A$, associa una classe $\delta(i,j)=\Delta_{ij}$ di geometrie di rango 2 su $\{i,j\}$, in modo che: 1) Δ_{ij} è costituita da piani parziali o da 2-goni generalizzati; 2) Δ_{ij} è chiusa per isomorfismi; 3) $\Delta_{ji}=\Delta^*_{ij}$ (Δ^*_{ij} è la classe *duale* di Δ_{ij}, essendo *duale* di una geometria $\Gamma_{ij}\in\Delta_{ij}$ la geometria che si ottiene da Γ_{ij} assumendo come punti e rette le rette e i punti, rispettivamente, di Γ_{ij}).

Al fine di rappresentare un diagramma (A, δ) si assegnano delle rappresentazioni standard alle geometrie di rango 2. Per esempio, convenendo di indicare i punti con un nodo a sinistra e le rette con un nodo a destra. il simbolo o o (grafo senza spigoli) indica la classe dei 2-goni generalizzati, e i simboli  ,  ,  ,  ,  , indicano rispettivamente le classi dei piani parziali, dei piani lineari (piani lineari duali), dei cerchi (cerchi duali), dei piani affini, degli $(m+2)$-goni generalizzati $(m>0)$. In particolare, i piani proiettivi generalizzati sono rappresentati da  (e i piani su GF(q) da ), e i 4-goni generalizzati da  .

Dopo di ciò. il diagramma $(A, 6)$ si rappresenta come un grafo (non orientato) avente per vertici gli elementi di Δ. in cui due vertici i,j sono congiunti da uno spigolo contrassegnato dal simbolo delle geometrie di A_{ij}, salvo quando Δ_{ij} è costituita da 2-goni generalizzati.

Si dice che *una geometria* Γ *su* A *ammette il diagramma* (Δ,δ) se, per ogni $i\neq j \in A$ e per ogni bandiera F di tipo $\Delta\setminus\{i,j\}$, $\mathrm{Res}(F)$ e Δ_{ij}. Una geometria può ammettere più di un diagramma.

In particolare, se Γ è una geometria pura, $A(r)$ si può considerare come il "diagramma universale" ammesso da Γ, in cui A_{ij} è la classe dei piani parziali o la classe dei 2-goni generalizzati, secondo che i,j sono congiunti oppure no in $\Delta(\Gamma)$.

Si dice che *un gruppo* G ammette un *diagramma* (A,δ), se esiste una geometria Γ che ammette (Δ,δ), e G è un sottogruppo

d i Aut(Γ), *transitivosulle bandiere*. Si noti che in generale un gruppo G può ammettere diagrammi diversi.

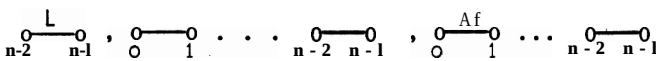
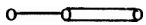
Se $G \leq Aut(\Gamma)$ ammette il diagramma (A, δ), e $J \subseteq A$, gli stabilizzantidelle bandiere di Γ di tipo J. formano una classe di sottogruppi coniugati di G: la classe dei *sottogruppi parabolici* di tipo J. Se P_j è un sottogruppo parabolico di G di tipo J, e Res(J) è il residuo della corrispondente bandiera di tipo J, P_j opera su Res(J) con nucleo U_j, e il gruppo $L_J \sim P_J / U_J$ indotto su Res(J) ammette il diagramma $(A \setminus J, \delta_{|\Delta \setminus J})$. Si osservi in particolare che Γ è canonicamente isomorfa alla geometria $\Gamma' = (S', I')$, dove S' è l'insieme dei sottogruppi parabolici massimali P_i, ie A, e $P_i I' P_j$ sse $P_i \cap P_j$ cont iene un sottogruppo parabolico PA.

1 concetti precedenti, e la nomenclatura corrispondente, sono ovviamente ispirati ai buildings. Invero, un building $\mathscr{B} = (X, \mathscr{A})$ di rango n si pub considerare come una geometria di Buekenhout (S,I) sull'insieme $\Delta = \{0,1,\ldots,n-1\}$ dei nodi del suo diagramma, quando si scelga per S l'insieme dei vertici di $\mathscr{B}$ (elementi di rango 1 di X), con la partizione in tipi indiciata da A, e per 1 l'incidenza così definita: due vertici di $\mathscr{B}$ sono incidenti se ammettono estremo superiore nel complesso X. La geometria (S,I) ammette il diagramma (A, δ), ove $\delta(i,j)$ è la classe degli $(m_{ij}+2)$-goni generalizzati. Nel caso del building $\mathscr{B}_G$ di un gruppo di Chevalley G, S è l'insieme dei sottogruppi parabolici massima1 i di G, e due vertici sono incidenti precisamente quando la loro intersezione cont iene un sottogruppo di Borel. G ammette il diagramma (A, 6) associato

al gruppo di Weyl e i gruppi P_J, U_J, L_J hanno l'usuale significato associato alla decomposizione di Levi.

Per le geometrie di Buekenhout si pongono due naturali problemi di classificazione:

(I) La determinazione delle geometrie che ammettono un assegnato diagramma.

Poiché un diagramma è determinato localmente da classi di geometrie di rango 2, può accadere che geometrie affatto diverse ammettano uno stesso diagramma. Solo per particolari diagrammi è stata ottenuta una classificazione delle corrispondenti geometrie (cfr. Buekenhout (1979A, 1981B)). A titolo d'esempio, ci limitiamo a ricordare che i diagrammi  ....  , caratterizzano rispettivamente gli spazi lineari, proiettivi, affini n-dimensionali. I diagrammi L o . . .  caratterizzano gli spazi "*localmente polari*", parzialmente classificati da Buekenhout, Hubaut (1977). Ricordiamo anche che notevoli risultati di carattere generale sui *diagrammi di Coxeter* sono stati ottenuti da Tits. in lavori non pubblicati oltre che in Tits (1976,1979).

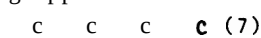
(11) La determinazione dei gruppi che ammettono un assegnato diagramma.

Questo è un terreno largamente inesplorato, salvo che nel caso dei diagrammi di Coxeter indecomponibili associati ai buildings finiti (Tits (1974)). Se il rango è $\geq$ 3, in virtù dei risultati di Seitz (1973) e Tits (1974) i gruppi in questione sono essenzialmente gruppi di Chevalley.

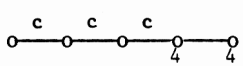
1 gruppi semplici sporadici non possono essere completamente descritti da diagrammi di Coxeter (cfr. Buekenhout (1979A. 1979C)). Buekenhout ha però provato che per ciascuno dei 26 gruppi sporadici esiste almeno una geometria pura che ammette un *diagramma di Coxeter generalizzato*, cioé un diagramma (Δ,δ) in cui per ogni $i\neq j\in\Delta$, $\delta(i,j)$ è una classe di (g,d_p,d_r)-*goni generalizzati* (cfr. Buekenhout (1981A)). Un (g,d_p,d_r)-*gono generalizzato* ($2 \leq g \leq d_p \leq d_r$) è una geometria Γ di rango 2 in cui il grafo della relazione d'incidenza è tale che: i) il numero minimo di elementi di un circuito è $2g$; ii) ogni punto è a distanza massima d_p da qualche altro elemento di Γ; iii) ogni retta è a distanza massima d_r da qualche altro elemento di Γ; iv) $d_p \leq g+2$.

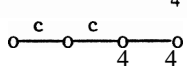
L'analisi condotta da Buekenhout (1979A) ha altresì messo in luce il ruolo che giocano i *cerchi*  . Gran parte dei gruppi sporadici ammette diagrammi in cui i residui di rango 2 sono cerchi o m-goni generalizzati (cfr. Buekenhout (1979A) e Tits (1978C)).

In particolare, se si indica con  un cerchio con $(s+2)$ punti, i gruppi di Mathieu ammettono i diagrammi:

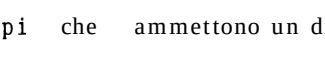
M_{12} 

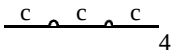
M_{11} 

M_{24} 

M_{23} 

M_{22} 

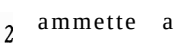
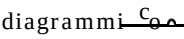
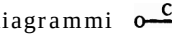
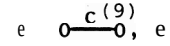
1 diagrammi per M_{12} e M_{11} si riferiscono in modo ovvio al grado di transitività di questi gruppi. Si osservi infatti che i gruppi che ammettono un diagramma  sono precisamente i gruppi k-transitivi di grado n.

1 diagrammi per M_{24}, M_{23}, M_{22} si riferiscono in modo naturale ai sistemi di Steiner associati. Invero, se si considera l'insieme $S = S_0 \cup S_1 \cup S_2 \cup S_3 \cup S_4$, ove S_0, S_1, S_2, S_3, S_4 sono rispettivamente gli insiemi delle monadi, diadi, triadi, tetradi e ottadi di $S(5,8,24)$, e l'incidenza 1 data dall'inclusione (simmetrizzata), si ottiene una geometria $\Gamma = (S,I)$ che ammette il diagramma:  (In particolare, si vede subito che il residuo di una bandiera di tipo $A \setminus \{3,4\}$ è un piano proiettivo PG(2.4). Poiché M_{24} è transitivo sulle bandiere, ammette il diagramma considerato. Discende poi subito che M_{23} e M_{22} ammettono i diagrammi corrispondenti.

In generale, il diagramma:

caratterizza la geometria formata dai punti, dalle coppie di punti, ... dalle (k-1)-ple di punti, e dai blocchi di un sistema di Steiner $S(k, q+k-1, q^2+q+k-1)$ con $q \geq 1$. Per $k \geq 3$, tali sistemi sono noti, e in particolare, per $q=4$ e $k=5,4,3$ sono i sistemi di Steiner associati a M_{24}, M_{23} e M_{22}. Pertanto i diagrammi precedenti determinano pienamente i gruppi di Mathieu M_{24}, M_{23} e M_{22}.

In nessun caso, tuttavia, quelli descritti sono i soli

diagrammi ammessi dai gruppi di Mathieu. E' ovvio, ad esempio, che M_{12} ammette anche i diagrammi  e  , Mll i diagrammi  e  , e diagrammi analoghi ammettono i grandi gruppi di Mathieu.

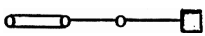
L'analisi dei gruppi sporadici ha condotto a considerare anche geometrie più "deboli", in particolare geometrie per le quali viene a cadere l'assioma iv) (proprietà d'intersezione) (anche in accezioni meno forti, come la condizione di "linearità" introdotta da Tits (1978)). Geometrie cosiffatte si presentano naturalmente, ad esempio. in Ronan, Smith (1980) e sono oggetto di studio corrente (cfr. Kantor (1981)).

Ronan, Smith (1980) hanno considerato "*geometrie 2-locali*" (non necessariamente soddisfacenti 1'assioma iv)) rea1 izzate da vari gruppi sporadici.

Se (A, 6) è il diagramma di tipo sferico ammesso da un gruppo di Chevalley G, definito su un campo GF(q), $q=p^r$, lo stabilizzante di un vertice di tipo i è un sottogruppo parabolico massimale P_i, i.e. un *sottogruppo p-locale massimale*. Prendendo lo spunto da ciò, e considerando i gruppi sporadici "patologie" dei gruppi di Chevalley su GF(2), come è suggerito dal ruolo che la maggior parte di essi gioca nella classificazione dei gruppi semplici, una *geometria 2-locale* per un gruppo sporadico G è, secondo Ronan. Smith (1980). una geometria Γ con diagramma (Δ, δ), tale che $G \leq \mathrm{Aut}(\Gamma)$ ammette il diagramma (Δ, δ), e lo stabilizzante di una bandiera di tipo i, ie Δ, è un *sottogruppo 2-locale massimale* (*2-costretto*) di G.

In particolare, Ronan, Smith (1980) hanno descritto un

notevole diagramma per M_{24}, considerato anche da Shult. Yanushka (1980). e successivamente investigato da Brouwer (1981). Ronan (1982). Smith (1982B), e da Aschbacher in un lavoro non pubblicato, Il diagramma è il seguente:

(*) 

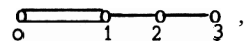
Il nodo quadrato □ significa che, se Γ è una geometria che ammette (*) , S_3 è vuoto, ma vi sono sottogeometrie di Γ che contengono oggetti atti a "riempire" S_3.

Una geometria 2-locale per M_{24}, che ammette (*) e soddisfa l 'assioma iv) , si ottiene considerando l'insieme $S = S_0 \cup S_1 \cup S_2$, ove S_0 è l'insieme delle *ottadi* di S(5,8,24), Sl l'insieme dei *trii* di ottadi disgiunte, S_2 l'insieme dei *sestetti* , e la relazione d'incidenza I è così definita: un'ottade è incidente con un trio se appartiene al trio. e è incidente con un sestetto se è unione di due tetradi del sestetto; un trio è incidente con un sestetto se le sue ottadi sono unione di tetradi del sestetto.

In particolare: i) Res(0), il residuo di un'ottade s_0, è costituito dai punti e dalle rette di uno spazio proiettivo PG(3.2): più precisamente, i trii e i sestetti incidenti con s_0, e le involuzioni (di tipo $1^8 2^8$) di M_{24} che fissano i punti di s_0, sono i punti, le rette e i piani di PG(3,2) (ciò spiega il nodo □); ii) Res(1), il residuo di un trio, è un grafo bipartito completo Y x Z, con |Y|=3 e |Z|=7 (i.e. un 2-gono generalizzato); iii) Res(2), il residuo di un sestetto s_2, è un 4-gono generalizzato con parametri (2,2) e gruppo delle

coll ineazioni $Sp(4,2) \simeq S_6$ (brevemente, un S_6-quadrangolo): infatti le ottadi e i trii incidenti con s_2 sono identificabili con le diadi e le partizioni di tipo 2^3 di un insieme di 6 oggetti; iv) se $G < Aut(\Gamma)$ è transitivo sulle bandiere, allora $G = M_{24}$, P_0 è lo stabilizzante di un'ottade. $[E_{24}] \cdot A_8$; P_1 è lo stabilizzante di un trio, $[E_{26}]$ $(PSL(3,2) \times S_3)$; P_2 è lo stabilizzante di un sestetto. $([E'_{26}]C_3) \cdot S_6$.

Si osservi inoltre che la geometria Γ si può realizzare nello spazio $C/<\Omega>$ (rispettivamente nel duale di $C/< \Omega >$), considerando come vertici di tipo 0,1,2 i sottospazi di dimensione 1,2,4 (rispettivamente: di dimensione 6,3,1) rappresentati da ottadi; trii e sestetti.

Oltre alla geometria 2-locale di M_{24} sopra descritta, altre geometrie ammettono il diagramma (*). Infatti. ammette certamente (*) ogni geometria che si ottiene da un building (debole) di tipo B_4: 

, rimuovendo i vertici di tipo 3 e gli elementi che li contengono: una tale geometria è un *building troncato* di tipo B_4, nella terminologia di **Ronan** (1982).

Un'altra geometria che ammette (*) si ottiene dal piano proiettivo PG(2,2), assumendo come vertici di tipo 0.1.2 rispettivamente i punti e le rette di PG(2,2), le 28 anti-bandiere di PG(2,2) (i.e. le coppie costituite da una retta e un punto che non le appartiene) , i 21 4-goni contenuti in PG(2.2). Il gruppo degli automorfismi di questa geometria è $PSL(3,2) \cdot C_2 = Aut(PSL(3,2))$.

Seguendo Ronan (1982), chiameremo i vertici di tipo 0.1.2

di una geometria Γ che ammette (*) rispettivamente *punti*, *rette*, *quads*. E' facile verificare che il residuo di un punto di Γ è costituito dai punti e dalle rette di uno spazio proiettivo 3-dimensionale PG(3,k), definito su un campo k indipendente dal punto considerato. Si dirà allora che Γ è *definita sul campo* k. (Si osservi che si considera qui anche il "campo" di ordine 1, corrispondente al caso in cui le rette dello spazio proiettivo hanno 2 punti, e punti e rette formano il grafo completo con 4 vertici. Ciò accade nella geometria sopra descritta per $PSL(3,2)\cdot C_2$).

Ronan (1982) ha provato che le sole geometrie *finite* che ammettono (*) sono quelle che abbiamo descritto.

Precisamente vale il seguente:

TEOREMA. Una geometria finita Γ che ammette (*), e è definita sul campo k di ordine q. è un building troncato di tipo B_4, oppure: i) q=2 e Γ è la geometria 2-locale di M_{24}; ii) q=1 e Γ è la geometria di $PSL(3,2)\cdot C_2$ sopra descritta.

La dimostrazione di Ronan è di tipo geometrico, e distingue le possibili strutture di Γ. Se Γ non è un building troncato, allora è un *quasi-esagono* (near-hexagon) nel senso di Shult. Yanushka (1980), e il residuo di un quad risulta essere un 4-gono generalizzato di parametri (2,2) o (1,1). Nel secondo caso si ottiene ii); nel primo caso ogni quad è un S_6-quadrangolo, e l'identificazione di Γ con la geometria 2-locale di M_{24} può passare per l'unicità del quasi-esagono regolare su 759 punti (Brouwer (1981)), oppure per una ricostruzione diretta, dentro Γ, di un sistema di Steiner S(5,8,24) per il quale

le ottadi, i trii e i sestetti sono rispettivamente i punti, le rette e i quads (Ronan (1982)).

Il teorema precedente implica in particolare che, se Γ è una geometria su GF(2) che ammette (*), o Γ è la geometria 2-locale di M_{24}, oppure Γ è la geometria del building (troncato) di tipo $B_4(2)$, e $Aut(\Gamma)=B_4(2)$ $(=Sp(8,2))$.

Le geometrie su GF(2) che ammettono (*) sono state determinate anche da Smith (19828) usando, in luogo di metodi puramente geometrici, *metodi omologici* per lo studio di $Aut(\Gamma)$ nell'ipotesi (non necessaria in Ronan (1982)) che $Aut(\Gamma)$ sia transitivo sulle bandiere. In virtù di tale ipotesi è determinata in $G = Aut(\Gamma)$ la struttura di $P_J/U_J \simeq LJ$, per ogni $J \subseteq \{0,1,2\}$. Precisamente: $L_0 = A_8$, $L_1 = PSL(3,2) \times S_3$, $L_2=S_6$; da cui $L_{0,1}= PSL(3,2)$, $L_{0,2} = LI_{,2} = S_3$ (e $L_{0,1,2} = \langle 1 \rangle$). Inoltre, i sottogruppi P_J risultano essere sottogruppi 2-locali di G.

Considerando Γ come un complesso simpliciale su $\{0,1,2\}$, è possibile assegnare ai simplessi J un opportuno prefascio di L_J-moduli V_J su GF(2), in modo che sia estendibile a un sistema G-equivariante di coefficienti $\mathcal{V}$ su Γ. Il metodo di Smith (1982B) consiste nel calcolare il G-modulo $V=H_0(\mathcal{V},\Gamma)$ su GF(2), e suo tramite determinare la struttura di Γ e di G; si appoggia a tecniche elaborate dallo stesso Smith e da Ronan, e si applica anche alle geometrie realizzate da altri gruppi sporadici.

In Smith (19828) V_0 è il modulo banale per L_0, V_1 è il modulo irriducibile 2-dimensionale per LI (in cui $P_0 \cap P_1$ fissa un vettore), V_2 è il modulo 4-dimensionale naturale per $L_2=$

= Sp(4.2) (in cui PO $\cap P_2$ fissa un vettore), e la costruzione di $V = \langle V_0^G, V_1^G, V_2^G \rangle$ è ridotta a calcoli "locali", corrispondenti alla costruzione, per ogni sottogruppo P_i, i=0,1,2, di una serie di composizione del P_i-modulo V. Si giunge a una separazione in due casi, secondo che $P_2/O_2(U_2) \simeq S_6 \times S_3$, oppure $P_2/_2(U_2) \simeq C_3 S_6$: i) nel primo caso dim(V) = 16, V è il modulo spinoriale per G = Sp(8,2) ($\simeq \Omega(9,2)$), e Γ è la geometria del building troncato di tipo B_4 su GF(2); ii) nel secondo caso dim(V) = 11, V è il modulo irriducibile $C/\langle\Omega\rangle$ per $G=M_{24}$, e Γ è la geometria a-locale di M_{24}, realizzata in V dai sottospazi di dimensione 1.2.4 corrispondenti alle ottadi, ai trii, ai sestetti.

Si noti che scelte diverse del prefascio conducono a moduli diversi (sia per Sp(8,2) che per M_{24}). Nel caso di M_{24}, si ottiene $V = C/\langle\Omega\rangle$ imponendo che P_0 fissi un vettore di V; se si impone invece che P_2 fissi un vettore di V, gli stessi calcoli conducono al duale di $C/\langle\Omega\rangle$, e alla geometria Γ degli spazi di dimensione 6.3.1 corrispondenti alle ottadi, ai trii e ai sestetti. Altri moduli si ottengono scegliendo altri sottogruppi P_J, $J \subseteq \{0,1,2\}$.

Smith ha parzialmente esaminato le scelte possibili, e ha riscontrato che sembrano ottenersi 14 "sistemi irriducibili" (nozione implicita in Smith (1982A)), in corrispondenza naturale con i 14 tipi di sottogruppi di M_{24} contenenti un 2-sottogruppo di Sylow (cfr. Aschbacher (1982)), e apparentemente legati ai 13 moduli irriducibili su GF(2) (cfr. §11.).

Ronan,Smith (1980) hanno anche descritto una geometria 2-locale per il gruppo di Mathieu M_{22}.

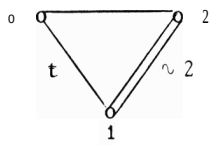
Fissati due punti α, β di un sistema di Steiner S(5,8,24), si consideri l'insieme $S = SO \cup Sl \cup S_2$, ove SO è l'insieme delle *esadi* del sistema di Steiner S(3,6,22) che si ottiene da S(5,8,24) contraendolo in α, β ; S_1 è l'insieme delle *ottadi* di S(5,8,24) contenute in S(3,6,22); e S_2 è l'insieme dei *sestetti* con la proprietà che cinque delle loro tetradi sono contenute in S(3,6,22). Gli elementi di S_0, S_1, S_2 si diranno brevemente *esadi*, *ottadi* e quintetti di S. Si consideri in S la relazione d'incidenza I così definita: un'esade è incidente con un'ottade se è da questa disgiunta, e è incidente con un quintetto se contiene una tetrade del quintetto; un'ottade è incidente con un quintetto se è unione di due tetradi del quintetto.

$\Gamma = (S,I)$ è una geometria su $\Delta = \{0,1,2\}$, e si osserva che:
i) fissata un'esade h. ogni coppia di punti di h individua un quintetto incidente con h, e ogni partizione di h di tipo 2^3 individua tre quintetti, che sono raffinamenti di uno stesso trio formato da $h \cup \{\alpha,\beta\}$ e da altre due ottadi (incidenti con h). Pertanto Res(h) è la geometria che si ottiene da un S_6-quadrangolo (formato da 15 quintetti e 15 trii) rimpiazzando ogni trio con le due ottadi del trio incidenti con h (i.e. Res(h) è un *doppio ricoprimento* spezzato del S_6-quadrangolo).
ii) fissata un'ottade o, esiste un'unica involuzione di M_{24} che fissa i punti di o e scambia fra loro α e β. Tale involuzione determina 7 trii e 7 sestetti incidenti con o, che formano un piano proiettivo PG(2,2) (cfr. la geometria 2-locale di M_{24}) e corrispondono precisamente alle esadi e ai quintetti

incidenti con o. Dunque Res(o) è un piano proiettivo PG(2,2).

iii) fissato un quintetto q, vi sono 5 esadi e 10 ottadi incidenti con q. e ciascuna esade è incidente con 3 ottadi. Res(q) ha perciò la struttura di un sistema di Steiner banale S(3.3.5).

Se si rappresentano con $\overset{\sim 2}{\circ\!=\!\circ}$ e $\circ\!\!-\!\!\overset{t}{\circ}$ il doppio ricoprimento del S_6-quadrangolo e il sistema S(3,3,5), rispettivamente, Γ è una geometria 2-locale per M_{22} che ammette il diagramma:



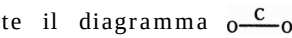
Gli stabilizzanti dei vertici sono sottogruppi 2-locali massimali di M_{22}: precisamente, P_0 è lo stabilizzante di un'esade, $[E_{2^4}] \cdot A_6$; P_1 è lo stabilizzante di un'ottade, $[E_{2^3}]PSL(3,2)$; P_2 è lo stabilizzante di un quintetto, $[E_{2^4}]S_5$.

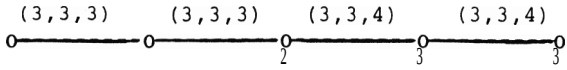
Si noti che Pl non contiene un 2-sottogruppo di Sylow di M_{22}. Questa situazione non si presenta nei gruppi di Chevalley, nei quali i sottogruppi 2-locali massimali contengono sempre un 2-sottogruppo di Sylow, ma ha luogo in vari gruppi sporadici. Dal punto di vista dei diagrammi 2-locali, ogniqualvolta P_i non contiene un 2-sottogruppo di Sylow, i residui di rango 2 che contengono il nodo i risultano essere opportuni n-ricoprimenti spezzati di geometrie standard (cfr. Ronan, Smith (1980)).

Per terminare, notiamo che, accanto a geomctrie 2-loca1 i relat ive a parabolici massima1 i, è ut ile considerare gcomctric relative a parabolici minimali. E.g., nel caso di M_{24}, vi

sono esattamente 3 tipi di sottogruppi che coprono un 2-sottogruppo di Sylow e si possono scegliere come parabolici P_0, P_1, P_2 (si ottiene allora un diagramma , dove rappresenta il triplo ricoprimento del S_6-quadrangolo). Per l'esempio precedente cfr. Ronan (1982) e Ronan, Stroth (1982). che trattano sistematicamente queste "2-Sylow geometrie". Un altro esempio è offerto da M_{12}, che contiene due tipi di sottogruppi che coprono un 2-sottogruppo di Sylow (il centralizzante di un'involuzione centrale, e il normalizzante di un sottogruppo E_{22} contenente tre involuzioni centrali i cui insiemi di punti fissi sono mutuamente disgiunti, entrambi massimali in M_{12}). Scegliendo tali sottogruppi come parabolici P_0, P_1 si ottiene una geometria simile a un (g, d_p, d_r)-gono generalizzato, salvo che $g=8, d_p=d_r=12$. (Cfr. Ronan, Stroth (1982)).

ADDENDA:

1) Buekenhout (1982) presenta uno studio dettagliato di varie geometrie "contenute" in M_{12}, scelto come cavia sulla quale verificare quali possano essere le geometrie più adatte a interpretare geometricamente i gruppi sporadici. In particolare, Buekenhout esamina residui e troncamenti dell'ovvia geometria $\Gamma = (S, I)$, con $S = S_0 \cup S_1 \cup S_2 \cup S_3 \cup S_4$, ove S_0, S_1, S_2, S_3, S_4 sono rispettivamente gli insiemi delle monadi, diadi, triadi, tetradi ed esadi di $S(5,6,12)$, e I l'inclusione simmetrizzata. (Γ ammette il diagramma  , o, più precisamente, in termini di (g, d_p, d_r)-goni generalizzati:



). Ne deriva nuove geometrie, e oltre a ciò elenca varie altre geometrie per M_{12} e $Aut(M_{12})$, legate in vari- modi a $S(5,6,12)$ e/o alla struttura di sottogruppi di M_{12}.

2) Un fitto catalogo aggiornato di geometrie ammesse dai 26 gruppi semplici sporadici è stato compilato da Buekenhout (1983).

513. GRUPPI SPORADICI ASSOCIATI AI GRUPPI DI MATHIEU

1 gruppi di Mathieu sono strettamente associati ad altri gruppi sporadici, sia perché intervengono in modo diretto nella loro costruzione, sia perché giocano un ruolo essenziale nella loro descrizione e caratterizzazione. In §8. abbiamo discusso i risultati che mettono in luce il legame fra M_{24} e il gruppo di Held He. In questo paragrafo descriveremo in qualche dettaglio il gruppo di Higman-Sims HS. i gruppi di Conway Co_1, Co_2, Co_3, i gruppi di Fischer F_{22}, F_{23}, F'_{24}, e i l quarto gruppo di Janko J_4, cercando di illustrarne i nessi con i gruppi di Mathieu.

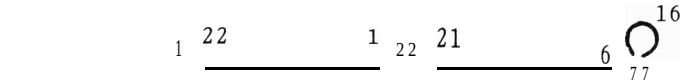
A) IL GRUPPO DI HIGMAN-SIMS HS.

Il gruppo sporadico HS fu scoperto da D.G.Higman e C.C.Sims (Higman. Sims (1968)). come estensione transitiva di rango 3 del gruppo di Mathieu M_{22}.

M_{22} si può considerare come gruppo di permutazioni sull'insieme $\Delta_1 \cup \Delta_2$, ove $\Delta 1$ è l'insieme dei punti, e Δ_2 è l'insieme dei blocchi del sistema di Steiner S = S(3,6,22). Aggiungendo un nuovo punto $*$, si ottiene l'insieme $\Omega = \{*\} \cup \Delta_1 \cup \Delta_2$, di cardinalità 100=1+22+77. HS è l'unica estensione transitiva di M22 su Ω (Higman,Sims (1968). Wales (1969A)).

La costruzione di HS in Higman,Sims (1968) procede dalla costruzione di un grafo $\mathcal{G}$ associato alla geometria di S=S(3,6,22). Si osserva infatti che: i) se a è un punto di S, vi sono esattamente 21 blocchi di S che contengono a ; ii) se α , β sono punti distinti di S, vi sono esattamente 5 blocchi che contengono

α e β ; iii) due blocchi sono disgiunti, oppure si intersecano in 2 punti; iv) dato un blocco b di S, per ii) e iii) vi sono esattamente 16 blocchi disgiunti da b. Si definisce allora il *grafo* $\mathcal{G}$, i cui *vertici* sono i punti di Ω , e i cui *spigoli* si ottengono congiungendo * con ogni punto di S, ogni punto α di S con i 21 blocchi che lo contengono, e ogni blocco b di S con i 16 blocchi disgiunti da b. $\mathcal{G}$ è un *grafo fortemente regolare* di valenza 22, e si può concisamente rappresentare mediante il diagramma:



Si consideri ora $Aut(\mathcal{G})$: è $(Aut(\mathcal{G})) \simeq Aut(M_{22})$. Per ottenere un'estensione transitiva, occorre provare che $Aut(\mathcal{G})$ è transitivo sui vertici di $\mathcal{G}$. Basta, a tale scopo, considerare un vertice $\alpha \in Al$, l'insieme $Al(o)$ dei vertici di $\mathcal{G}$ adiacenti ad α, l'insieme $\Delta_2(\alpha) = \Omega \setminus (\{\alpha\} \cup \Delta_1(\alpha))$, e provare che gli elementi di $\Delta_1(\alpha)$ e $A_2(\alpha)$ possono interpretarsi come i punti e i blocchi di un sistema di Steiner S'=S(3,6,22) (con l'incidenza indotta da $\mathcal{G}$). Allora la transitività di $Aut(\mathcal{G})$ su Ω si deduce osservando che $(Aut(\mathcal{G}))_\alpha \simeq Aut(M_{22})$, o alternativamente osservando che ogni isomorfismo $\tau : S \to S'$ si estende a un automorfismo $\bar{\tau}$ di $\mathcal{G}$ tale che $(*)\bar{\tau} = \alpha$ e $(Al)? = Al(a) = \{*\} \cup Bo$.

Sia $G=Aut(\mathcal{G}) \cap A_\Omega$: G ha indice 2 in $Aut(\mathcal{G})$, poiché $Aut(M_{22})$ contiene una permutazione che fissa esattamente 8 punti e 21 blocchi di S. Inoltre G è primitivo su Ω, poiché $(1+22) \nmid 100$, e $G_* = M_{22}$: segue subito che G è un gruppo semplice. G è il

gruppo sporadico HS, di ordine $|M_{22}| \cdot 100 = 2^9 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$: in particolare, $Aut(\mathcal{G}) = Aut(HS)$.

L'idea di associare un *grafo* (0 una famiglia di grafi) a un gruppo di permutazioni è stata introdotta e utilizzata per la prima volta da Sims (1967,1968). Se G è un gruppo transitivo su un insieme Ω, e G_α ($\alpha \in \Omega$) ha orbite $\Delta_0(\alpha) = \{\alpha\}, \Delta_1(\alpha), \ldots, \Delta_{k-1}(\alpha)$ su Ω (i.e. G ha rango k e parametri $|\Delta_i(\alpha)|, 1 \leq i \leq k-1$), ad ogni orbita $\Delta_i(\alpha)$ è possibile associare un grafo orientato $\mathcal{G}_i$, i cui vertici sono i punti di Ω, e i cui spigoli si ottengono congiungendo α con ogni punto di $A_i(\alpha)$, e ogni immagine α^g ($g \in G$) con i punti di $\Delta_i(\alpha)^g$. Il grafo $\mathcal{G}_i$ è il *grafo orbitale* (o *grafo di Sims*) di G, relativo all'orbita $\Delta_i(\alpha)$. Se, in particolare, si ha $\alpha \in A_i(\alpha)^g$ se e solo se α^g e $\Delta_i(\alpha)$, si può considerare $\mathcal{G}_i$ come un grafo non orientato. Ciò accade, per i=1,2, quando G ha ordine pari e rango 3: le orbite Δ_1 e $\Delta_2(\alpha)$ danno luogo ai grafi non orientati e complementari $\mathcal{G}_1$ e $\mathcal{G}_2$. Di più, ciascuno di questi due grafi è *fortemente regolare*, i.e. $|\Delta_i(\alpha) \cap \Delta_i(\alpha)^g|$ dipende unicamente dall'essere $\alpha^g \in \Delta_i(\alpha)$ o $\alpha^g \notin \Delta_i(\alpha)$ (i=1,2). Dunque G si può considerare come un gruppo di automorfismi di un grafo fortemente regolare, transitivo sui vertici e sugli spigoli.

Nel caso della costruzione di HS, sopra delineata, l'esistenza di HS come estensione transitiva di M_{22} è provata mediante la costruzione del grafo $\mathcal{G}$. $\mathcal{G}$ è precisamente il grafo orbitale $\mathcal{G}_1$ relativo all'orbita $\Delta_1 = \Delta_1(*)$. Wales (1969A) ha provato che, se G è un'estensione transitiva di M_{22} di grado 100, e $G_\alpha = M_{22}$ ha orbite $\{\alpha\}, A_1(\alpha), \Delta_2(\alpha)$ di lunghezza 1,22,77,

l'azione di M_{22} sulle orbite $\Delta_1(\alpha)$, $\Delta_2(\alpha)$ coincide necessariamente con l'azione sui punti e sui blocchi di S(3,6,22), e determina completamente il grafo orbitale $\mathcal{G}_1$ dell'estensione G. L'unicità di $\mathcal{G}_1$ implica allora, ovviamente, che HS è l'unica estensione transitiva di M_{22} di parametri 22.77. (Per ulteriori caratterizzazioni di HS in termini del grafo $\mathcal{G}_1$, cfr. Gewirtz (1969) e M.S. Smith (1975)).

Altri gruppi sporadici. oltre a HS. sono stati costruiti e caratterizzati secondo le stesse linee. Si tratta dei gruppi seguenti :

(i) il gruppo di McLaughlin Mc. Mc è l'unica estensione transitiva di PSU(4,3) di grado 275 e parametri 112.162 (cfr. McLaughlin (1969)). (L'unicità del grafo orbitale è provata in Janko,Wong S.K. (1972) secondo le linee di Wales (1969A)).

(ii) il secondo gruppo di Janko J_2 e il gruppo di Suzuki sz.

Suzuki (1969) ha descritto una catena di 4 grafi, estensioni successive del grafo nullo con 4 vertici, cui corrisponde la seguente catena di estensioni transitive del gruppo simmetrico S_4 : PGL(2,7), di grado 14 e parametri 4,9; $G_2(2) = PSU(3,3) \cdot C_2$, di grado 36 e parametri 14.21; $Aut(J_2) = J_2 \cdot C_2$, di grado 100 e parametri 36,63; $Aut(G_2(4))$, di grado 416 e parametri 100,315; $Aut(Sz) = Sz \cdot C_2$, di grado 1782 e parametri 416,1315. (J_2 è stato scoperto da Janko (1968c) mediante un centralizzante di involuzione, ma è stato costruito da Hall, Wales (1968) come estensione transitiva di rango 3 di PSU(3,3)). Un'elegante costruzione di J_2 come gruppo di un grafo, equivalente a quella

di Suzuki (1969) è stata ottenuta da Tits (1969). Per l'unicità di J_2, cfr. Hall, Wales (1968) e Wales (1969B)).

(iii) il gruppo di Rudval is Ru. Ru è l'unica estensione transitiva del gruppo di Ree ${}^2F_4(2)$ di grado 4060 e parametri 1755, 2304. Ru coincide con il gruppo degli automorfismi del suo grafo di Sims, e è stato costruito da Conway, Wales (1973). La costruzione non fa riferimento diretto al grafo orbitale; tuttavia, come nel caso di HS. l'unicità del grafo implica che Ru è l'unica estensione di ${}^2F_4(2)$ con i parametri descritti.

Notiamo infine che i gruppi di Fischer F_{22}, F_{23}, F_{24} (cfr.C) in questo paragrafo), pur originando dalla classificazione dei gruppi generati da una classe D di 3-trasposizioni. sono costruiti come estensioni di rango 3 del centralizzante di un elemento di D, e caratterizzati come gruppi di automorfismi dei grafi orbitali corripondenti (Fischer (1969)).

Concludiamo con una sommaria rassegna di ulteriori informazioni su HS:

1) Una costruzione alternativa di HS. come gruppo degli automorfismi di un 2-(176,50,14) disegno simmetrico, si deve a G.Higman :(Higman (1969)). (L'isomorfismo del gruppo costruito da G. Higman con HS è stato provato da Sims (1969). e in seguito anche da M.S.Smith (1976A, 1976B) nell'ambito dello studio di strutture combinatorie ottenute generalizzando la costruzione di Higman (1969). Di fatto, HS è l'unico gruppo semplice del suo ordine (Parrott, Wong S.K. (1970)). HS è 2-transitivo sui 176 punti e sui 176 blocchi del disegno Di Higman (1969). Le due azioni sono distinte (e fuse da un automorfismo esterno di HS), e lo

stabilizzante di un punto (blocco) è isomorfo al gruppo $PSU(3,5)\langle\sigma\rangle$ (ove è l'automorfismo indotto dall'automorfismo di Frobenius di $GF(5^2)$). Dunque HS è estensione Z-transitiva di $PSU(3,5)\langle\sigma\rangle$. L'estensione è unica, e se ne può ottenere una costruzione alternativa applicando il "graph extension theorem" di E. Shult (cfr. Shult (1972)). Un'ulteriore estensione di rango 3 di HS non è possibile (cfr. Magliveras (1974.1976)). Sia la costruzione di Higman, Sims (1968). sia quella di Higman (1969), sono realizzabili nel gruppo di Leech L: una breve dimostrazione ne è data da Conway (1969A), identificando HS con il sottogruppo di L che fissa un certo "triangolo" del reticolo di Leech (cfr. B), II) in questo paragrafo). Infine: una caratterizzazione di HS come gruppo Z-transitivo è data da Kimura (1978). Precisamente: se G è un gruppo 2-transitivo su Ω, con $|\Omega|$ pari, e $G_{\alpha\beta} = PGL(2,q^2) \cdot C_2$ (ove q è dispari, e C_2 induce su $PGL(2,q^2)$ un automorfismo di ordine 2), allora q=3 e G è il gruppo HS nella sua azione sui 176 punti del disegno di G.Higman.

2) HS è generabile da un'involuzione e da un elemento di ordine 7 (Higman. Sims (1968)). Magliveras (1971) ha determinato i sottogruppi massimali di HS: vi sono 12 classi di sottogruppi massimali, fra le quali due classi di sottogruppi isomorfi a M_{11}.

Kassab (1982) ha classificato le cliques (= sottografi nulli massimali) del grafo di HS, e descritto gli stabilizzanti delle cliques (e.g. M_{11} è lo stabilizzante di una clique di 12 vertici).

3) HS ha due classi di involuzioni: una classe di involuzioni

centrali, il cui centralizzante è estensione di un prodotto centrale $D_8*D_8*C_4$ mediante S_5, e una classe di involuzioni non centrali, il cui centralizzante è $C_2 x Aut(A_6)$. HS è stato caratterizzato mediante il centralizzante di un'involuzione centrale da Janko, Wong S.K. (1969), e mediante la struttura di un 2-sottogruppo di Sylow (Gorenstein, Harris (1973), O'Nan (1976B)). Nel gruppo sporadico di Harada-Norton F_5, il centralizzante di una involuzione non centrale è isomorfo al ricoprimento $C_2 \cdot Aut(HS)$ (Harada (1975B)).

4) Frame (1972) ha calcolato le tavole dei caratteri di HS e di Aut(HS). Il moltiplicatore di Schur di HS ha ordine 2 (McKay, Wales (1971)), e i caratteri del ricoprimento $C_2 \cdot HS$ sono stati calcolati da Rudvalis (1975). La struttura dei 2-blocchi non-principali di HS è stata analizzata da Landrock (1978), e Humphreys (1982) ha poi determinato tutti i caratteri modulari. L'indice di Schur delle rappresentazioni di HS è 1 (Benard(1979)).

5) Una geometria 2-locale per HS (nel senso di 111) è descritta da Ronan. Smith (1980).

B) 1 gruppi di Conway Col. Co_2, Co_3.

1 tre gruppi semplici scoperti da J.H.Conway sono sezioni del gruppo degli automorfismi di un singolare oggetto combinatorio, il cosiddetto reticolo . di Leech, strettamente associato al codice binario esteso di Golay e alla geometria di M_{24}.

1) (Costruzione di gruppi di Conway)

Sia E uno spazio euclideo reale di dimensione n. Un *reticolo*

in E è un sottogruppo di rango n del gruppo additivo di E, che contiene una base di E. Un reticolo Λ in E si dice *pari* se (x,x) è 22 per ogni $x \in \Lambda$; si dice *unimodulare* se, per ogni Z-base $\{x_1,\ldots,x_n\}$ di Λ, è $|\det((x_i,x_j))|=1$. Una rotazione dello spazio E che lasci un reticolo Λ invariante, si dice *simmetria*, o *automorfismo*, di Λ : il gruppo delle simmetrie di Λ si indica con $\mathrm{Aut}(\Lambda)$.

Se $n=24$, a meno d'isometrie esiste un unico reticolo Λ, pari e unimodulare. tale che sia $(x,x) > 2$ per ogni $x \in \Lambda$, $x \neq 0$. Ciò i? stato dimostrato da Conway (1969B) (la dimostrazione di Conway è di natura costruttiva, e può essere usata come definizione di Λ), e indipendentemente da Niemeier (1968), che ha classificato tutti i reticoli pari e unimodulari in $\mathbb{R}^{24}$ (provando che tali reticoli si distribuiscono in 24 classi d'equivalenza rispetto alle isometrie di $\mathbb{R}^{24}$, ciascuna delle quali è determinata dalla configurazione dei vettori di norma $\sqrt{2}$).

Il reticolo Λ in $\mathbb{R}^{24}$, pari, unimodulare, e privo di vettori di norma $\sqrt{2}$, è il *reticolo di Leech*, scoperto da J.Leech in relazione a problemi di "packings" densi di sfere (cfr. Leech (1964, 1967)). $\mathrm{Aut}(\Lambda) = L$ è il *gruppo di Leech*: L è un sottogruppo finito del gruppo delle isometrie (= congruenze euclidee) di $\mathbb{R}^{24}$.

Al fine di descrivere la geometria di Λ e analizzare la struttura di L, conviene considerare, scegliendo una scala opportuna, una rappresentazione di Λ in coordinate intere (Conway (1969A)).

Sia dunque C il codice binario (esteso) di Golay, considerato come sottospazio di dimensione 12 dello spazio 2^{Ω}, Ω = PG(1.23) (cfr. §6), e sia $\{e_i\}_{i\in\Omega}$ la base standard di $\mathbb{R}^{24}$. Per $X \subseteq \Omega$, $z \in Z$, sia (X,z) l'insieme dei vettori $v = \Sigma x_i e_i$, con $x_i \in Z$, $\Sigma x_i = 4z$, e $x_i \equiv z$, o $z+2 \pmod 4$ secondo che $i \notin X$ oppure $i \in X$. *Il reticolo* di Leech è *l'unione di tutti gli insiemi* (X,z), con X e C. z e Z. Alternativamente, si può definire Λ come lo Z-modulo generato in $\mathbb{R}^{24}$ dai vettori $-3e_\infty + \Sigma_{i=0}^{22} e_i$, e $\Sigma_{i\in S} 2e_i$, ove S varia nell'insieme delle ottadi di C.

(Sul reticolo Λ, cfr. anche **McKay (1972)**, che costruisce una classe di reticoli pari unimodulari contenente Λ, esibendone una matrice generatrice, e Thompson (1976). Sia in **McKay** (1972). che in Thompson (1976) emergono connessioni fra Λ e il reticolo delle radici del gruppo di Weyl $W(E_8)$.(*) Eleganti costruzioni di Λ, e dimostrazioni di unicità, sono date da Tits (1978A. 1980). cfr. II), 2)).

Per ogni $x,y \in \Lambda$, si ha $(x,y) \equiv 0 \pmod 8$ e $(x,x) \equiv 0 \pmod{16}$. Se $(x,x) = 16d$. si dice che x è un *vettore di tipo* d, e si indica con Λ_d l'insieme dei vettori di tipo d. Per $x \in \Lambda$, si indica A(x) il reticolo dei vettori ortogonali a x. e con $\Lambda_d(x)$ l'insieme dei vettori di tipo d ortogonali a x. In particolare, si ha: $|\Lambda_1| = 0$ (i.e. Λ non contiene vettori di tipo 1); $|\Lambda_2| = 196.560$; $|\Lambda_3| = 16.773.120$; $|\Lambda_4| = 398.034.000$; $|\Lambda_5| = 4.629.381.120$. Inoltre, se $x \in \Lambda_2$, $|\Lambda_2(x)| = 93.150$.

La geometria di Λ consente di determinare la struttura di L. In primo luogo, ogni permutazione $\pi \in S_\Omega$ induce una trasformazione ortogonale $\tilde{\pi} : e_i \to e_{\pi(i)}$ di $\mathbb{R}^{24}$, che appartiene al

(*) Cfr. gli Addenda alla fine di questa sezione.

gruppo di Leech L se e solo se $\tilde{\pi}(C) = c$. Si deduce che L contiene un sottogruppo M isomorfo a M_{24}. D'altra parte, per ogni $X \subseteq \Omega$, si consideri la riflessione ε_X definita ponendo $\varepsilon_X(e_i) = e_i$ se $i \notin X$, $\varepsilon_X(e_i) = -e_i$ se $i \in X$. Il gruppo $A = \langle \varepsilon_X | X \in C \rangle$ è un sottogruppo di L. abeliano elementare di ordine 2^{12}, isomorfo al gruppo additivo di C. e normalizzato da M. Considerato come M-modulo, A è isomorfo al modulo C: il prodotto semidiretto $[A]M$ è il sottogruppo *monomiale* N di L, e coincide con l'insieme degli elementi di L che lasciano invariante l'insieme $\{\pm e_i\}$. N è un sottogruppo proprio di L: infatti, se $T_1, T_2, \ldots, T_6$ sono le tetradi di un sestetto di C, L contiene la rotazione $\zeta_{T_1} = \varepsilon_{T_1} \circ \eta_{T_1}$, ove $\eta_{T_1} : e_i \to e_i - \frac{1}{2} \Sigma_{j \in T_s} e_j$, se $i \in T_s$ (cfr. Conway (1969A)). Sia $x \in \Lambda_2$, e sia H un sottogruppo di L contenente propriamente N. Si può dimostrare che H è transitivo su Λ_2, H_x è transitivo su $\Lambda_2(x)$, e per ogni $y \in \Lambda_2(x)$, H_{xy} è un sottogruppo di N, prodotto semidiretto di E per M_{22}. Poiché $|\Lambda_2(x)| = 93.150$, si deduce che $|H| = (196.560)(93.150)\, 2^{10}\, |M_{22}| = 2^{21} 3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23$, e quindi necessariamente, H=L. In particolare, N è un *sottogruppo massimale* rii L, e $L = \langle N, \zeta_{T_r} \rangle$.

Un insieme costituito da 24 vettori mutuamente ortogonali di Λ_4 e dai loro opposti è una *croce*. Le croci danno luogo a una partizione di Λ_4 in sottoinsiemi di cardinalità 48; in particolare $\Lambda_4 \supset \{\pm 8e_i\} \cdot \{\pm 8e_i\}$ è la *croce standard* (e lo stabilizzante in L della croce standard è N). Modulo 2Λ, ogni vettore del reticolo Λ è equivalente: i) al vettore $\underline{0}$; ii) a $\pm x$, per un unico $x \in \Lambda_2$; iii) a $\pm x$, per un unico $x \in \Lambda_3$; iv) ai 48 vettori di un'unica croce. In particolare:

posto $\bar{\Lambda}_2 = \{\{\pm x\} | x \in \Lambda_2\}$, $\bar{\Lambda}_3 = \{\{\pm x\} | x \in \Lambda_3\}$, $\bar{\Lambda}_4 \{\{\pm 8e_i\}^g | g \in L, i \in \Omega$, si ha $|\Lambda/2\Lambda| = 1 + |\bar{\Lambda}_2| + |\bar{\Lambda}_3| + |\bar{\Lambda}_4| = 2^{24}$.

Il gruppo di Leech L ha centro Z(L) di ordine 2. generato dalla riflessione ε_Ω (=-I), e il gruppo quoziente L/Z(L) opera come un gruppo primitivo su $\bar{\Lambda}_2$, $\bar{\Lambda}_3$, e $\bar{\Lambda}_4$. L/Z(L) = Co1 è il *primo gruppo di Conway*, di ordine $2^{21}3^9 5^4 7^2 11 \cdot 13 \cdot 23$. Considerando l'azione di Co_1 su $\bar{\Lambda}_2$, si può dedurre senza troppa difficoltà che Co_1 è un gruppo semplice (cfr. Conway (1969A)).

Lo stabilizzante di un punto di $\bar{\Lambda}_2$ in Co_1 è il *secondo gruppo di Conway*, Co_2, di ordine $2^{18}3^6 5^3 7 \cdot 11 \cdot 23$; lo stabilizzante di un punto di $\bar{\Lambda}_3$ in Co è i l *terzo gruppo di Conway*, Co_3 di ordine $2^{10}3^7 5^3 7 \cdot 11 \cdot 23$. 'Anche Co_2 e Co_3 sono gruppi semplici (per una dimostrazione di semplicità, valida simultaneamente per Co_1, Co_2, e Co_3, cfr. Tits (1975)).

In particolare, l' immagine $\bar{N}$ di N in Co è estensione spezzata di un gruppo abeliano elementare $E_{2^{11}}$ ($\simeq A/\langle\varepsilon_\Omega\rangle$) mediante M_{24}. Come M_{24}-modulo, $E_{2^{11}}$ è isomorfo al modulo $V=C/\langle\Omega\rangle$, considerato in §11.

11) (Sottogruppi di L e dei gruppi di Conway)

1) Oltre ai tre gruppi di Conway e ai cinque gruppi di Mathieu, il gruppo di Leech L ammette come sottogruppi o sezioni i gruppi sporadici HS, Mc, J_2 e Sz.

a) HS e Mc.

Sia x un vettore di tipo d: se x è somma di due vettori di tipo a e b, si dice che x è un vettore di tipo d_{ab}. In virtù di ciò che si è detto in I) su $\Lambda/2\Lambda$, si ha che ogni

vettore. di tipo d è di tipo dab, con $a+b = \frac{1}{2}(d+r)$, $r=0,2,3,4$ (ove queste possibilita si escludono a vicenda).

Il gruppo di Leech L opera transitivamente sull'insieme dei vettori di Λ di ciascuno dei tipi seguenti: $2,3,4,5,6_{22},6_{32}$, $7,8_{22},8_{32},8_{42},9_{33},9_{42},10_{33},10_{42},11_{43},11_{52}$. Pertanto, se $d < 12$, è univocamente determinato il sottogruppo $L_{d_{ab}}$ di L che fissa un vettore di tipo d_{ab}. La struttura di tali sottogruppi è determinata in Conway (1969A) (cfr. anche Conway (1971)). In particolare $L_2 = Co_2$, $L_3 = Co_3$, $L_4 = [E_{2}11]M_{23}$, $L_5 = Aut(Mc)$ $(= Mc \cdot C_2)$, $L_{6_{22}} = PSU(6,2)\ C_2$, $L_{6_{32}} = M_{24}$, $L_7 = HS$.

1 gruppi sporadici HS e Mc si possono ottenere anche in altro modo come sottogruppi di Co3 (di fatto, HS e Aut(Mc) sono sottogruppi massimali di Co_3):

Siano $x,y \in \Lambda$, di tipo a e b rispettivamente,e sia $z = x-y$ di tipo c. 1 vettori x,y,z formano un "triangolo" di tipo abc. La struttura del sottogruppo L_{abc} di L che fissa i vertici del triangolo (i.e. i punti del sottoreticolo di Λ generato da x e y) è specificata in Conway (1969A), per varie terne abc.

In particolare:

i) $M_{22} \leq L_{222}$, e $L_{222} \simeq PSU(6,2)$. (Questa identificazione è alla base della rappresentazione di $C_3 \cdot M_{22}$ studiata da Jónsson, McKay (1976) (cfr. §11)).

ii) $L_{322} \simeq Mc$.

(A un triangolo di tipo 322 si associa una configurazione di 275 vettori di Λ : ritenendo incidenti due vettori x,y se $x - y \in \Lambda_3$, si ottiene un grafo isomorfo al grafo di Mc. Inoltre:

se x e Λ_3, vi sono esattamente 276 coppie non ordinate $\{y,z\}$ tali che sia $x=y+z$, con $y,z\in\Lambda_2$. $L_3=Co_3$ è 2-transitivo sull'insieme di tali coppie. e lo stabilizzante di una coppia in L_3 è L_{322}. $C_2 \simeq$ Aut(Mc). Ciò mostra che Co3 è estensione 2-transitiva di Aut(Mc). (Per una costruzione diretta di Co3 come estensione di Aut(Mc), ottenuta estendendo il grafo orbitale di Mc, cfr. Shult (1972))).

iii) $L_{332} \simeq$ HS.

(A un triangolo di tipo 332 si associa una configurazione di 100 vettori di Λ. Definendo l'incidenza come in ii), si ottiene un grafo isomorfo al grafo di HS. Al triangolo si può anche associare una configurazione di 176 coppie di punti di Λ, identificabile con il disegno considerato da Higman (1969). mostrando in tal modo l'identità delle costruzioni di Higman,Sims (1988) e Higman (1969)).

iv) $L_{333} \simeq [E_{35}]M_{11}$.

(L'azione di M_{11} su E_{35} è irriducibile, e realizza la rappresentazione descritta in Assmus. Mattson (1966A), Ward (1975). Fissato un triangolo T di tipo 333. vi sono in Λ esattamente altri 11 triangoli con lo stesso centro di T. Il sottogruppo di L che permuta questi 12 triangoli è estensione di E_{36} mediante $C_2 \cdot M_{12}$; l'azione di $C_2 \cdot M_{12}$ su E_{36} coincide con quella descritta da Coxeter-Todd e investigata da Assmus-Mattson e Ward, i.e. con l'azione di M_{12} come gruppo degli automorfismi del codice ternario di Golay. (Una dettagliata analisi della struttura di E_{36} $(C_2 \cdot M_{12})$, in relazione alla sua azione sul reticolo

complesso di Leech $\Lambda_{\mathbb{C}}$ (cfr.b)). si trova in Curtis (1980))).

b) J_2 e Sz.

La locazione di Sz (e del suo sottogruppo J_2) in L è convenientemente descritta mediante la cosiddetta "catena *di Thompson*". L contiene un elemento u di ordine 3, il cui centralizzante è isomorfo a $\langle u \rangle \times (C_2 \cdot A_9)$ (dove $C_2 A_9$ è il doppio ricoprimento di A_9). L contiene pertanto una catena di sottogruppi $C_2 \cdot A_i$ (i=2,...,9); posto $G_i = G_L(C_2 \cdot Ai)$, si ha: $G_2 = L = C_2 \cdot Col$; $G_3 = C_6 \cdot S_z$ (il ricoprimento completo di Sz); $G_4 = C_2 \cdot G_2(4)$; $G_5 = C_2 \cdot J_2$ (il ricoprimento di J_2; $G_6 = C_2 \cdot PSU(3,3)$; $G_7 = C_2 \cdot PSL(2,7)$; $G_8 = C_2 \cdot A_4$; $G_9 = C_6$ (Cfr. la catena di *Suzuki* in A)).

La catena di Thompson suggerisce una rappresentazione projettiva 12-dimensionale di Sz su Q(w), ove ω è una radice cubica primitiva dell'unita. Essa si ottiene considerando il *reticolo complesso di Leech* $\Lambda_{\mathbb{C}}$, i.e. scegliendo in L un elemento ω_L di ordine 3, privo di punti fissi, e considerando Λ come modulo 12-dimensionale su $Z(\omega)$, con l'azione $x(a+b\omega)=ax+b(x\omega_L)$, per ogni $x \in \Lambda, a+b\omega \in Z(\omega)$. Si ha $Aut(\Lambda_{\mathbb{C}}) = C_6 \cdot Sz$.(*)

(Il reticolo complesso $\Lambda_{\mathbb{C}}$ è associato al codice ternario (esteso) di Golay $C_{(3)}$, così come Λ è associato al codice binario C. $\Lambda_{\mathbb{C}}$ è infatti generato nello spazio $\mathbb{C}^{12}$ dai vettori $\sqrt{-3}\ \sum_{i \in S} e_i$ ($S \in C_{(3)}$, $3(e_i - e_j)$, e $\sum_{i=0}^{11} e_i + 3e_j$ (Conway (1971)).

La rappresentazione 12-dimensionale di $C_6 \cdot Sz$ su Q(ω) si può anche ottenere a partire da una rappresentazione 6-dimensionale di $C_6 \cdot PSU(4,3)$ su Q(w), e, a sua volta, può servire per

(*) Per una descrizione dettagliata della geometria del reticolo complesso $\Lambda_{\mathbb{C}}$, considerato come $C_6 \cdot Sz$-modulo, cfr. anche Wilson(1983).

una costruzione di L=Aut(Λ)(Lindsey (1970B,1971).

Tits (1978A) dà quattro presentazioni del reticolo di Leech Λ associate alla catena di Thompson (incluso il reticolo $\Lambda_{\mathbb{C}}$), il cui interesse risiede principalmente nell'elegante uniformità della costruzione. Infatti, indicando con R_i l'anello degli endomorfismi di Λ generato da $C_2 \cdot A_i$, Tits da una descrizione diretta, con formule quasi identiche, di Λ come R_i-modulo, per i=2,3,4,5.

In tale descrizione, osserva Tits, si separano una parte "aritmetica" di Λ, espressa dall'anello R_i, e una parte "combinatoria", espressa da un codice. Al crescere di i. la parte "aritmetica" si arricchisce: R_2 è naturalmente Z (e si ottiene l'ordinaria presentazione di Λ come reticolo intero), mentre R_3=Z(ω), R_4 è un ordine massimale dell'algebra quaternionale $\mathbb{Q}(i,j,k)$, e R_5 è un ordine massimale dell'algebra quaternionale su $\mathbb{Q}(\sqrt{5})$. Parallelamente, la parte "combinatoria" si riduce: per i=2, è espressa dal codice binario di Golay; per i=3, dal codice ternario di Golay; per i=4, da un codice in $GF(4)^6$; e infine per i=5, da un codice in $Mat(2,GF(4))^3$. Come R_i-modulo (i=2,3,4,5), Λ ha rango d_i=24,12,6,3, rispettivamente. Il gruppo G_i (i=2,3,4,5) è il gruppo degli R_i-automorfismi di Λ, che preservano la forma hermitiana standard $h=h_i$ su $R_i^{d_i}$. In particolare, per i=3, si ottiene la rappresentazione di $C_6 \cdot Sz$ sul reticolo $\Lambda_{\mathbb{C}}$, mentre per i=5 si ottiene una rappresentazione quaternionale 3-dimensionale di $C_2 \cdot J_2$. In quest'ultima rappresentazione, considerata anche in Cohen (1980), e ampiamente analizzata in Tits (1980). $C_2 \cdot J_2$ appare come il gruppo generato dalle

riflessioni unitarie r_a d i $V_3(Q(\sqrt{5})(i,j,k)$, relative ai vettori a, con h(a,a) = 4. Dalla rappresentazione così ottenuta, si deduce in modo naturale una rappresentazione o-dimensionale di $C_2 \wr J_2$, realizzabile in $Q(\omega,\sqrt{5})$, già investigata da Lindsey (1970A). Infine. il caso i = 4 è trattato in Tits (1978B).

2) Curtis (1973.1980) ha ulteriormente investigato i sottogruppi di L.

L'analisi dei sottogruppi di L che fissano sottoreticoli di Λ è portata a compimento in Curtis (197). Ci si può ridurre a considerare gli $\mathscr{S}$-reticoli contenuti in Λ,i.e. i sottoreticoli Σ di Λ, tali che il sottogruppo L_Σ di L che fissa i punti di Σ : i) non fissa croci in Λ ; ii) non contiene alcun sottogruppo di indice $\leq$ 2. che fissi i punti di un sottoreticolo $\Sigma' \supset \Sigma$. Gli Y-reticoli di dimensione 1 sono i reticoli generati da un punto di Λ_2 o Λ_3, e gli y-reticoli di dimensione 2 sono quelli generati da triangoli di tipo 222, 322, 332 o 333.In genera le. un Y-reticolo Σ è generato da $(\Lambda_2 \cup \Lambda_3) \cap \Sigma$ (anzi da $\Lambda_2 \cap \Sigma$, se dim $\Sigma > 2$), e si dice di tipo $2^i 3^k$ se $|\Lambda_2 \cap \Sigma| = i$ e $|\Lambda_3 \cap \Sigma| = k$.

Vi sono esattamente 12 tipi di Y-reticoli in Λ , e L opera transitivamente sui reticoli di uno stesso tipo; ne segue che, indicato con $\Sigma(i,k)$ un Y-reticolo di tipo $2^i 3^k$, è univocamente determinato il sottogruppo $L_{\Sigma(i,k)}$, così come $\mathrm{Aut}_L(\Sigma(i,k)) = L \cap \mathrm{Aut}(\Sigma(i,k))$. 1 risultati di Curtis (1973) possono essere riassunti nella seguente tavola:

Tipo di Σ	$L_{\Sigma(i,k)}$	$Aut_L(\Sigma(i,k))$
$2^0 3^0$	L	L
$2^1 3^0$	$Co_2 = L_2$	$C_2 \times Co_2$
$2^0 3^1$	$Co_3 = L_3$	$C_2 \times Co_3$
$2^3 3^0$	$PSU(6,2) = L_{222}$	$(C_2 \cdot PSU(6,2)) \cdot S_3$
$2^2 3^1$	$Mc = L_{322}$	$C_2 \cdot Aut(Mc)$
$2^1 3^2$	$HS = L_{332}$	$C_2 \cdot Aut(HS)$
$2^0 3^3$	$[E_{35}]M_{11} = L_{333}$	$C_2(E_{35}M_{11})S_3$
$2^5 3^2$	$PSU(4,3)$ ($\subseteq$ Mc)	$(C_2 \cdot PSU(4,3)) \cdot D_8$
$2^9 3^6$	$E_{34} \cdot A_6$	$(C_2 \cdot E_{34}A_6)(S_3 \times S_3)C_2$
$2^3 3^4$	$PSU(3,5)$ ($\subseteq$ MC)	$(C_2 \cdot PSU(3,5))S_3$
$2^5 3^{10}$	G c $PSU(3,5)$, $\lvert G\rvert = 2^2 5^3$	$C_2 \cdot G \cdot S_5$
$2^{27} 3^{36}$	$\lvert G\rvert = 2 \cdot 3^5$	$C_2 \cdot G \cdot PSU(4,2)$

e nel seguente:

TEOREMA. Sia $G = L_X \leq L$, $\underline{0} \neq x$ e Λ. Esiste una catena $K_0 \lhd K_1$ a... $\lhd K_r = G$, con $\lvert K_{i+1} : K_i \rvert = 2$ per ogni i. tale che: 1) $K_0 \leq N$ (stabilizzante della croce standard), oppure: 2) $K_0 \leq L_\Sigma$, dove Σ è un Y-reticolo $\neq \{\underline{0}\}$.

Curtis (1980) ha invece come obiettivo la determinazione della struttura locale di L. Usando sistematicamente il MOG in una delicata analisi della geometria di Λ e $\Lambda/2\Lambda$, e delle corrispondenti azioni di L (e.g., per i sottogruppi 2-locali. 1 'azione dei 2-sottogruppi di L sulle croci in $\Lambda/2\Lambda$), Curtis ottiene un elenco di sottogruppi di L con la proprietà che: i) ogni sottogruppo locale di L è coniugato

a un sottogruppo di un gruppo dell'elenco; ii) nessun gruppo dell'elenco è coniugato a un sottogruppo di un altro gruppo dell'elenco.

Da Curtis (1973. 1980) si ricavano naturalmente informazioni sui sottogruppi massimali di L. i.e. di Col = L/Z(L). Tuttavia, un elenco completo dei sottogruppi massimali di Col (e di Co_2), non è disponibile. (*) Un elenco completo dei sottogruppi massimali di Co_3 è stato invece ottenuto (insieme a quello dei sottogruppi massimali di MC) da Finkelstein (1973).

3) Una caratterizzazione di tipo gruppale dei sottoreticoli A(d) di Λ, ortogonali a un vettore di tipo d. per $d=2,3,6_{32}$, è contenuta in un fondamentale articolo di W. Feit sulle rappresentazioni integrali dei gruppi finiti (Feit (1974)). Fra l'altro, Feit indaga quali restrizioni imponga l'azione di un gruppo finito con certe proprietà, sulla struttura di un R-reticolo di uno spazio vettoriale V=V(K), con K campo numerico algebrico e R anello degli interi di K. In particolare, Feit (1974) contiene i seguenti teoremi:

TEOREMA 1: Sia G un gruppo finito, privo di sottogruppi di indice 23 o 24. e sia F una rappresentazione razionale, fedele e assolutamente irriducibile di G, di grado 23. Nella rappresentazione F, G opera su un reticolo razionale di dimensione 23, identificabile con uno dei reticoli $\Lambda(2)$, $\Lambda(3)$, $\Lambda(6_{32})$. In particolare, G è un sottogruppo di uno dei gruppi $C_2 \times Co_2$, $C_2 \times Co_3$, $C_2 \times M_{24}$, rispettivamente.

TEOREMA 2: Sia G un gruppo finito di ordine divisibile per 23, e sia F una rappresentazione razionale e fedele di G di grado 24. Se G è privo di sottogruppi di indice 23,24

(*) Ma cfr. gli Addenda alla fine di qs. sezione.

0 25, G' opera su un reticolo razionale di dimensione 24. identificabile con il reticolo di Leech Λ. In particolare, $G' \leq L$.

111) (Centralizzanti di involuzioni)

Poiché il gruppo monomiale N contiene $Syl_2 L$, ogni involuzione di L è coniugata a un'involuzione di N, e precisamente a una riflessione ε_X, con $X \in C$. L ha dunque 4 classi di involuzioni: (i) la classe costituita dalla riflessione $\varepsilon_\Omega = -1$; (ii) la classe delle involuzioni coniugate a una riflessione ε_S, ove S è un'ottade di C (L'insieme $\Lambda^-(\varepsilon_S) = \{x \in \Lambda \mid \varepsilon_S(x) = x\}$ è un sottoreticolo di Λ, isomorfo al reticolo delle radici del gruppo di Weyl $W(E_8)$. Il nucleo dell'azione di $C_L(\varepsilon_S)$ su $\Lambda^-(\varepsilon_S)$ è un gruppo extraspeciale 2^{1+8} di tipo +, e $C_L(\varepsilon_S)/2^{1+8}_+$ è isomorfo a $W(E_8)'$.); (iii) la classe delle involuzioni coniugate a una riflessione $\varepsilon_{S'}$, ove S' è il complemento di un'ottade S di C ($C_L(\varepsilon_{S'})$ ha la stessa struttura di $C_L(\varepsilon_S)$.); (iv) la classe delle involuzioni coniugate a una riflessione ε_D, ove D è una dodecade di C (Lo spazio dei punti fissi di ε_D ha dimensione 12; $C_L(\varepsilon_D) = C_N(\varepsilon_D) = [E_{212}]M_{12}$.).

Consideriamo il gruppo $Col = L/\langle \varepsilon_\Omega \rangle$ indicando con un soprassegno le immagini in Col di sottogruppi o elementi di L. Ogni involuzione di Col è coniugata a un'involuzione di $\bar{N}$. Col ha 3 classi di involuzioni, rappresentate dagli elementi $\bar{\varepsilon}_S$ $(= \bar{\varepsilon}_{S'})$, $\bar{\varepsilon}_D$, e $\bar{z}$ (ove $\bar{z}$ è l'immagine di un elemento di ordine 4 di L, con $z^2 = -1$). $\bar{\varepsilon}_S$ è centrale in Col, e $C_{Co_1}(\bar{\varepsilon}_S) = 2^{1+8}_+ . \Omega^+_8(2)$; $C_{Co_1}(\bar{\varepsilon}_D) = [E_{211}]Aut(M_{12})$; $C_{Co_1}(\bar{z}) = (E_{2^2} \times G_2(4)) \langle \alpha \rangle$,

ove $\alpha^2 = 1$ e $G_2(4) \cdot \langle\alpha\rangle \cong \mathrm{Aut}(G_2(4))$. Col è stato caratterizzato mediante $C(\bar{\varepsilon}_S)$ da Patterson (1974). e mediante $C(\bar{\varepsilon}_D)$ da Reifart (1977C).

Co_2 contiene 3 classi di involuzioni, rappresentate da $\bar{\varepsilon}_S$, $\bar{\varepsilon}_D$, $\bar{z}$. ε_S è centrale, e $C_{Co_2}(\bar{\varepsilon}_S) = [2_+^{1+8}]Sp(6,2)$; $C_{Co_2}(\bar{\varepsilon}_D) = E_{210} \cdot \mathrm{Aut}(A_6)$; $C_{Co_2}(\bar{z}) = (E_{24} \times (2_+^{1+6}))\, A_8$. F.L. Smith (1974) ha caratterizzato Co_2 mediante $C(\bar{\varepsilon}_S)$; la struttura di Syl_2Co_2 è analizzata da Yoshida (1977). che fornisce una caratterizzazione di Co_2 mediante un 2-sottogruppo di Sylow.

Co_3 contiene 2 classi di involuzioni. rappresentate da $\bar{\varepsilon}_S$ e $\bar{\varepsilon}_D$. $\bar{\varepsilon}_S$ è centrale, e $C_{Co_3}(\bar{\varepsilon}_S) = \langle\varepsilon_S\rangle \cdot Sp(6,2)$ (estensione non spezzata) ; $C_{Co_3}(\bar{\varepsilon}_D) = \langle\bar{\varepsilon}_D\rangle \times M_{12}$. Co_3 è stato caratterizzato mediante $C(\bar{\varepsilon}_S)$ da Fende1 (1973), mediante $C(\bar{\varepsilon}_D)$ da Yoshida (1974). e mediante la struttura di un 2-sottogruppo di Sylow da Solomon (1974).

(Notiamo inoltre che una caratterizzazione 2-locale di Co_3, mediante un sottogruppo, estensione non spezzata di E_{24} mediante GL(4.2). è stata ottenuta da O'Nan, Solomon (1976). cfr. §8,C). Un'altra caratterizzazione 2-locale di Co_3 è data da Stroth (1979)).

Ci limitiamo poi a ricordare che: 1) il gruppo sporadico di Fischer F_2 (Baby Monster) contiene un'involuzione il cui centralizzante è estensione di un gruppo extraspeciale 2^{1+22}_+ di tipo + mediante Co_2, F_2 è stato caratterizzato in funzione di tale centralizzante da Bierbrauer (1979). 2) il gruppo sporadico di Fischer-Griess Fl ("Monster", o "Friendly Giant") contiene due classi di involuzioni, con centralizzanti. rispettiva-

mente, il ricoprimento $C_2 \cdot F_2$ e un'estensione Cl di un gruppo extraspeciale 2^{1+24} mediante Col. Proprio a partire da Cl Griess (1982) ha costruito un'algebra A (commutativa e non-associativa) di dimensione 196.884 su $\mathbb{C}$, e ha provato l'esistenza di F_1 mostrando che $Aut(A) = F_1$. Nella complessa costruzione di Griess, gioca un ruolo determinante l'analisi di alcuni moduli per i gruppi di Conway. legati all'azione su Λ. Inoltre, F_1 è determinato univocamente dalla struttura di Cl (Griess. S.D.Smith, Thompson, Norton).

Notiamo, infine, che nessun gruppo semplice contiene L come centralizzante di un'involuzione (Finkelstein (1974)).

IV) La tavola dei caratteri di L è stata calcolata da Guy, Patterson e Thompson. Anche le tavole dei caratteri dei gruppi di Conway sono note (in particolare, Fende1 (1973) riproduce la tavola di Co_3). 1 Z-blocchi non-principali dei gruppi di Conway sono stati analizzati da Landrock (1978).

Il gruppo di Conway Col ha moltiplicatore di Schur di ordine 2 (e ricoprimento L); Co_2 e Co_3 hanno moltiplicatori banali (Griess (1974)). Infine, Co_i $(i=1,2,3)$ non ha automorfismi esterni.

V) Geometrie Z-locali per Col e Co_2 sono descritte in dettaglio in Ronan. Smith (1980).

ADDENDA:

1) Vogliamo qui porre riparo ad alcune omissioni, e documentare il persistente interesse di cui è oggetto il reticolo di Leech,

menzionando alcuni risultati recenti:

a) Oltre a quelle già considerate in questo paragrafo (Leech (1964. 1967). Conway (19696. 1969B, 1971). Lindsey (1970B, 1971), McKay (1972), Curtis (1973.1980). Thompson (1976). Tits (1978A, 1980)), descrizioni del reticolo di Leech sono contenute in Leech, Sloane (1971) e Sloane (1977.1979). con enfasi particolare sui nessi fra reticoli, codici e "sphere packings"; una costruzione "ciclotomica" di Λ è ottenuta da Craig (1978) ; e generalizzazioni di Λ sono studiate da Neumaier (1982).

b) Sulla classificazione dei reticoli pari e unimodulari in $\mathbb{R}^{24}$, ottenuta da Nieneier (1967). sono tornati, producendo dimostrazioni alternative, Venkov (1980) e Conway. Sloane (1982A).

c) Conway, Parker, Sloane (1982) hanno determinato il "raggio di copertura" R del reticolo di Leech Λ, i.e. la massima distanza di un punto di $\mathbb{R}^{24}$ da Λ : R è uguale a $1/\sqrt{2}$ volte la distanza minima fra due punti di Λ . L'esatta determinazione di R è raggiunta (valendosi anche di un risultato di Norton (1982), che dava un limite superiore per R) attraverso una completa classificazione dei "buchi" di Λ aventi raggio massimo. (Un "buco" in un reticolo di $\mathbb{R}^n$ è una coppia (x,P), ove x è un punto di $\mathbb{R}^n$ la cui distanza d dal reticolo è un massimo locale. e P è il politopo convesso determinato dagli r $\geq$ n+l punti del reticolo a distanza d da x. x e d sono rispettivamente il centro e il raggio del buco (x,P); R=max {d} è il raggio di copertura del reticolo.) Conway, Parker, Sloane (1982) analizzano i buchi di raggio massimo nel reticolo di Leech Λ,

provando che si distribuiscono in 23 classi d'equivalenza. rispetto alle congruenze euclidee di $\mathbb{R}^{24}$, in corrispondenza biunivoca con le 23 classi di reticoli di Niemeier. distinte da quella contenente Λ. Accade infatti che: i) se (x,P) è un buco di Λ, e i vertici di P sono $y_1,\ldots,y_r$, il vettore y_i-y_j $(i\neq j)$ è di tipo 2.3. o 4 (in Λ); ii) a (x,P) è associato un "diagramma" di nodi $1,\ldots,r$, nel quale i nodi i,j $(i\neq j)$ sono disgiunti se y_i-y_j è di tipo 2, congiunti da uno spigolo se y_i-y_j è di tipo 3. e congiunti da due spigoli se y_i-y_j è di tipo 4; iii) il diagramma di un buco di raggio massimo è un grafo le cui componenti connesse sono diagrammi completi di Dynkin (nel senso di Bourbaki (1968)) di tipo A_ℓ $(\ell \geq 1)$, D_ℓ $(\ell \geq 4)$, E_6, E_7, E_8, che descrivono esattamente le componenti di uno dei 23 tipi di reticoli di Niemeier; iv) a buchi non congruenti corrispondono, via i diagrammi, reticoli di Niemeier non congruenti, e si stabilisce pertanto una bijezione fra le classi di buchi e le classi di reticoli di Niemeier diversi da Λ.

d) Dai risultati descritti in c). Conway, Sloane (1982B) deducono 23 costruzioni del reticolo di Leech, una per ciascun tipo di buco, ovvero per ciascun tipo di reticolo di Niemeier. Precisamente: ad ogni reticolo di Niemeier $\mathcal{N}$ vengono associati un insieme $\{v_i\}$ di "vettori fondamentali" (corrispondenti ai nodi dei sistemi completi di radici di tipo $A_\ell, D_\ell, E_6, E_7, E_8$ che individuano le componenti di $\mathcal{N}$), e un insieme $\{g_w\}$ di "vettori colla" (glue vectors) (che servono ad "incollare" fra loro le componenti di $\mathcal{N}$, e sono indiciati dalle parole

w di un opportuno "codice colla" (glue code)), in modo che: i) $\mathcal{N} = \{\Sigma z_i v_i + \Sigma t_w g_w \mid \Sigma t_w = 0; z_i, t_w \in Z\}$; ii) $\{\Sigma z_i v_i + \Sigma t_w g_w \mid \Sigma z_i + \Sigma t_w = 0; z_i, t_w \in Z\}$ è una copia del reticolo di Leech Λ. In particolare, al reticolo di Niemeier di tipo A_1^{24} corrisponde, secondo una scala opportuna, l'usuale costruzione di Λ descritta in 1) (e il codice colla è il codice binario esteso di Golay), mentre al reticolo di Niemeier di tipo A_2^{12} corrisponde, per una scelta di coordinate in $Z(\omega)$, $\omega = e^{(2/3)\pi i}$, la costruzione del reticolo complesso $\Lambda_{\mathbb{C}}$ (cfr. 11)) (e il codice colla è in questo caso il codice ternario esteso di Golay).

(I risultati di Conway, Sloane (1982B) sono utilizzati in Conway, Sloane (1982C) per ottenere altre costruzioni di Λ, come sottoreticolo dei reticoli di Lorentz $Z^{24,1}$ e $Z^{25,1}$: e.g., Λ si può considerare come l'insieme dei vettori di $Z^{24.1}$ ortogonali al vettore $x = (3,5,7,\ldots,47,51|145)$.)

e) Sia $E = \mathbb{R}^8$, riferito a una base ortonormale $\{e_i \mid i \in \Delta\}$, e sia $\Gamma = \langle e_i \pm e_j, \ (\frac{1}{2}) \Sigma_{i \in \Delta} e_i \mid i,j \in \Delta \rangle = \{\Sigma x_i e_i \mid 2x_i \in Z, \ x_i - x_j \in Z, \ \Sigma_{i \in \Delta} x_i \in 2Z; \ i,j \in \Delta\}$ il reticolo generato dal sistema di radici E_8. $\mathrm{Aut}(\Gamma)$ è il gruppo di Weyl $W(E_8)$, e Γ è, a meno d'isometrie, l'unico reticolo pari unimodulare in E (cfr. Bourbaki (1968). Serre (1973)). Le connessioni di Γ con il reticolo di Leech Λ, già emerse, come si è accennato, in McKay (1972) e Thompson (1976), sono portate in piena luce da una recente costruzione di Lepowski, Meurman (1982), ispirata alla descrizione del codice binario esteso di Golay data da Turyn (1966) (cfr. §5,B)) e Curtis (1976) (cfr.§6,3)).

La costruzione di Lepowski, Meurman (1982) è a grandi

linee la seguente:

Per ogni $x \in \Gamma$, sia $\bar{x}$ l'immagine di x nell'applicazione canonica di Γ su $\bar{\Gamma} = \Gamma/2\Gamma$, e per ogni $z \in \mathbb{Z}$, sia $\bar{z}$ l'immagine di z nell'applicazione canonica di $\mathbb{Z}$ su GF(2). La funzione $q : x \to (1/2)(x,x)$ induce su $\bar{\Gamma}$ la forma quadratica di indice massimale $\bar{q} : \bar{x} \to \overline{q(x)}$. E' pertanto possibile decomporre $\bar{\Gamma}$ nella somma diretta di due sottospazi totalmente singolari massimali $\bar{\Phi}$, $\bar{\Psi}$ di dimensione 4 su GF(2). le cui preimmagini in Γ sono due reticoli Φ, Ψ, con $2\Gamma \subset \Phi, \Psi \subset \Gamma$, e $\Phi + \Psi = \Gamma$, $\Phi \cap \Psi = 2\Gamma$, $(x,x) \in 4\mathbb{Z}$ per ogni $x \in \Phi \cup \Psi$. Posto allora $\Gamma^3 = \Gamma_1 \perp \Gamma_2 \perp \Gamma_3$ (somma diretta ortogonale di tre copie di Γ in tre copie di $\mathbb{R}^8$), Γ^3 è un reticolo pari unimodulare di $\mathbb{R}^{24}$ che contiene il reticolo $\Lambda^\circ = \Phi_{(12)} \oplus \Phi_{(13)} \oplus \Psi_{(123)}$, ove $\Phi_{(12)} = \{(a,a,0) \mid a \in \Phi\}$, $\Phi_{(13)} = \{(b,0,b) \mid b \in \Phi\}$, e $\Psi_{(123)} = \{(c,c,c) \mid c \in \Psi\}$ sono reticoli contenuti in Γ^3, isometrici a multipli di Γ. E' $\Lambda^\circ = \{(a_1+x, a_2+x, a_3+x) \mid a_i \in \Phi,\ x \in \Psi,\ a_1+a_2+a_3 \in 2\Gamma\}$, e $(1/\sqrt{2})\Lambda^\circ$ risulta essere un reticolo pari unimodulare. privo di vettori di norma $\sqrt{2}$: pertanto, in forza di Conway (1969B) $(1/\sqrt{2})\Lambda^\circ$ è isometrico al reticolo di Leech Λ.

Dalla costruzione precedente si può ricavare la presentazione usuale di Λ, e la costruzione di Turyn (1966) del codice binario esteso di Golay. A tale scopo, conviene porre $A = PG(1,7) = GF(7) \cup \{\infty\}$, $N = \Delta \setminus Q$ (con $Q = \{\alpha^2 \mid \alpha \in GF(7)\}$), e considerare nello spazio 2^Δ i sottospazi $H1 = \langle N+\alpha \mid a \in GF(7) \rangle$, $H_2 = \langle -N-\alpha \mid \alpha \in GF(7) \rangle$. H_1, H_2 sono copie dei codici $\bar{H}a, \bar{H}a'$ (cfr. §5,B)), ed è possibile scegliere $\Phi = \langle 2e_i,\ \Sigma_{j \in A} e_j \mid i \in \Delta, A \in H_1 \rangle$ e $\Psi = \langle -2e_i + (1/2)\Sigma_{j \in \Delta} e_j,\ \Sigma_{k \in B} e_k \mid i, j \in \Delta;\ B \in H_2 \rangle$. Se ora si pone

$\Omega = \Delta \times \{1,2,3\}$, e si indica con (X,Y,Z) il sottoinsieme di Ω $(X \times \{1\}) \cup (Y \times \{2\}) \cup (Z \times \{3\})$, delle scelte fatte segue $\Lambda^\circ =$ $= \langle 2(e_i \pm e_j), (i,j \in \Omega);\ -2 \sum_{r \in (\{\infty\},\emptyset,\emptyset)} e_r + (1/2) \sum_{i \in \Omega} e_i;\ \sum_{k \in S} e_k,$ $(S \in C) \rangle$, ove $C = \langle (A,A,\emptyset),(A,\emptyset,A),(B,B,B) \mid A \in H_1, B \in H_2 \rangle \subset 2^{\Omega}$, i.e. si ottengono l'usuale presentazione di $\Lambda = (1/\sqrt{2})\Lambda^\circ$ (Leech (1967)) (ovvero, cambiando scala di $2\cdot\sqrt{2}$, la rappresentazione intera di Conway (1969A)), e la descrizione di Turyn del codice binario esteso di Golay.

Lepowski. **Meurman** (1982) contiene poi una costruzione del gruppo di Leech L. mediante un sottogruppo a-locale la cui struttura è facilmente esprimibile in funzione dell'azione del gruppo di Weyl $W(E_8)$ sui reticoli Φ e Ψ. Indicato con O_i il sottospazio di R^{24} generato da Γ_i $(i=1,2,3)$, e con ε_{O_i} e $O(24,R)$ la riflessione rispetto a O_i, il gruppo $\langle \varepsilon_{O_i} \mid i=1,2,3 \rangle$ è contenuto in L, e il sottogruppo a-locale in questione è $N_L(\langle \varepsilon_{Oi} \rangle)$, estensione spezzata di un a-gruppo speciale di tipo 2^{2+12} mediante $(C_2 \cdot A_8) \times S_3$ (e di fatto massimale in L).

2) (Sottogruppi massimali dei gruppi di Conway)

A correzione di quanto detto in II), segnaliamo che i sottogruppi massimali di Col e Co_2 sono oggi noti. In proposito notiamo che, poiché in un gruppo semplice un sottogruppo massimale è il normalizzante di un sottogruppo caratteristicamente semplice. i sottogruppi massimali di un gruppo semplice vanno ricercati fra i) i sottogruppi locali massimali; ii) i norma1 izzant i dei sottogruppi che sono prodotto diretto di gruppi semplici (non-abeliani) fra loro isomorfi. Nel caso di Col, essendo

i sottogruppi di tipo i) virtualmente noti in forza di Curtis (1980), restavano da determinare i sottogruppi di tipo ii). Recentemente R.A. Wilson a Cambridge ha determinato (facendo anche uso della classificazione generale dei gruppi semplici) i sottogruppi massimali di vari gruppi semplici, fra i quali i gruppi di Conway Col e Co_2, il gruppo di Suzuki Sz. il gruppo di Tits ${}^2F_4(2)'$, e il gruppo di Rudvalis Ru. In particolare, Wilson ha provato che un sottogruppo di tipo ii) di Col è contenuto in un sottogruppo locale. oppure in un coniugato dei seguenti sottogruppi: Co_2 $(= L_\Sigma(1,0))$; Co_3 $(=L_\Sigma(0,1))$; $PSU(6,2)\cdot S_3$ $(=Aut_{Co_1}(\Sigma(3.0)))$; $N(A_5) = (A_5 \times J_2)\cdot C_2$; $N(A_6) = (A_6 \times PSU(3,3))\cdot C_2$; $N(A_7) = (A_7 \times PSL(2,7))\cdot C_2$. Questo risultato. aggiunto all'analisi locale, consente di produrre un elenco completo di 24 classi di sottogruppi massimali di Col. Wilson determina inoltre le 11 classi di sottogruppi massimali di Co_2, e ritrova 14 classi di sottogruppi massimali di Co_3. (Cfr. Wilson (1982)).

C) I gruppi di Fischer F_{22}, F_{23}, F_{24} e F'_{24}.

1) (Costruzione dei gruppi di Fischer (Fischer (1969)).

Sia G un gruppo, e sia D una classe di involuzioni coniugate di G, tali che il prodotto di due involuzioni distinte di D abbia ordine 2 o 3. Si dice allora che D è una classe di 3- *trasposizioni* di G. Ad esempio, il gruppo simmetrico S_n, $n > 1$, è generato da una classe di 3-trasposizioni: le trasposizioni (cicli di lunghezza 2). Anche alcuni tipi di gruppi di Chevalley su GF(2) e GF(3) sono generati da una classe D di 3-trasposizio-

ni: in questi casi, D è una classe di naturali trasformazioni geometriche.

Cercando di caratterizzare i gruppi finiti generati da una classe di 3-trasposizioni, B. Fischer fu condotto alla scoperta di tre nuovi gruppi sporadici (Fischer (1969,1971)). I risultati di Fischer (1969) fanno capo alla seguente classificazione:

TEOREMA. Sia $\bar{G}$ un gruppo finito, generato da una classe $\bar{D}$ di 3-trasposizioni. e soddisfacente le condizioni: (*) $O_2(\bar{G}) \leq Z(\bar{G}) \geq O_3(\bar{G})$; (**) $\bar{G}' = \bar{G}''$. Sia $G = \bar{G}/Z(\bar{G})$, e sia $D = \bar{D}Z(\bar{G})/Z(\bar{G})$. Allora G è uno dei gruppi seguenti:

1. S_6 (e D è la classe delle trasposizioni, oppure la classe delle permutazioni prodotto di 3 cicli disgiunti di lunghezza 2);
2. S_n, con $n=5$ o $n > 6$ (e D è la classe delle trasposizioni);
3. $Sp(2n,2)$, con $n > 2$ (e D è la classe delle trasvezioni simplettiche);
4. $O^{\pm}(2n,2)$, con $n > 3$ (e D è la classe delle trasvezioni ortogonali);
5. $PSU(n,2)$ con $n > 4$ (e D è la classe delle trasvezioni unitario);
6. (a) $PO(n,3)$, con n dispari, $n \geq 5$ (e D è la classe delle riflessioni r_v, con $(v,v) = -1$);
   (b) $P\Omega(n,3)$, con n dispari, $n \geq 5$ (e D è la classe delle riflessioni r_v, con $(v,v) = 1$);
7. (a) $P\Omega^-(n,3) \cdot C_2$, con $n \equiv 2 \pmod 4$, $n > 2$ (vi sono due gruppi distinti, ma isomorfi, in $PO^-(n,3)$: uno generato dalla classe delle

riflessioni r_v, con $(v,v) = 1$; l'altro generato dalla classe delle riflessioni r_v, con $(v,v) = -1$);

(b) $PO^+(n,3)$, con $n \equiv 2 \pmod 4$, $n > 2$ (e D è la classe delle riflessioni r_v con $(v,v) = 1$, oppure la classe delle riflessioni r_v con $(v,v) = -1$);

8.(a) $P\Omega^+(n,3)) \cdot C_2$, con $n \equiv 0 \pmod 4$, $n > 4$ (e vi sono due gruppi distinti, ma isomorfi, in $PO^+(n,3)$, generati rispettivamente dalla classe delle riflessioni r_v con $(v,v) = 1$, e dalla classe delle riflessioni r_v con $(v,v) = -1$);

(b) $PO^-(n,3)$, con $n \equiv 0 \pmod 4$, $n > 4$ (e D è la classe delle riflessioni r_v con $(v,v) = 1$, oppure la classe delle riflessioni r_v con $(v,v) = -1$);

9. un gruppo semplice F_{22} di ordine $2^{17} \cdot 3^9 5^2 \cdot 7 \cdot 11 \cdot 13$ (e D è una classe di 3-trasposizioni univocamente determinata, con $|D| = 3510$);

10. un gruppo semplice F_{23} di ordine $2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$ (e D è una classe di 3-trasposizioni univocamente determinata, con $|D| = 31671$):

11. un gruppo F_{24} di ordine $222.316.52.73 \cdot 11 \cdot 13 \cdot 17 \cdot 23.29$, con $|F_{24} : F'_{24}| = 2$, e F'_{24} semplice (e D è una classe di S-trasposizioni univocamente determinata, con $|D| = 306936$).

In particolare, la classe D delle 3-trasposizioni di G è univocamente determinata, salvo che in 1.,7.(b), e 8.(b). Inoltre, nei casi 1.,2.,4.,6.(a), 7.,8.,11. G contiene un sottogruppo semplice di indice 2; negli altri casi, G è semplice.

(L'elenco precedente è redatto in modo da escludere sovrapposizioni

dovute a isomorfismi "eccezionali" quali, $S_6 \simeq Sp(4,2) \simeq PO^-(4,3)$, $S_8 \simeq O^+(6,2)$, $PSU(4,2) \simeq P\Omega(5,3)$, e $O^-(6,2) \simeq PO(5.3)$.

Per una dettagliata descrizione dei gruppi ortogonali su GF(3) che compaiono in 6.,7.,8., cfr. Wagner (1980. 1981)).

I gruppi F_{22}, F_{23} e F'_{24} sono semplici sporadici. e sono usualmente indicati come i (piccoli) *gruppi di Fischer*. La notazione dei gruppi di Fischer è motivata dal legame con i gruppi di Mathieu M_{22},M_{23} e M_{24}. Si supponga infatti che $\bar{G}$ soddisfi le ipotesi del Teorema precedente, e sia per semplicità $Z(G) = 1$, i.e. $\bar{G} = G$, $\bar{D} = D$. Sia E un insieme di *3-trasposizioni fondamentali*, i.e. un insieme massimale di elementi a due a due permutabili di D: poiché G è non risolubile, $|E| \geq 2$; inoltre $E = D \cap S$, con $S = Syl_2G$, e quindi $N_G(E)$ contiene S. Orbene, $N_G(E)$ opera come un gruppo 2-transitivo su E, e in ciascuno dei casi che si presentano la struttura di $NG(E)/C_G(E)$ può essere determinata: precisamente, $N_G(E)/C_G(E)$ è isomorfo al gruppo simmetrico $\$_E$ o al gruppo alterno A_E nei casi 1.,2.,6.,7., 8.,; a GL(n,2) nel caso 3.; all'olomorfo $[E_{2^n}]GL(n,2)$ nel caso 4.; a PSL([n/2],4) nel caso 5.; infine, nei casi 9.,10.,11. si ha $|E| = 22,23,24$, $C_G(E) = \langle E \rangle$ e $N_G(E)/\langle E \rangle$ è isomorfo a M_{22},M_{23},M_{24}, rispettivamente.

Due sono i risultati preliminari che consentono a Fischer di portare a termine la classificazione:

(i) Per ogni $d \in D$, posto $D_d = C_D(d) \setminus \{ d \}$, D_d è una classe di coniugio del sottogruppo $\langle D_d \rangle$.

Si hanno, di conseguenza, due possibilità:

1) $\langle D_d \rangle$ non soddisfa entrambe le condizioni (*),(**). Si

presentano allora i casi seguenti: a) $O_3(\langle D_d \rangle) \not\subseteq Z(\langle D_d \rangle)$, e $G \simeq S_5$; b) $\langle D_d \rangle$ è risolubile, e $G \simeq S_5$, S_6, PSU(4,2), o PSU(5.2); c) $O_2(\langle D_d \rangle) \not\subseteq Z(\langle D_d \rangle)$, e $G \simeq Sp(2n,2)$, o PSU(n.2). Si ottengono così, insieme a S_5, i casi 1.,3.,5. del Teorema.)

2) $\langle D_d \rangle$ soddisfa le condizioni (*), (**), e allora si può procedere usando argomenti induttivi.

(ii) G opera per coniugio su D come un gruppo transitivo di rango 3, e G_d ha orbite $\{d\}$, D_d e $A_d = D \setminus D_d \cup \{d\}$. Precisamente, $\langle D_d \rangle \subseteq G_d$ è transitivo su D_d (in forza di (i)), e anche su A_d.

Si può allora considerare il grafo di Sims di G, $\mathcal{G} = \mathcal{G}(D)$, relativo all'orbita D_d.

In generale, il grafo (fortemente regolare) $\mathcal{G}=\mathcal{G}$ (D) è un "3-grafo (triple-graph), i.e. un grafo in cui, indicando con $\mathcal{G}_x$ l'insieme dei vertici connessi a un vertice x. per ogni vertice $y \notin \mathcal{G}_x$ esiste uno e un solo vertice z tale che sia $\mathcal{G}_x \cap \mathcal{G}_y = \mathcal{G}_x \cap \mathcal{G}_z = \mathcal{G}_y \cap \mathcal{G}_z$. 1 3-grafi possono essere studiati efficacemente mediante le loro 3-mappe, i.e. le applicazioni ϕ_x (x vertice di $\mathcal{G}$) definite ponendo. per ogni vertice v di $\mathcal{G}$, $v\phi_x$ se $v \in \mathcal{G}_x$, e $v\phi_x = v$ in caso contrario. Se l'insieme $\mathcal{G}^+$ delle 3-mappe di $\mathcal{G}$ è contenuto in Aut($\mathcal{G}$), si dice che $\mathcal{G}$ è un 3-grafo *transitivo*: in tal caso $\Pi(\mathcal{G}) = \langle \mathcal{G}^+ \rangle$ è un sottogruppo di Aut($\mathcal{G}$).

In particolare, si può dare una definizione naturale di "estensione centrale" di un 3-grafo, e stabilire, in certe condizioni, teoremi di esistenza e unicità per una tale estensione.

Questi teoremi, applicati al grafo orbitale $\mathcal{G}(D_d)$ di $< D_d>/Z(< D_d>)$, consentono allora di costruire in modo unico un 3-grafo transitivo Y(D), con $\mathcal{G}_d = \mathcal{G}(D_d)$, e di identificare G come gruppo di automorfismi di $\mathcal{G}(D)$.

Nell'ipotesi che $< D_d >$ soddisfi le condizioni (*), (**) del Teorema, occorre considerare i casi seguenti:

i) $< D>/Z(< D_d >) \simeq S_n$, $n \geq 5$. Allora $G \simeq S_{n+2}$, oppure n=6 e $G \simeq W(E_6) \simeq O^-(6,2)$.

ii) $< D_d>/Z(< D_d>) \simeq Sp(2n,2)$, $n > 2$. Allora $Ci \simeq O^{\pm}(2n+2,2)$.

iii) $< D_d>/Z(< D_d>)$ è isomorfo a uno dei gruppi ortogonali che appaiono in 6., 7.. 8., in dimensione n. Allora G è uno dei gruppi ortogonali in 6.. 7., 8.. in dimensione (n+1).

iv) $< D_d>/Z(<D_d>) \simeq O^+(2n,2)$. Allora $n \leq 3$ e ci si riconduce a casi già esaminati, "via" isomorfismi eccezionali.

v) $< D_d>/Z(<D_d>) \simeq PSU(,n,2)$, con $n > 4$, $n \neq 6$. In questo caso, non si ottiene alcun gruppo G soddisfacente le condizioni del Teorema.

(In ciascuno dei casi i). ii), iii) ,iv) il 3-grafo orbitale $\mathcal{G}(D_d)$ determina univocamente il grafo orbitale $\mathcal{G}(D)$ di G. $\mathcal{G}(D)$ è un 3-grafo transitivo, estensione di $\mathcal{G}(D_d)$, e coincide con il grafo orbitale della rappresentazione "naturale" di G; in particolare, D è una classe "naturale" di 3-trasposizioni di G.)

vi) $< D_d>/Z(< D_d >) \simeq PSU(6,2)$. Allora $C_G(d) = <D_d> = <d> \cdot PSU(6,2)$, e $G \simeq F_{22}$.

Più precisamente: $G = \langle D \rangle = \Pi(\mathcal{G}_1)$, dove $\mathcal{G}_1$ è un J-grafo transitivo, estensione centrale di $\mathcal{G}(D_d)$ $(D_d Z(\langle D_d \rangle)/Z(\langle D_d \rangle)$ = trasvezioni unitarie di $PSU(6,2))$. $\mathcal{G}_1$ è univocamente determinato da (D_d), $D = \mathcal{G}_1^+$ è l'unica classe di 3-trasposizioni di G; $|D| = 1+|D_d|+|A_d| = 1+693+$ $+2816=3510$. Inoltre $Aut(\mathcal{G}_1) = Aut(F_{22})$, e $|Aut(F_{22}):F_{22}| = 2$.

vii) $\langle D_d \rangle/Z(\langle D_d \rangle) \simeq F_{22}$. Allora $C_G(d) = \langle D_d \rangle = \langle d \rangle F_{22}$, e $G \simeq F_{23}$. Più precisamente: $G = \langle D \rangle = \Pi(\mathcal{G}_2)$, dove $\mathcal{G}_2$ è un 3-grafo transitivo. estensione centrale del grafo $\mathcal{G}_1$. $\mathcal{G}_2$ è univocamente determinato da $\mathcal{G}_1 = \mathcal{G}(D_d)$, $D = \mathcal{G}_2^+$ è l'unica classe di 3-trasposizioni di $G; |D| = 1+|D_d|+|A_d| = 1+3510+$ $28160=31671$. Inoltre $Aut(\mathcal{G}_2) = \Pi(\mathcal{G}_2) = F_{23}$.

viii) $\langle D_d \rangle/Z(\langle D_d \rangle) \simeq F_{23}$. Allora $C_G(d) = \langle D_d \rangle = \langle d \rangle \times F_{23}$, e $G \simeq F_{24}$. Più precisamente: $G = \langle D \rangle = \Pi(\mathcal{G}_3)$, dove $\mathcal{G}_3$ è un 3-grafo transitivo, estensione centrale di $\mathcal{G}_2$. $\mathcal{G}_3$ è univocamente determinato da $\mathcal{G}_2 = \mathcal{G}(D_d)$, $D = \mathcal{G}_3^+$ è l'unica classe di 3-trasposizioni di $G; |D| = 1 + |D_d| + |A_d| = 1+31671+275264 =$ $= 306936$. Inoltre $|G : G'| = 2$, $G' = F_{24}'$ è semplice, e $Aut(F_{24}') = F_{24}$.

Si ha infine:

ix) $\langle D_d \rangle/Z(\langle D_d \rangle) \not\simeq F_{24}$. (E ciò completa la classificazione dei gruppi generati da 3-trasposizioni, soddisfacenti le condizioni (*) e (**).)

11) (Generalizzazioni, grandi gruppi di Fischer)

La linea di ricerca iniziata da B.Fischer, e sviluppata dallo stesso Fischer, da M. Aschbacher e da F.Timmesfeld, ha avuto un impatto notevole sia nell'ambito ristretto della ricerca

di gruppi sporadici, sia nel quadro generale della classificazione dei gruppi semplici finiti. Descrivere in dettaglio questi sviluppi, sfociati nella costituzione di ciò che Aschbacher ha chiamato una "teoria dei gruppi finiti", basata sull'analisi della loro "geometria interna". non rientra negli scopi della nostra trattazione. Su tale argomento rimandiamo perciò alle note originali, e, per una visione d'insieme, all'ampia "survey" contenuta in Gorenstein(l982). Ci limitiamo qui ad alcune concise segnalazioni:

1) Aschbacher (1972.1973). prendendo le mosse da Fischer(1969), ha classificato i gruppi finiti G, privi di sottogruppi normali risolubili non banali e con $G' = G''$, generati da una classe d i *trasposizioni dispari*, i.e. una classe D di involuzioni coniugate, tali che il prodotto di due elementi distinti di D ha ordine 2. o un numero dispari. Oltre ai gruppi generati da 3-trasposizioni, Aschbacher caratterizza così i gruppi simplettici, unitari e ortogonali su $GF(2^t)$, con $t > 1$ (e in tal caso, D è una classe di trasvezioni); dei gruppi ortogonali su GF(5), con D costituita da riflessioni: i gruppi di Suzuki $Sz(2^t)$; e dei prodotti intrecciati $PSL(2,2^t) \wr S_n$, con $t > 1$.

2) Timmesfeld (1970,1973,1975A) ha caratterizzato i gruppi finiti generati da una classe di Involuzioni *radicali* (root involutions), i.e. da una classe D di involuzioni coniugate, tali che: a) il prodotto di due elementi distinti di D ha ordine 2,4, 0 un numero dispari; b) se $x,y \in D$, e $o(xy) = 4$, allora $(xy)^{\pm 1} \in D$. Il termine "involuzione radicale" è mutato dalla teoria di

Lie: in ogni gruppo di Chevalley G definito su $GF(2^t)$, $G \neq {}^2F_4(2^t)$, gli elementi radicali $x_r(k), k \in GF(2^t)$, relativi alle radici lunghe del sistema radicale Φ di G, formano appunto una classe di "involuzioni radicali". Inversamente, Timmesfeld prova che un gruppo finito, non lontano dalla semplicità e generato da involuzioni radicali, è "quasi sempre" un gruppo di Chevalley in caratteristica 2.

In forza di Fischer(1969) e Aschbacher(1972,1973), Timmesfeld si può ridurre al caso in cui la classe D sia *non degenere*, i.e. contenga effettivamente involuzioni il cui prodotto ha ordine 4.

Timmesfeld (1975A) prova il seguente:

TEOREMA; Se G è un gruppo finito, con $O_2(G)=Z(G)=1$, generato da una classe non degenere D di involuzioni radicali, allora: 1) G è un gruppo di Chevalley su $GF(2^t)$, con l'esclusione di $PSU(n,2^t)$, $Sz(2^t)$, e ${}^2F_4(2^t)$; 2) $G = A_6$; 3) $G = J_2$ (il secondo gruppo di Janko).

La classe D è univocamente determinata nei vari casi, salvo che per $G=F_4(2^t)$. In particolare, se G è un gruppo di Chevalley. diverso da $Psp(2n,2^t)$ e da $F_4(2^t)$, D è la classe degli elementi radicali di G, relativi alle radici lunghe di G. Se $G = Psp(2n,2^t)$, D è la classe degli elementi radicali relativi alle radici corte di G; se $G = F_4(2^t)$, D è la classe degli elementi radicali relativi. alle radici lunghe, oppure quella degli elementi radicali relativi alle radici corte di G. (Si noti che in 1) $PSU(n,2^t)$ e $Sz(2^t)$ sono esclusi perché generati da una classe degenere di involuzioni radicali. Inoltre: $Psp(2n,2^t) \simeq P\Omega(2n+1,2^t)$, e in tale isomorfismo si scambiano radici corte e radici lunghe).

3) In Timmesfeld (1975A) il punto centrale è la costruzione.

all'interno di G, di una classe di sottogruppi coniugati, che possa poi essere identificata in generale con una classe di sottogruppi radicali $X_r (r \in \Phi)$ di un gruppo di Chevalley G^*. La classe adatta allo scopo è quella costituita dai sottogruppi X_d di G, dove, per ogni $d \in D$, $X_d = C_d \cup \{1\}$, e $C_d = \{x \in D | C_D(d) = C_D(x)\}$ (in particolare, $X_d = X_c$ se $c \in C_d$).

Da questo punto di vista, i risultati citati di Fischer, Aschbacher, Timmesfeld si collocano nel più ampio contesto della classificazione dei gruppi finiti generati da un *sistema di sottogruppi radicali*, i.e. da un insieme R di sottogruppi, invariante per coniugio, che soddisfi le condizioni seguenti: a) ogni elemento di R è un gruppo abeliano elementare di ordine $q=p^n$; b) per ogni $X \neq Y$ e R, $\langle X,Y \rangle$ è uno dei gruppi seguenti: i) un gruppo abeliano elementare di ordine q^2; ii) un gruppo di ordine q^3, con $[X,Y]$ e R; iii) SL(2.q). Nel caso p=2, la classe $R = \{X_d \; d \in D\}$ è appunto un tale sistema di sottogruppi radicali per G, e i risultati precedenti contengono sostanzialmente la classificazione richiesta. Il caso p dispari, $p \geq 5$. corrisponde essenzialmente alla situazione descritta dalle cosiddette "coppie quadratiche", analizzate in un famoso (e mai pubblicato) lavoro di J.G. Thompson (cfr. Thompson (1970)). Thompson, valendosi di metodi della teoria della rappresentazione, ha classificato 1 gruppi in questione, provando che ci si può ridurre all'ipotesi che siano quasisemplici. e che in tal caso sono dei gruppi di Chevalley su $GF(p^n)$. Più recentemente B. Stark (1977) ha provato che, se G è un gruppo quasisemplice generato da un sistema R di p-sottogruppi radicali, con $p \geq 5$, R è una classe

di sottogruppi coniugati di G, e G contiene un sottogruppo $H \simeq SL(2,p^n)$, subnormale nel centralizzante in G della sua (unica) involuzione. Il fatto che G sia un gruppo di Chevalley s u $GF(p^n)$ risulta allora immediata conseguenza del "teorema dell'involuzione classica" di Aschbacher (1977A) (un teorema centrale nella classificazione dei gruppi semplici, cfr. §8). Tenendo conto di un risultato di Aschbacher. Hall (1973). gli argomenti di Stark (1977) si estendono al caso p=3, n=1, mentre un risultato di Aschbacher (1974) dispone del caso $q=3^n > 3$. quando $\langle X,Y\rangle \simeq SL(2,3^n)$ per ogni $X \neq Y \in R$. In conclusione dunque, salvo una lacuna nel caso $q=3^n > 3$, i gruppi (non lontani della semplicità) generati da un sistema di sottogruppi radica1 i, sono sostanzialmente noti: essi sono, "in generale ", gruppi di Chevalley su GF(q).

4) Dal suo teorema delle involuzioni radicali, Timmesfeld ha dedotto risultati sui sottogruppi debolmente chiusi e a intersezioni banali nei gruppi semplici, di importanza fondamentale per la classificazione dei cosiddetti "gruppi di tipo-caratteristica 2" (cfr. ad es. Gorenstein (1982)). In particolare, menzioniamo il seguente:

TEOREMA (Timmesfeld (1975B)). Sia G un gruppo semplice, e si supponga che G contenga un 2-sottogruppo abeliano elementare $A \neq \{1\}$, soddisfacente le condizioni seguenti: i) per ogni $g \in G$, $A \cap A^g = \{1\}$, oppure $A \cap A^g = A$ (i.e. A è un sottogruppo "a intersezioni banali"); ii) p e r ogni $A^g \neq A$, $A \not\leq C_G(A^g)$. Allora G è uno dei gruppi seguenti: 1) $PSL(n,2^t)$; 2) $Sz(2^t)$; 3) $PSU(3,2^t)$; 4) A_n, con $6 \leq n \leq 9$; 5) M_{22}, M_{23}, M_{24}.

5) La caratterizzazione dei gruppi generati da 3-trasposizioni è all'origine della scoperta dei "grandi gruppi di Fischer" F_2 e Fl:

(i) F_2 fu scoperto da B. Fischer nel corso del tentativo di ampliare la sua analisi. considerando gruppi generati da una classe di (3,4)-trasposizioni, i.e. da una classe D di involuzioni coniugate, tali che il prodotto di due elementi distinti di D abbia ordine 2,3, oppure 4. Fra tali gruppi (per i quali non esiste tuttora un teorema generale di classificazione) vi è $Aut(F_{22})$ $(=[F_{22}]C_2)$, il quale è generato da una classe D di (3,4)-trasposizioni che inducono automorfismi esterni di F_{22} (e non sono involuzioni radicali. venendo meno la condizione b) della definizione). Sulla base della convinzione, suffragata da evidenti indizi, che $Aut(F_{22})$ fosse un sottogruppo del gruppo $(C_2 \cdot {}^2E_6(2)) \cdot C_2$, e di tecniche di estensione analoghe a quelle elaborate per la costruzione di F_{22}, F_{23} e F_{24}, Fischer fu condotto a supporre l'esistenza di un gruppo semplice G, generato da una classe di (3,4)-trasposizioni $\tilde{D}$ contenente D, e tale che, per ogni $\tilde{d}$ e $\tilde{D}$, $C_G(\tilde{d})$ fosse isomorfo a $(C_2 \cdot {}^2E_6(2)) \cdot C_2$. Fischer esplorò in dettaglio la struttura di un eventuale gruppo G, mostrando fra l'altro che G doveva operare per coniugio come un gruppo di rango 5 su $\tilde{D}$, con $|\tilde{D}| = 13.571.955.000$. Ciò permise a J. Leon e C. Sims (Leon, Sims (1977)) di costruire G ricorrendo all'uso di un computer, e di provarne l'unicità. G è un gruppo semplice sporadico di ordine $2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$, noto anche come "Baby monster" e usualmente denotato con F_2. F_2 è, per quanto si è detto, univocamente determina-

to dalla struttura del centralizzante di una sua (3,4)-trasposizione. Oltre a $\tilde{D}$, F_2 contiene una seconda classe di involuzioni (centrali), con centralizzante isomorfo a $2_+^{1+22}\cdot Co_2$ (cfr. B),III)).

(ii) La questione dell'esistenza di un eventuale gruppo semplice G, contenente un'involuzione z con $CG(z) = \langle z \rangle \cdot F_2$, ha condotto alla scoperta del gruppo sporadico F_1, di ordine $2^{46}\cdot 3^{20}\cdot 59\cdot 76\cdot 112\cdot 133\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$, noto come "Monster", e più recentemente ribattezzato da Griess con il nome di "Friendly Giant". F_1 è il più grande dei gruppi sporadici, i quali si presentano come sottogruppi 0 sezioni di F_1, ad esclusione di J_3, Ly, Ru. O'N e J_4. La dimostrazione dell'esistenza e dell'unicità di un gruppo F_1 soddisfacente le condizioni richieste ha coinvolto vari specialisti (in particolare, Fischer, Thompson, Conway, Harada, Norton, S.Smith. Livingstone, Griess). Si è già accennato (cfr. B), 111)) alla costruzione di F_1, dovuta a Griess (1982); per una descrizione sommaria cfr. anche Gorenstein (1982).

111) (Struttura di F_{22}, F_{23} e F_{24}; caratterizzazioni)

1) In base alla costruzione delineata in 1), F_{22}, considerato come gruppo di permutazioni sulla classe D delle 3-trasposizioni, è estensione transitiva di rango 3 di $C_2\cdot PSU(6,2)$, con parametri 693 e 2816. Un insieme E di 3-trasposizioni fondamentali ha cardinalità 22. $\langle E \rangle = C_{F_{22}}(E)$ è un gruppo abeliano elementare di ordine 2^{10}, e $N_{F22}(E)/\langle E \rangle$ è isomorfo a M_{22}. Come M_{22}-modulo, $\langle E \rangle$ è isomorfo al modulo $2^{\Omega}/\langle C, 2^{\Omega}\rangle$ <C,{∞},{0}> considerato in §11,B).

In particolare: i) posto E= (dl,. . . ,d_{22}} , l'azione di M_{22} su E è quella naturalmente indotta dall'azione sui punti di S(3.6.22): i blocchi di S(3,6,22) sono i 6-sottoinsiemi J di {1,...,22} per i quali $\prod_{j\in J} d_j = 1$; ii) $N_{F_{22}}(E)$ ha 3 orbite su <E>\{1}: una è ovviamente E, una seconda orbita di lunghezza $22\cdot 21/2=231$ è costituita dai prodotti $d_i d_j$ ($1 \leq i,j \leq 22$), la terza orbita, di lunghezza $22\cdot 21\cdot 20/(3!\cdot 2)=770$, è costituita dai prodotti $d_i d_j d_k$ ($1\leq i,k\leq 22$); iii) $N_{F_{22}}(E)$ ha 3 orbite sulla classe D (Conway (1972)): una è E; un'altra è costituita da $2^5\cdot 77$ 3-trasposizioni, ciascuna delle quali commuta con esattamente 6 elementi di E. costituenti un blocco di S(3,6,22) (2^5 per ogni blocco); la terza orbita è costiuita da 210 3-trasposizioni. ciascuna delle quali non commuta con alcun elemento di E. Lo stabilizzante di un punto della terza orbita è un sottogruppo di indice 2^{10} in $N_{F_{22}}(E)$, isomorfo a M_{22}: pertanto $N_{F_{22}}(E) = [<E>]M_{22}$ è un'estensione spezzata.

2) F_{23}, considerato come gruppo di permutazioni sulle classe D delle 3-trasposizioni. è estensione transitiva di rango 3 di $C_2\cdot F_{22}$, con parametri 3510 e 28160. Un insieme E di S-trasposizioni fondamentali ha cardinalità 23. $<E>=C_{F_{23}}(E)$ è un gruppo abeliano elementare di ordine 2^{11}, e $N_{F_{23}}(E)/<E>$ è isomorfo a M_{23}. L'estensi2ne $<E>\cdot M_{23}$ non è spezzata: considerato come M_{23}-modulo, <E> è isomorfo al modulo $2^{\Omega}/<C,\{\infty\}>$ descritto in §11,B). In particolare i) posto E = { $d_0,d_1,\ldots,d_{22}$} , l'azione di M_{23} su E è quella naturalmente indotta dall'azione sui punti di S(4,7,23): i blocchi di S(4,7,23) sono i 7-sottoinsiemi J di {0,1,...,22} per i quali $\prod_{j\in J} d_j = 1$; ii) $N_{F_{23}}(E)$ ha 3 orbite su <E>\{1}: una è E; un'altra è costituita dai prodotti $d_i d_j$ ($0 \leq i, j \leq 22$). e ha lunghezza $23\cdot 22/2 = 253$; la terza è costituita dai prodotti

$d_i d_j d_k$ ($0 \leq i,j,k \leq 22$), e ha lunghezza $23 \cdot 22 \cdot 21/3! = 1771$; iii) $N_{F_{23}}(E)$ ha 3 orbite su D: E; un'orbita di lunghezza $2^5 \cdot 253$, costituita da 3-trasposizioni che commutano con un blocco di $S(4,7,23)$, 2^5 per ogni blocco; e un'orbita di lunghezza $2^{10} \cdot 23$, costituita da S-trasposizioni che commutano con un unico elemento di E. 2^{10} per ogni elemento di E.

3) F_{24}, considerato come gruppo di permutazioni sulla classe D delle 3-trasposizioni, è estensione transitiva di rango 3 di $C_2 \times F_{23}$, con parametri 31671 e 275264. Un insieme E di 3-trasposizioni fondamentali ha cardinalita 24. $\langle E \rangle = C_{F_{24}}(E)$ è un gruppo abeliano elementare di ordine 212. e $N_{F_{24}}(E)/\langle E \rangle$ è isomorfo a M_{24}. L'estensione $\langle E \rangle \cdot M_{24}$ non è spezzata: come M_{24}-modulo, $\langle E \rangle$ è isomorfo al modulo $C^* = 2^{\Omega}/C$ descritto in §11,B). In particolare: i) posto $E = \{d_0, d_1, \ldots, d_{22}, d_\infty\}$, l'azione di M_{24} su E è quella naturalmente indotta dall'azione sui punti d i S(5,8,24): i blocchi di S(5,8,24) sono gli 8-sottoinsiemi J di $\{0,1,\ldots,22,\infty\}$ per i quali $\prod_{j \in J} d_j = 1$; ii) $N_{F_{24}}(E)$ ha 4 orbite su $\langle E \rangle \setminus \{1\}$, di lunghezze 24,276,2024 e 1771: una è E, e le altre sono costituite rispettivamente dai prodotti $d_i d_j$, $d_1 d_j d_k$, $d_i d_j d_k d_\ell$ ($i,j,k,\ell \in \{0,1,\ldots,22,\infty\}$); i i i) $N_{F_{24}}(E)$ ha 3 orbite su D: una è E; un'altra è costituita da $2^5 \cdot 759$ 3-trasposizioni, ciascuna delle quali commuta con un' ottade d i S(5,8,24), 2^5 per ogni ottade; la terza orbita è costituita da $2^{10}\binom{24}{2}$ J-trasposizioni, ciascuna delle quali commuta con una coppia univocamente determinata di elementi di E, 210 per ogni coppia.

4) Anche F'_{24} (che non contiene 3-trasposizioni) può considerar-

si come gruppo di permutazioni su D. estensione transitiva di rango 3 e F_{23}, con parametri 31671 e 275264. Gli elementi di $<E> = <d_0,d_1,\ldots,d_{22},d_\infty>$ che appartengono a F'_{24} sono, oltre A 1, i prodotti di un numero pari di elementi di E, i.e. gli elementi della forma d_id_j e $d_id_jd_kd_\ell$. Tali elementi formano un sottogruppo H di $<E>$ di ordine 2^{11}, con $F'_{24} \cap N_{F_{24}}(E) = H \cdot M_{24}$. L'estensione è non spezzata. e come M_{24}-modulo H è isomorfo al modulo V* considerato in §11,B).

5) (Centralizzanti di involuzioni)

F_{22} ha tre classi di involuzioni: i) la classe D delle 3-trasposizioni; ii) una classe T di involuzioni centrali, i cui elementi sono prodotto di due elementi di D; iii) una classe N, ogni elemento della quale è prodotto di tre elementi di D. F_{22} è stato caratterizzato mediante il centralizzante di una 3-trasposizione da Hunt (1972), e mediante il centralizzante di un elemento di T da Parrott (1981). (Se $t \in T$ e $H = C_{F_{22}}(t)$, si ha $O_2(H) = C_2 \times 2^{1+8}_+$, con $O_2(H)' = <t>$ e $C_H(O_2(H)) \subseteq O_2(H)$, e $H/O_2(H) = \mathrm{Aut}Psp(4,3)$.) Infine, il centralizzante di un elemento di N è un gruppo risolubile di ordine $2^{16} \cdot 3^3$.

Tutte le involuzioni di F_{23} sono centrali, e si distribuiscono in tre classi, analoghe a quelle di F_{22}: i) la classe D delle S-trasposizioni; ii) una classe T, i cui elementi sono prodotto di due elementi di D; iii) una classe N i cui elementi sono prodotto di tre elementi di D. F_{23} è stato caratterizzato mediante il centralizzate di una 3-trasposizione da Hunt (1973). e mediante il centralizzante di un elemento di T da Parrott (1981). (Se $t \in T$ e $H = C_{F_{23}}(t)$, si ha $O_2(H) = E_{2^2} \times 2^{1+8}_+$, con $O_2(H)' =$

$= \langle t \rangle$ e $C_H(O_2(H)) \subseteq O_2(H)$, e $H/O_2(H) = C_3 \cdot \mathrm{AutPsp}(4,3)$.) Infine, il centralizzante C di un elemento di N ha la struttura $C = (E_{22} \cdot \mathrm{PSU}(6,2))C_2$, con $C' = E_{22} \sim \mathrm{PSU}(6.2)$ estensione perfetta.

F_{24} ha quattro classi di involuzioni: la classe D delle 3-trasposizioni e tre classi T,N,S costituite da involuzioni che sono prodotto di due, tre, quattro elementi di D, rispettivamente. F'_{24} ha due classi di involuzioni: T e S. Il centralizzante in F'_{24} di un' involuzione t della classe T è il ricoprimento $\langle t \rangle \cdot \mathrm{Aut}(F_{22})$. Le involuzioni della classe S sono centrali, e, posto $H = C_{F'_{24}}(s)$, $s \in S$, si ha $O_2(H) = 2_+^{1+12}$, con $C_H(O_2(H)) \subseteq O_2(H)$, e $H/O_2(H) = (C_3 \cdot \mathrm{PSU}(4,3))C_2$. F'_{24} e F_{24} sono stati caratterizzati mediante la struttura di H da Parrott (1981).

6) (D-sottogruppi)

Bnright (1977A) ha provato che F_{22} contiene un sottogruppo $S \simeq S_{10}$, il quale, considerato come gruppo di permutazioni su D, ha tre orbite A,B,C di lunghezze 45,1575,1850 rispettivamente. In particolare, $A = S \cap D$ coincide con la classe delle trasposizioni di S_{10}. Assegnando dei nomi agli elementi di D, che riflettono l'azione di S, è possibile calcolare esplicitamente gli elementi d^x, per ogni $d,x \in D$ (i.e. l'intera "tavola di coniugio" di F_{22}). Bnright (1977A) migliora in modo sostanziale un risultato di Conway (1972), che, basandosi su una descrizione di F_{22} in termini di $N_{F_{22}}(E) = [\langle E \rangle]M_{22}$, ha prodotto una tavola di coniugati d^x, con $x \in E \cup \{v\}$, $v \in \langle E \rangle$, e $F_{22} = \langle E, v \rangle$.

Bnright (19778) ha ottenuto con tecniche analoghe la "tavola

di coniugio" di F_{23}. In questo caso, si assegnano agli elementi di D dei nomi che riflettono l'azione su D di un sottogruppo $\Sigma \simeq S_{12}$. Σ ha quattro orbite su D: tre orbite A,B,C analoghe a quelle di S in F_{22}, di lunghezze 66,5775,20790 (e $A = \Sigma \cap D$ è la classe delle trasposizioni di S_{12}), e una quarta orbita L, con $|L| = 5040$. e $C_\Sigma(\ell)$, $\ell \in L$, isomorfo a M_{12}.

Usando in modo sistematico le "tavole di coniugio" di F_{22} e F_{23}, Enright (1978) ha determinato tutti i D-sottogruppi di F_{22} e F_{23}, i.e. i sottogruppi H generati da un sottoinsieme $D_0 \subset D$ tale che D_0 è una classe di coniugio di H, e soddisfacenti le condizioni (*) e (**) del Teorema di Fischer (1969).

7) (Caratterizzazioni P-locali)

F_{22} contiene un sottogruppo 2-locale, estensione spezzata di E_{26} mediante il gruppo simplettico Sp(6,2). Assa (1981) ha provato che, se un gruppo semplice finito G contiene un sottogruppo abeliano elementare E_{26}, con $C_G(E_{26}) = E_{26}$ e $N_G(E_{26})/E_{26} \simeq Sp(6,2)$, allora l'estensione è spezzata e $G \simeq F_{22}$.

F_{23} è stato caratterizzato da Wong S.K. (1977) mediante il sottogruppo 2-locale $NF_{23}(E)$. Si ha il seguente:

TEOREMA. Sia G un gruppo finito, con $O(C_G(z)) = 1$ per ogni involuzione z di G. Se G contiene un sottogruppo abeliano elementare E_{211}, con $C_G(E_{211}) = E_{211}$ e $N_G(E_{211})/E_{211} \simeq M_{23}$, allora $G \simeq N_G(E_{211})$ oppure $G \simeq F_{23}$.

Fi4 è stato caratterizzato da Reifart (1977A) mediante il sottogruppo 2-locale $N_{F'_{24}}(E) = H \cdot M_{24}$ (cfr. 4)). Per tale caratterizzazione, che stabilisce uno stretto legame tra F'_{24}

e il gruppo di Janko J_4, cfr.D). F'_{24} contiene inoltre un sottogruppo Z-locale massimale M della forma $2^{3+12}(A_6 \times PSL(3,2))$ $M = N_{F'_{24}}(Z)$, dove $Z = Z(O_2(\tilde{N})) \simeq E_{23}$ e $\tilde{N}$ è la preimmagine in $N_{Fi4}(E)$ dello stabilizzante di un trio in M_{24}). Riconducendosi a Reifart (1977A). Bierbrauer (1980) ha caratterizzato F'_{24} mediante la struttura di M.

(1 gruppi di Fischer sono stati anche caratterizzati mediante sottogruppi standard (cfr.§8,E)): 1) Koch (1982) ha caratterizzato F_{22} in funzione del sottogruppo standard $O^+(8,2)$; 2) Davis, Solomon (1981) hanno caratterizzato: i) F_{22} (e $Aut(F_{22})$) in funzione del sottogruppo standard $C_2 \cdot PSU(6,2)$, ii) F_{23} e F'_{24} in funzione del sottogruppo standard $C_2 \cdot F_{22}$.)

8)

Le tavole dei caratteri dei gruppi di Fischer sono note. In particolare, la tavola dei caratteri di F_{22} è stata calcolata da Hunt (1971). che ha anche calcolato la tavola di $P\Omega(8,3) \subseteq F_{23}$ (Hunt (1974A)), e quindi quella di F_{23} (Hunt (1974B)). Pahlingts (1974) ha provato che i gruppi generati da 3-trasposizioni classificati da Fischer (1969). e quindi in particolare F_{22}, F_{23} e F_{24}, sono univocamente determinati dalle rispettive tavole dei caratteri.

Moori (1981,1982) ha determinato classi di coniugio e tavole dei caratteri del gruppo $N_{F_{22}}(E) = [\langle E \rangle]M_{22}$, del suo gruppo di automorfismi $N_{Aut(F_{22})}(E) = [\langle E \rangle]Aut(M_{22})$, e di $Aut(O^+(8,2))$, centralizzante in F_{22} di un'involuzione di $Aut(F_{22})$. I moltiplicatori di Schur dei gruppi di Fischer sono stati calcolati da Griess (1974). F_{22} ha moltiplicatore ciclico di ordine 6. F_{23} e F_{24} hanno moltiplicatore banale, F'_{24} ha moltiplicatore di ordine 3.

9) Una geometria Z-locale per F'_{24} è descrtta i n Ronan,Smith(1980).

D) Il gruppo di Janko J_4.

1) I gruppi di Janko J_2 e J_3 furono scoperti da Janko (1968C) mediante un centralizzante d'involuzione. Precisamente, vale il seguente: TEOREMA. Se G è un gruppo semplice finito, contenente un'involuzione z tale che sia $C_G(z)=P\cdot A_5$, ove P è un Z-gruppo extraspeciale di ordine 2^{1+4} e tipo -, allora $G \simeq J_2, J_3$. In particolare. in tale situazione, si ha: i) $O_2(C_G(z))=P$, e ii) $C_G(P)=\langle z\rangle$. Janko fu allora condotto a formulare il cencetto di *sottogruppo extraspeciale* ampio (large): un p-sottogruppo extraspeciale P di un gruppo finito G si dice ampio se $F^*(C_G(Z(P)))=P$ (o equivalentemente: i) $O_2(C_G(Z(P)))=P$, e ii) $C_G(P) \subseteq P$). E a porre il cosiddetto "problema extraspeciale": determinare i gruppi semplici contenenti 2-sottogruppi extraspeciali ampi. La soluzione di questo problema ha avuto un ruolo rilevante nel processo generale di classificazione dei gruppi semplici, e si deve ai contributi di vari autori (fra gli altri. lo stesso Janko, e M.Aschbacher, F.Tummesfeld (con una nota fondamentale in cui il problema viene ridotto alla soluzione di otto casi legati a configurazioni specifiche ((Timmesfeld (1978))),A.Reifart, G.Stroth, F.Smith, S.D.Smith, Tran Van Trung). Per una breve "survey" sul l' argomento, cfr. S.D. Smith (1980C). e per un elenco di tutti i gruppi semplici contenenti 2-sottogruppi extraspeciali ampî, cfr. S.D. Smith (1979): ne risulta che la maggior parte dei gruppi sporadici (15 su 26, inclusi F_2 e F_1), e dei gruppi di Chevalley su GF(2), contengono 2-sottogruppi extraspeciali ampi. (In particola

re. tali sottogruppi esistono nei gruppi di Mathieu M_{11}, M_{12} e M_{24}. Infatti: 1) il centralizzante di un'involuzione di Mll è isomorfo a $GL(2,3) = [Q_8]S_3$, e basta porre P = Q,; 2) il centralizzante di un'involuzione centrale di M_{12} è isomorfo all'olomorfo di Q_8, e si può perciò considerare come estensione di $Q_8 * Q_8 = 2_+^{1+4}$ mediante S_3: basta allora porre $P = Q_8 * Q_8$; 3) il centralizzante di un'involuzione centrale di M_{24} è prodotto semidiretto di un gruppo extraspeciale $D_8 * D_8 * D_8 = 2_+^{1+6}$ mediante PSL(3,2), e basta porre $P = D_8 * D_8 * D_8$.)

Il "problema extraspeciale" ha condotto Janko, diversi anni dopo la scoperta di J_2 e J_3, alla scoperta di un nuovo gruppo speradico. il "quarto gruppo di Janko" J_4. Precisamente, Janko (1976) prova il seguente:

TEOREMA. Sia G un gruppo semplice finito, z un'involuzione di G, H = CG(z). Se: i) $O_2(H) = P$ e $CH(P) \subseteq P$, con P 2-gruppo extraspeciale di ordine 2^{1+12} e tipo + (P è ampio in G); ii) posto $S = Syl_3(O_{2,3}(H))$, $|S| = 3$ e $C_P(S) = \langle z \rangle$; iii) $H/O_{2,3}(H) \simeq Aut(M_{22})$, $N_H(S) \neq C_H(S)$, e $S \subseteq (C_H(S))'$; allora 1) $|G| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 113 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$. 2) $C_H(S) = C_G(S) = C_6 \cdot M_{22}$ (di indice 2 nel ricoprimento completo di M_{22}). 3) $Syl_2 G$ possiede un unico sottogruppo abeliano alementare di ordine 211, $E_{2^{11}} \cdot E_{2^{11}}$ è autocentralizzante in G, e $M = N_G(E_{2^{11}})$ è un sottogruppo massimale di G, prodotto semidiretto di $E_{2^{11}}$ per M_{24}. Come M_{24}-modulo, E_{211} è isomorfo a V* (cfr. §11,B)): in particolare, M_{24} ha due orbite su $E_{2^{11}}$ {1}, di lunghezze 1771 e 276. con rappresentanti z e t. 4) G ha due classi di involuzioni, con rappresentazioni z e t: z è centrale, e $C_G(z) = H = P \cdot N_H(S)$; t è non-centrale. e $C_G(t)$ è estensione spezzata fedele di E_{211} mediante $Aut(M_{22})$.

E inoltre: a) G ha 62 classi di elementi coniugati; b) la struttura locale di G è completamente determinata (in particolare G contiene un sottogruppo 2-locale massimale, estensione spezzata di $E_{2^{10}}$ mediante PSL(5.2) (con $E_{2^{10}}$ autocentralizzante in G, e irriducibile come PSL(5,2)-modulo), e un sottogruppo 2-locale massimale, estensione non spezzata di un a-gruppo speciale di ordine 2^{15} mediante S_5 x PSL(3,2)); c) la tavola dei caratteri di G è univocamente determinata (ed è stata calcolata da Conway, Hunt, Norton e Thompson: il grado minimo di un carattere non banale di G è 1333).

La dimostrazione dell'esistenza e dell'unicità di un gruppo "di tipo J_4" (i.e. di un gruppo G soddisfacente le condizioni del Teorema precedente) è stata completata solo nel febbraio 1980. e si deve a S.Norton, con la collaborazione di altri matematici dell'Università di Cambridge (cfr. Norton (1980)). La costruzione di Norton si basa sulla realizzazione di una rappresentazione di $G = \langle H, M \rangle$ in GL(112,2), la cui esistenza era stata suggerita da Thompson. Quanto all'unicità, essa è provata mostrando che G è un sottogruppo univocamente determinato, a meno di coniugio, di GL(1333,$\mathbb{C}$).

2) Il legame di J_4 con i gruppi di Mathieu si fonda sull'esistenza in J_4 del sottogruppo 2-locale $M = [E_{2^{11}}]M_{24}$, e dei centralizzanti d'involuzione $H = C(z) \; 2_+^{1+12} \cdot (C_3 \cdot M_{22}) \cdot C_2$ e $C(t) = [E_{2^{11}}] \; \mathrm{Aut}(M_{22})$.

Conviene riassumere qui i nessi che intercorrono, "via" M_{24}, fra Co_1, F_{24}' e J_4:

a) I gruppi Co_1, F_{24}' e J_4 contengono dei sottogruppi della

forma $E_{2^{11}} \cdot M_{24}$, estensioni fedeli di $E_{2^{11}}$ mediante M_{24}, non isomorfe tra loro. Precisamente: i) in Col 1 'estensione è spezzata, e $E_{2^{11}}$ è isomorfo come M_{24}-modulo a V (cfr. §11, B)); ii) in F'_{24} l'estensione non è spezzata, e $E_{2^{11}}$ è isomorfo come M_{24}-modulo a V*; iii) in J_4 l'estensione è spezzata, e $E_{2^{11}}$ è isomorfo come M_{24}-modulo a V*.

b) L'esistenza della configurazione 2-locale $E_{2^{11}} \cdot M_{24}$ caratterizza i gruppi semplici Co_1, F'_{24} e J_4 (Reifart (1977A, 1978)). Si ha infatti il seguente:

TEOREMA. Sia G un gruppo semplice finito. e si supponga che G contenga un sottogruppo abeliano elementare $E_{2^{11}}$, con $C_G(E_{2^{11}}) = E_{2^{11}}$ e $N_G(E_{2^{11}})/E_{2^{11}} \simeq M_{24}$. Si supponga inoltre che sia $O(C_G(z)) = 1$ per un'involuzione z, centrale in $N_G(E_{2^{11}})$. Allora si hanno due casi: i) M_{24} ha due orbite di lunghezza 759 e 1288 su $E_{2^{11}} \setminus \{1\}$, e G è isomorfo a Col (Reifart (1978)); ii) M_{24} ha due orbite di lunghezza 1771 e 276 su $E_{2^{11}} \setminus \{1\}$, e G è isomorfo a F'_{24}, oppure a J_4 (Reifart (1977A)).

(Nel caso ii), Reifart (1977A) giunge a provare che $C_G(z)/O_{2,2'}(C_G(z))$ è isomorfo a $\mathrm{Aut}(M_{22})$, oppure a un'estensione di PSU(4,3) mediante un automorfismo esterno di ordine 2. Nel primo caso, la caratterizzazione di Janko (1976) implica $G \simeq J_4$; nel secondo caso, $C_G(z)$ è isomorfo al centralizzante di un'involuzione centrale in F'_{24}, e $G \simeq F'_{24}$ in forza di Parrott (1981)).

3) J_4 ammette caratterizzazioni mediante i centralizzanti di entrambe le involuzioni z e t. Janko (1976) può infatti considerarsi come una caratterizzazione mediante il centralizzante

di z, mentre una caratterizzazione mediante il centralizzante di t è stata ottenuta da Reifart (1977B).

4) (Altre caratterizzazioni locali). Una caratterizzazione di J_4 mediante il sottogruppo 2-locale $[E_{2^{10}}]PSL(5,2)$ è stata ottenuta da Lempken (1978A) e indipendentemente, ma sotto ipotesi più forti, da G.Mason (1977). Un'altra caratterizzazione di J_4, mediante il sottogruppo L-locale $L = 2^{3+12}.(S_5 \times PSL(3.2))$ è stata invece ottenuta da Tran Van Trung (1980). (Il sottogruppo L è il normalizzante in J_4 di un a-gruppo abeliano elementare Z di ordine 2^3, dove $Z = Z(O_2(\tilde{N}))$, e $\tilde{N}$ è la preimmagine in $M = [E_{2^{11}}]M_{24}$ dello stabilizzante di un trio in M_{24}. La caratterizzazione di J_4 mediante L è simile a quella ottenuta da Bierbrauer (1980) per F'_{24}, mediante l'analogo sottogruppo $2^{3+12}.(A_6 \times PSL(3,2))$, e consiste in una riduzione alla situazione descritta da Reifart (1977A)). Infine, J_4 è stato caratterizzato anche mediante il centralizzante di un elemento di ordine 3. isomorfo a $C_6.M_{22}$ (Stafford (1979). Güloğlu (1981). e precedentemente, sotto ipotesi più forti, Stroth (1978)).

5) Il moltiplicatore di Schur di J_4 è banale (Griess. e indipendentemente Lempken (19788)). $Out(J_4) = 1$ (Finkelstein (1977C). 1 caratteri 2-modulari di J_4 sono stati investigati da Thompşon; in particolare, i 2-blocchi non-principali sono stati analizzati da Landrock (1978).

6) Finkelstein (1977C) ha provato che, se un gruppo G. con $O(G) = 1$, ha una componente standard A di tipo J_4, allora $\langle A^G \rangle = A$ oppure $\langle A^G \rangle = A \times A$.

7) Una geometria 2-locale (cfr. §12) per J_4, in cui gli stabilizzanti dei vertici sono i sottogruppi $N_{J_4}(E_{2^{11}})$, $[E_{2^{10}}]\mathrm{PSL}(5,2)$, $2^{3+12}\cdot(S_5 \times \mathrm{PSL}(3,2))$, e $C_{J_4}(z)$, è descritta in Ronan, Smith (1980).

8) Lempken (1984) ha determinato tutti i sottogruppi massimali di J_4.

BIBLIOGRAFIA

ADEMAJ E.(1978), A characterization of the simple group $L_n(2)$, Glas Math.Ser. 111. 13(33), pp. 15-37.

ALLTOP W.O. (1972), An infinite class of 5-designs, J.Comb.Theory, 12, pp. 390-395.

ALPERIN J.L., BRAUER R.. GORENSTEIN D. (1970), Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, Trans.Amer. Math. Soc., 151, pp.1-261.

ARTIN E . (1955), The orders of the classica1 simple groups, Comm. Pure Appl.Math., 8, pp. 455-472.

ASCHBACHER M. (1972). Finite groups generated by odd transpositions .I, Math.Z., 127, pp. 45-56.

- - (1973), Finite groups generated by odd transpositions. II, 111, IV, J.Algebra. 26, pp. 451-459, 460-478, 479-491.

- - (1974) $\mathcal{F}$-sets and permutation groups, J.Algebra, 30, pp. 400-416.

- - (1975). On finite groups of component type, Illinois J. Math., 19, pp. 87-115.

- - (1976A). Tightly embedded subgroups of finite groups, J. Algebra, 45, pp. 85-101.

- - (1976B), Finite groups in which the generalized Fitting group of the centralizer of some involution is symplectic but not extraspecial, Comm. Algebra, 4, pp. 595-616.

- - (1977A), A characterization of Chevalley groups over fields of odd order. 1.11, Ann.Math., 106, pp.353-468. (Correction: Ann. Math., 111, 1980, pp. 411-414.)

- - (1977B), On finite groups in which the generalized Fitting group of the centralizer of some involution is extraspecial, Illinois J.Math., 21, pp.347-364.

- - (1978), A survey of the classification program for finite simple groups of even characteristic, Proc.Int.Congr. Math.Helsinki 1978. Vol.1, pp. 281-284 (1980).

- - (1980), The finite Simple Groups and Their Classification. Yale Mathematical Monographs, 7, Yale University Press.

- - (1982). Parabolics in groups of GF(2)-type, to appear.

ASCHBACHER M.,HALL,M.Jr. (1973), Groups generated by a class of elements of order 3. **J.Algebra**, 24, pp.591-612.

ASSA S.B. (1981). A characterization of $M_{(22)}$. **J.Algebra**, 69, pp. 455-466.

ASSMUS E.F.Jr.,MATTSON H.F.Jr. (1966A), Perfect codes and the Mathieu groups, **Arch.Math.**, 17, pp. 121-135.

- - (1966B), Disjoint Steiner systems associated with the Mathieu groups, **Bull.Amer.Math.Soc.**, 72, pp.843-845.

- - (1967), On tactical configurations and error-correcting codes, **J.Comb.Theory**, 2, pp. 243 - 257.

- - (1969), New 5-designs, J.Comb.Theory. 6, pp. 122-151.

ASSMUS E.F.Jr., MEZZAROBA J.A.,SALWACH C.J. (1977). Planes and biplanes, in M.Aigner (ed.) Higher Combinatorics, Reidel Dordrecht 1977. pp. 205-212.

BANNAI E. (1973), A note on multiply transitive permutation groups, J.Algebra, 26, pp. 383-384.

- - (1974), On multiply transitive permutation groups. I,II, 111, Osaka **J.Math.**,11, pp. 401-411, 413-416. 577-586.

- - (1975). A note on multiply transitive permutation groups. 11, J.Algebra, 36, pp. 294-301.

- - (1976A), On multiply transitive permutation groups. IV. Osaka J.Math., 13, pp.123-129.

- - (1976B), Normal subgroups of 6-transitive permutation groups, **J.Algebra**, 42, pp. 46-59.

BARANYAI ZS. (1973). On the factorization of the complete uniform hypergraph, in Infinite and finite sets, Colloq. Keszthely 1973, Vol.I, pp.91-108 (Colloq. Math. Soc. J.Bolyai, 10, North Holland 1975).

BEISIEGEI B. (1974), Eine Charakterisierung einiger einfacher sporadischer Gruppen, **Rend.Sem.Mat.Univ.Padova**, 51, 1975, pp. 131-165.

- - (1977). Über einfache endliche Gruppen mit Sylow-2-Gruppen der ordnung hochstens 2^{10}, Comm. Algebra,,, pp. 113-170.

BENARD M. (1979). Schur indexes of sporadic simple groups. **J.Algebra**, 58, pp. 508-522.

BENDER H. (1968), Endliche zweifach transitive Permutations-Gruppen derer Involutionen keine Fixpunkte haben, **Math.Z.**, 104,

pp. 174-204.

- - (1971). Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlässt, J.Algebra, 17, pp.527-554.

BERGSTRAND D.J. (1982). New uniqueness proofs for the (5,8,24), (5,6,12) and related Steiner systems. J.Comb. Theory (A), 33, pp. 247-272.

BERLEKAMP E.R. (1971). Coding theory and the Mathieu groups. Inform. and Control, 18, pp. 40-64.

BETH TH. (1981). Some remarks on D.R.Hughes' construction of M_{12} and its associated designs, in Finite Geometries and Designs (Proc. Isle of Thorn Conf.. 1980), LMS Lecture Note Series, 49, pp. 22-30, Cambridge University Press.

BETH TH., JUNGNICKEL D. (1981). Mathieu groups. Witt designs and Golay codes, in Geometries and Groups (Proc.Berlin 1981). ed. M. Aigner. D.Jungnickel, Springer Lecture Notes in Math. 893, pp. 157-179.

BHATTACHARYA P. (1981). Permutation groups containing projective special linear groups of the same degree: A problem of Mathi&, Arch.Math., 37, p p . 198-205.

BIERBRAUER J. (1979). A characterization of the baby monster F_2, including a note on $^2E_6(2)$, J.Algebra, 56, PP. 384-395.

- - (1980). On a certain class of 2-local subgroups in finite simple groups, Rend.Sem.Mat.Univ.Padova, 62, pp.137-163.

BILIOTTI M.,PASINI A. (1982). Intersection properties in geometry, Geom. Dedicata, 13, pp. 257-275.

BIRKHOFF G. (1966), Lattice theory, 3rd edition, AMS Colloq. Publ. 25.

BOSE R.C. (1961), On some connections between the design of experiments and information theory. Bull.Intern.Statist.Inst., 38, pp. 257-271.

BOURBAKI N. (1968). Eléments de Mathématique. Groupes et algèbres de Lie, Ch. 4,5 et 6; Hermann, Paris.

BRAHANA H.R. (1930), Pairs of generators for the known simple groups whose orders are less than one milion, Ann.of.Math.,31, pp. 529-549.

BRAUER R. (1943). On permutation groups of prime degree and related classes of groups. Ann. of Math.. 44, pp. 57-79.

- - (1954), On the structure of groups of finite order. in Proc. Intern.Congr. Math. Amsterdam 1954, North Holland 1957, Vol.1, pp. 209-217.

- - (1966), On finite Desarguesian planes. 1.11. Math.Z., 90, pp. 117-151.

BRAUER R., FONG P. (1966), A characterization of the Mathieu group M_{12}, Trans.Amer.Math.Soc., 122, pp. 18-47.

BRAUER R.,FOWLER K. (1955). On groups of even order, Ann.of.Math.62, pp. 565-583.

BREMNER A. (1979). A diophantine equation arising from tight 4-designs, Osaka J.Math., 16, pp. 353-356.

BROUWER A.E. (1981). The uniqueness of the near-hexagon on 759 points. in Finite Geometries (Proc. of a Conference in honor of T.G. Ostrom, Pullman 1981), Lecture Notes in Pure and Applied Math., 82, Marcel Dekker 1983. pp. 47-60.

BRYCE N. (1971), On the Mathieu group M_{23}, J.Austral. Math. Soc., 12, pp. 385-392.

BUEKENHOUT F. (1972A), Transitive groups in which involutions fix one or three points, J.Algebra, 23, pp. 438-451.

- - (1972B) Doubly transitive groups in which the maximum number of fixed points of involutions in four. Arch.Math., 23, pp. 362-369.

- - (1979A), Diagrams for geometries and groups, J.Comb.Theory (A), 27, pp. 121-151.

- - (1979B), The geometry of diagrams. Geom. Dedicata, 8, pp. 253-257.

- - (1979C), The geometry of diagrams, Proc. Symp. Pure Math. 34, AMS, pp. 69-75.

- - (1979D), Separation and dimension in a graph, Geom. Dedicata, 8, pp. 291-298.

- (1981A), (g,d*.d)-gons. in Finite Geometries (Proc. of a Conference in honor of T.G. Ostrom, Pullman 1981). Lecture Notes in Pure and Applied Math., 82, Marcel Dekker 1983, pp. 93-111.

- - (1981B), The basic diagram of a geometry, in Geometries and Groups (Proc. Berlin 1981), ed.M.Aigner, D.Jungnickel, Springer Lecture Notes in Math. 893, pp.1-29.

- - (1982), Geometries for the Mathieu group M_{12}, in Combinatorial Theory, Proc. Schloss Ranischholzhausen 1982. Springer Lecture Notes in Math. 969, pp. 74-85.

- - (1983), Diagram geometries for sporadic groups, Preprint.

BUEKENHOUT F., HUBAUT X. (1977). Locally polar spaces and related rank 3 groups. J.Algebra, 45, pp. 391-434.

BUEKENHOUT F.. ROWLINSON P. (1974). On (1,4)-groups.II, J.London Math. Soc. (2), 8, pp. 507-513.

- - (1976). On (1,4)-groups. III, J.London Math.Soc.(2), 14, pp. 487-495.

BURGOYNE N.,FONG P. (1966). The Schur Multipliers of the Mathieu groups. Nagoya Math.J.,27, pp. 733-745. (Correction: ibid., 31, 1968. pp. 297-304.)

BUTLER G. (1981). The maximal subgroups of the sporadic simple group of Held, J.Algebra, 69, pp. 67-81.

CAMERON P.J. (1974), Characterizations of some Steiner systems, Parallelisms and Biplanes. Math.Z., 136, pp. 31-39.

- - (1975). Two remarks on Steiner systems. Geom. Dedicata, 4, pp. 403-418.

- - (1976), Parallelisms of complete designs, LMS Lecture Note Series, 23, Cambridge University Press.

- - (1980), Extremal results and configuration theorems for Steiner systems. in Lindner. Rosa (ed.), Topics on Steiner systems, Annals of Discrete Math., 7, pp. 43-63.

- - (1981), Finite permutation groups and finite simple groups, Bull. London. Math. Soc., 13, pp. 1-22.

CAMERON P.J.. VAN LINT J.H.(1980), Graphs Codes and Designs. LMS Lecture Note Series. 43, Cambridge University Press.

CANNON J.J.,HAVAS G.(1976), Defining relations for the Held-Higman-Thompson simple group, Bull.Austral.Math.Soc., 11, pp.43-46.

CANNON J.J.,MCKAYJ., YOUNG K.C. (1979). The non-abelian simple groups $G, |G| < 10^6$-Presentations, Comm. Algebra, 7, pp. 1397-1406.

CARMICHAEL R.D. (1931), Tactical configurations of rank two. Amer. J.Math., 53, pp. 217-240.

UNIVERSITÀ DEGLI STUDI DIP.TO DI MAT.M. L.E.C.C.E.

- - (1937). Introduction to the Theory of Groups of Finite Order, Ginn, Boston-New York.

CARTER R.W. (1972), , Simple groups of Lie type. Pure and Applied Math., Vol. 28, Wiley Interscience, New York.

CHAWATHE P.D. (1978). A geometry associated with the Steiner system S(24,8,5), Geom. Dedicata, 7, pp. 407-413.

CHOI C. (1967). The maximal subgroups of M_{24}, Ph.D.Thesis, University of Michigan, Ann Arbor.

- - (1972A), On subgroups of M_{24}. 1: Stabilizers of subsets, Trans. Amer.Math.Soc., 167, pp. l-27.

- - (1972B), On subgroups of M_{24}. II: The maximal subgroups of M_{24}, Trans.Amer.Math.Soc., 167, pp. 29-47.

COHEN A.M. (1980). Finite quaternionic reflection groups, J.Algebra, 64, pp. 293-324.

COLLINS M.J. (1980), A survey of the Classification Project. in Finite Simple Groups 11, Collins M.J. ed. (Proc. LMS Research Meeting, Durham 1978), Academic Press 1980). pp. 3-40.

COLLINS M.J. ed. (1980), Finite Simple Groups 11. (Proc. LMS Research Meeting, Durham 1978), Academic Press 1980.

CONWAY J.H.(1969A), A group of order 8,315,553,613,086,720,000, Bull. London Math. Soc..', pp.79-88.

- - (1969B), A characterization of Leech's lattice, Invent.Math.. 7, pp. 137-142.

- - (1971), Three lectures on exceptional groups. in Finite Simple Groups, ed. M.B.Powell. G.Higman Academic Press, pp. 215-247.

- - (1972), A construction for the smallest Fischer group F_{22}, in Finite Groups '72, Proc. Gainesville Conference 1972, North Holland 1973, pp. 27-35.

CONWAY J.H., PARKER R.A., SLOANE N.J.A. (1982), The covering radius of the Leech Lattice, Proc.Roy.Soc.London, A 380, pp.261-290.

CONWAY J.H., SLOANE N.J.A. (1982A). On the enumeration of lattices of determinant one, J. Number Theory, 15, pp.83-94.

- - (1982B), Twenty-three constructions for the Leech lattice, Proc. Roy.Soc.London, A 381, pp. 275-283.

- - (1982C), Lorentzian forms for the Leech lattice, Bull. Amer. Math. Soc., 6, pp. 215-217.

CONWAY J.H., WALES D.B. (1973), Construction of the Rudvalis group of order 145. 956. 144, 000, J.Algebra, 27, pp.538-548.

CONWELL G.M. (1910), The three space PG(3,2) and its group, Ann.of Math.(2), 11, pp. 60-76.

COOPERSTEIN B., MASON G., ed. (1980). The Santa Cruz conference on finite groups, Santa Cruz 1979. Proc.Symp.Pure Math., AMS, 37.

CORBAS V. (1965), Determinazione di una classe di gruppi di permutazioni semplicemente transitivi, Atti Accad.Naz.Lincei Rend. Cl.Sci.Fis.Mat.Natur., 38, pp.808-809; (dimostrazioni in: On a class of transitive permutation groups, Rend.Mat. e Appl., 26, 1967. pp. 153-162).

COXETER H.S.M. (1958). Twelve points in PG(5,3) with 95,040 self-transformations, Philos.Trans.Roy.Soc.London Series A, 247, pp. 279-293.

COXETER H.S.M., MOSER W.O.J. (1957). Generators and Relations for Discrete Groups, Ergebn.der Math.und ihr.Grenzgebiete, 14, Springer Verlag. Berlin.

- - (1972). Generators etc. . . . . Third Edition.

CRAIG M. (1978), A cyclotomic construction for Leech's lattice, Mathematika. 25, pp. 236-241.

CURRAN M.J. (1975), Centralizers involving Mathieu groups, Bull. Austral. Math.Soc., 13, pp. 321-323.

CURTIS R.T. (1973). On subgroups of ·0.I: Lattice stabilizers, J.Algebra, 27, pp. 549-573.

- - (1976), A new combinatoria1 approach to M_{24}, Math.Proc.Camb. Phil.Soc.. 79, pp. 25-41.

- - (1977), The maximal subgroups of M_{24}, Math.Proc.Camb.Phil.Soc., 81, pp.185-192.

- - (1980). On subgroups of ·0.II: Loca1 structure, J.Algebra, 63 pp. 413-434.

DAVIS S.L., SOLOMON R.(1981), Some sporadic characterizations, Comm. Algebra, 9, pp. 1725-1742.

DECKERS M. (1974), On groups related to Held's simple group, Arch. Math., 25, pp. 23-28.

DELSARTE P., GOETHALS J.-M(1975), Unrestricted codes with the Golay parameters are unique, Discrete Math., 12, pp.211-224.

DEMBOWSKI P. (1965), Die Nichtexistenz von transitiven Erweiterungen der endlichen affinen Gruppen, J.Reine Angew.Math., 220, pp. 37-44.

- - (1968), Finite Geometries, Ergebn.der Math. und ihr.Grenzgebiete, 44, Springer Verlag, Berlin.

DEMPWOLFF U. (1972). Eine Kennzeichnung der Gruppen A_5 und M_{23}, J. Algebra, 23, pp. 590-601.

- - (1974), A characterization of $L_n(2^m)$ by the centralizer of one 2-central involution. J.Algebra, 28, pp. 10-14.

DEMPWOLFU., WONG S.K. (1977), On finite groups whose centralizer of an involution has norma1 extraspecial and abelian subgroups 1, J.Algebra. 45, pp. 247-253.

- - (1978), On finite groups . . . 11, J.Algebra, 52, pp.210-217.

DENNISTON R.H.F. (1976). Some new 5-designs, Bull. London Math.Soc., 8, pp.263-267.

- - (1980). The problem of the higher values of t. in Lindner. Rosa (ed.), Topics on Steiner systems. Annals of Discrete Math., 7, pp. 65-70.

DICKSON L.E. (1901). Linear groups with an exposition of the Galois field theory. Teubner, Leipzig (ristampa: Dover. New York 1958).

DURAKOV B.K. (1979), Caratterizzazione di alcuni gruppi semplici finiti mediante il centralizzante di elementi di ordine 3 (Russo) Mat.Sb. (N.s.) 109(151), pp.533-554 (647).

EDGE W.L. (1954), The geometry of the linear fractional group LF(4.2). Proc. London Math.Soc. (3), 4, pp. 317-342.

- - (1970), Permutation representations of a group of order 9, 196, 830, 720, J.London Math.Soc. (2), 2, pp.753-762.

EGAWA Y. (1981). Standard components of type M_{24}, Comm.Algebra, 9, pp. 451-476.

ENOMOTO H., ITO N., NODA R.(1979), Tight 4-designs, Osaka J.Math., 16, pp. 39-43.

ENRIGHT G.M. (1977A), A description of the Fischer group F_{22}, J.Algebra, 46, pp. 334-343.

- - (1977B), A description of . . . F_{23}, J.Algebra, 46, pp.344-354.

- - (1978), Subgroups generated by transpositions in F_{22} and F_{23}, Comm. Algebra, 6, pp. 823-837.

FEIT W. (1970). The current situation in the theory of finite simple groups. in Act.Congr.Internat.Math. Nice 1970. Vol.I, Gauthier-Villars, Paris 1971, pp. 55-93.

- - (1974). On integra1 representations of finite groups, Proc. London Math. Soc., 29, pp.633-683.

FENDEL D. (1973), A characterization of Conway's group C_3 J.Algebra. 24,pp.159-196.

FINKELSTEIN L. (1973), The maximal subgroups of Conway's group C_3 and McLaughlin's group, J.Algebra, 25, pp.58-89.

- - (1974). Finite groups in which the centralizer of an involution is -0, J.Algebra, 32, pp. 173-177.

- - (1976), Finite groups with a standard component isomorphic to M_{23}, J.Algebra. 40, pp. 541-555.

- - (1977A). Finite groups with a standard component isomorphic to M_{22}, J.Algebra, 44, pp. 558-572.

- - (1977B), Finite groups with a standard component whose centralizer has cyclic Sylow 2-subgroups, Proc.Amer.Math.Soc.. 62, pp. 237-241.

- - (1977C) Finite groups with a standard component of type J_4, Pacific J.Math., 71, pp.41-56.

FINKELSTEIN L., SOLOMON R. (1979). Standard components of type M_{12} and $\cdot 3$, Osaka J.Math., 16, pp. 759-774.

FISCHER B. (1969). Finite groups generated by 3-transpositions, Mimeographed Notes, Warwick University, pp.l-169.

- - (1971). Finite groups generated by 3-transpositions.I,Invent. Math. , 13, pp. 232-246.

FOMIN A.N. (1979). Permutational characterizations of some Mathieu groups, Algebra and Logic, 18, 1980, pp.144-155 (trad. da Algebra i Logika, 18, pp. 232-249).

FOOTE R. (1976). Finite groups with components of 2-rank 1.I,II, J. Algebra, 41, pp. 16-46,47-57.

FRAME J.S. (1972). Computation of characters of the Higman-Sims group and its automorphism group, J.Algebra, 20, pp.320-349.

FROBENIUS G. (1904), Über die Charaktere der mehrfach transitive Gruppen, Sitzungsber. Berlin Akad.. pp.769-771.

FRYER K.D. (1955), A class of permutation groups of prime degree, Canad. J.Math., 7, pp. 24-34.

FUMY W. (1981), The large Witt design - Materialized. in Geometries and Groups (Proc. Berlin 1981), ed. M.Aigner, D.Jungnickel, Springer Lecture Notes in Math. 893, pp. 189-194.

GARBE D., MENNICKE J.L.(1964), Some remarks on the Mathieu groups. Canadian Math. Bull., 7, pp. 201-212.

GEWIRTZ A. (1969), Graphs with maximal even girth. Canad. J.Math., 2,pp.915-934.

GIBSON I.B., BLAKE I.F. (1978). Decoding the binary Golay code with Miracle Octad Generator. IEEE Transactions on Information Theory,24, pp.261-264.

GOETHALS J.-M.(1971), On the Golay perfect binary code, J.Comb. Theory,11, pp. 178-186.

GOLAY M.J.E.(1949), Notes on digita1 coding, Proc.Inst.Radio Engrs.,37, 657.

GORENSTEIN D. (1974), Finite simple groups and their classification, Israel J.Math., 19, pp. 5-66.

- - (1978). The classification of finite simple groups, in Proc.Int. Congr.Math.Helsinki 1978, Vol.I, pp.129-137 (1980).

- - (1979), The classification of finite simple groups. 1: Simple groups and local analysis, Bull. Amer.Math.Soc., 1, pp.43-199.

- - (1982), Finite simple groups.An introduction 'to their classification. The University Series in Math., Plenum Press.

GORENSTEIN D., HARADA K. (1971A), On finite groups with Sylow 2-subgroups of type $\hat{A}_n$, n=8,9,10 and 11, J.Algebra, 19, pp. 185-227.

- - (1971B), Finite simple groups of low 2- rauk and the families G (q),$D_4^{\prime}$(q), q odd, Bull. Amer. Math. Soc., 77, pp. 829-862.

- - (1974), Finite groups whose 2-subgroups are generated by at most 4 elements, AMS Memoirs, 147, pp.1-464.

GORENSTEIN D., HARRIS M.E. (1973). A characterization of the Higman-Sims simple group, J-Algebra, 24, pp.565-590.

GORENSTEIN D., HUGHES D.R.(1961), Triply transitive groups in which only the identity fixes four letters, Illinois J.Math.,5, pp.486-491.

GREENBERG P. (1973), The Mathieu Groups. Courant Institute of Math. Sciences, New York.

GRIESS R.L.Jr.(1974), Schur multipliers of some sporadic simple groups. J.Algebra, 32, pp.445-466.

- - (1980), Schur multipliers of the known finite simple groups. 11, in The Santa Cruz conference on finite groups, Santa Cruz 1979, Proc.Symp.Pure Math., AMS, 37, pp. 279-282.

- - (1982). The friendly giant, Invent.Math., 69, pp.1-102.

GROSS B.H.(1974), Intersection triangles and block intersection numbers for Steiner systems. Math.Z., 139, pp.87-104.

GÜLOĞLU I.S.(1981), A characterization of the simple group J_4, Osaka J.Math., 18, pp.13-24.

HALL M.Jr.(1954), On a theorem of Jordan. Pacific J.Math., 4, pp.219-226.

- - (1959). The Theory of Groups. MacMillan, New York.

- - (1960), Automorphisms of Steiner triple systems, IBM J.Res. Develop., 4, pp.460-471.

- - (1962), A note on the Mathieu group M_{12}, Arch. Math., 13, pp. 334-340.

- - (1967), Combinatoria1 Theory, Wiley. New York.

- - (1975), Semi-automorphisms of Hadamard matrices, Math. Proc. Camb. Phil.Soc., 77,pp.459-473.

- - (1980), Group problems arising from combinatorics, in The Santa Cruz conference on finite groups. Santa Cruz 1979, Proc. Symp. Pure Math., AMS, 37, pp.445-456.

HALL M.Jr.,WALES D.(1968), The simple group of order 604,800, J.Algebra, 9, pp.417-450.

HAMMING R.W.(1950), Error detecting and error correcting codes, Bell Syst.Tech.J., 29, pp.147-160.

HARADA K. (1970), Finite simple groups whose Sylow 2-subgroups are of order 2^7, J.Algebra, 14, pp. 386-404.

- - (1975A), On finite groups having self-centralizing 2-subgroups of small order, J.Algebra, 33, pp.144-160.

- - (1975B), On the simple group F of order $2^{14} \cdot 36 \cdot 56 \cdot 7 \cdot 11 \cdot 19$, in Proc.Utah Conference on Finite Groups, ed.F.Gross,Academic Press 1976, pp.119-276.

- - (1978). Finite groups having 2-local subgroups El6 $L_4(2)$. 1, J.Fac.Sci.Univ.Tokio,Sect. IA25, pp.220-236.

HARADA K.,YAMAKI H. (1979). Finite groups having 2-local subgroups $E_{16}.L_4(2)$. 11, J. Fac. Sci. Univ. Tokio, Sect. IA26, pp.97-114.

HARRIS M.E.(1971), A characterization of odd order extensions of the simple groups $PSp(4,q)$, $G_2(q)$, $D_4^2(q)$, Nogaya Math.J., 45, pp. 79-96.

HAUCK P.(1982), Eine Charakterisierung des Steinersystems S(5.8.24). J.Comb.Theory(A), 32, pp.99-102.

HELD D.(1968A), Eine Kennzeichnung der Mathieu-Gruppe M_{22} und der alternierenden Gruppe A_{10}, J.Algebra, 8, pp. 436-449.

- - (1968B). A characterization of some multiply transitive permutation groups.II,Arch.Math., 19, pp.378-382.

- - (1969A). A characterization of some multiply transitive permutation groups.I,Illinois J.Math., 13, pp.224-240.

- (1969B), The simple groups related to M_{24}, J. Algebra, 13, pp. 253-296.

- - (1973), The simple groups related to M_{24}.II,J.Austral. Math. Soc., 16, pp.24-28.

HELD D..SCHOENWAELDER U.(1970), A characterization of the simple group M_{24}, Math.Z.,117, pp.289-308.

HERING C.(1968), Zweifach transitive permutationsgruppen. in denen zwei maximale Anzahl von Fixpunkten von Involutionen ist, Math.Z.. 104, pp.150-174.

HIGMAN D.G.(1964), Finite permutation groups of rank 3,Math.Z.. 86, pp.145-156.

HIGMAN D.G., SIMS C.C.(1968), A simple group of order 44.352.000, Math.Z., 105, pp.110-113.

HIGMAN G.(1969), On the simple group of D.G.Higman and C.C.Sims, Illinois J.Math., 13, pp.74-80.

HIRAMINE Y.(1977), On multiply transitive groups, Osaka J.Math., 14, pp.453-463.

- - (1978). On transitive groups in which the maximal number of fixed points of involutions is five. J. Math.Soc.Japan, 30, pp.215-235.

- - (1979A), On some doubly transitive permutation groups in which socle (G_α) is non-solvable, Osaka J.Math., 16, pp. 797-816.

- - (1979B), Doubly transitive groups of even degree whose one-point stabilizer has a normal subgroup isomorphic to PSL(3,2^n), Osaka J.Math., 16, pp.817-830.

HUGHES D.R. (1965A), On t-designs and groups, Amer.J.Math., 87, pp.761-778.

- - (1965B), Extensions of designs and groups: Projective, symplectic and certain affine groups, Math.Z., 89, pp.199-205.

- - (1981A), On designs, in Geometries and Groups (Proc. Berlin 1981), ed. M. Aigner, D. Jungnichel, Springer Lecture Notes in Math. 893, pp. 43-67.

- - (1981B). A combinatorial construction of the small Mathieu designs and groups (to appear in Annals of Discrete Math.)

HUMPHREYS J.F. (1980), The projective characters of the Mathieu group M_{12} and of its automorphism group. Math.Proc.Camb. Phil.Soc., 87., pp. 401-412.

- - (1982). The modular characters of the Higman-Sims simple group, Proc.Roy.Soc.Edinburgh (A), 92, pp.319-335.

HUNT D.C. (1971), Character tables of certain finite simple groups, Bull.Austral.Math.Soc., 5, pp.1-42.

- - (1972), A characterization of the finite simple group M(22), J.Algebra, 21, pp.103-112.

- - (1973), A characterization of the finite simple group M(23), J.Algebra, 26, pp.431-439.

- - (1974A), The character table of $D_4(3)$, Math.Comp., 28, p.659 (with microfiche supplement).

- - (1974B), The character table of Fischer's simple group M(23), Math.Comp., 28, pp.660-661 (with microfiche supplement).

HUPPERT B. (1962), Scharf dreifach transitive Permutationsgruppen, Arch.Math., 13, pp.61-72.

- - (1967), Endliche Gruppen 1, Grundlehren der math. Wissenschaften. Band 134, Springer Verlag,Berlin.

HUPPERTB .„BLACKBURN N.(1982), Finite Groups II,III,Grundlehren der math. Wissenschaften. Banden 242,243. Springer Verlag, Berlin.

HUSSAIN Q.M.(1945), On the totality of solutions for the symmetrical incomplete block designs: λ = 2,k = 5 or 6 . Sankhyā, 7, pp.204-208.

ITO N. (1975). On tight 4-designs, Osaka J.Math.. 12, pp. 493-522.

- - (1978), Corrections and supplements to "On tight 4-designs", Osaka J.Math., 15,pp.693-697.

- - (1980), Hadamard matrices with "doubly transitive" automorphism groups, Arch.Math., 35, pp.100-111.

JAMES G.D.(1973), The modular characters of the Mathieu groups, J.Algebra, 27, pp.57-111.

JANKO Z.(1968A), A characterization of the Mathieu simple groups. 1, J.Algebra, 9, pp.1-19.

- - (1968B), A characterization of the Mathieu simple groups.II, J.Algebra. 9, pp.20-41.

- - (1968C), Some new simple groups of finite order .I, Symposia Mathematica (INDAM), 1, pp.25-64.

- - (1976). A new finite simple group of order 86.775.571.046.077. 562.880 which possesses M_{24} and the full covering group of M22 as subgroups, J.Algebra, 42, pp.564-596.

- - (1978). On the finite simple groups (according to Aschbacher and Gorenstein). Sém.Bourbaki (1976/77) n . 502, Springer Lecture Notes in Math. 677, pp. 183-188.

JANKO Z.. WONG S.K. (1969). A characterization of the Higman-Sims simple group, J.Algebra, 13, pp.517-534.

- - (1972), A characterization of the McLaughlin simple group. J.Algebra, 20, pp.203-225.

JÓNSSON W. (1972), On the Mathieu groups M_{22},M_{23},M_{24} and the associated Steiner systems. Math Z.,. 125, pp.193-214.

JÓNSSON W.,MCKAY J.(1976), More about the Mathieu group M_{22}, Canad.J.Math.,28, pp.929-937.

JORDAN C.(1870), Trait6 des substitutions et des équations algébriques, Gauthier-Villars. Paris.

- - (1872). Recherches sur les substitutions. J.Math.Pures Appl. (2). 17, pp.351-363.

- - (1874). Sur deux points de la théorie des substitutions, Comptes Rendus, 79, pp.1149-1151.

KANTOR W.M.(1969A), Jordan groups, J.Algebra, 12, pp.471-593.

- - (1969B), Automorphism groups of Hadamard matrices, J.Comb.Theory, 6, pp.279-281.

- - (1974), Dimension and embedding theorems for geometric lattices, J.Comb.Theory (A), 17, pp.173-195.

- - (1975A), Envelopes of geometric lattices. J.Comb.Theory (A), 18, pp.12-26.

- - (1975B), 2-transitive designs, in Combinatorics (Proc. Advanced Study Inst. on Combinatorics, Breuleken 1974), ed.M.Hall.J.H. van Lint, Math.Centre Tracts, Amsterdam.

- - (1976), Some highly geometric lattices, Convegno sulle Teorie Combinatorie (Roma 1973). Atti Conv. Lincei, 17, pp.183-191.

- - (1981). Some geometries that are almost buildings, Burop.J.Comb.2, pp.239-247.

KARLIN M.(1969), New binary coding results by circulants, IEEE Trans.Information Theory. 15, pp.81-92.

KASSAB J.N. (1982). On the geometry of certain strongly regular graphs, Ph.D.Thesis, University of Birmingham.

KIERMAN G.R.(1975), On finite groups with a 2-local subgroup which is a non-trivial split extension of E_{2^4} by $L_4(2)$, Ph.D. Thesis. Rutgers University.

KIMURA H. (1978), On the Higman-Sims simple group of order 44.352.000, J.Algebra, 52, pp.88-93.

KING J.(1969), Doubly transitive groups in which involutions fix one or three points, Math.Z., 111, pp.311-321. (Corrections: Math.Z., 112, pp.393-394.)

KIRKMAN T.P.(1847), On a problem in combinations, Cambridge and Dublin Math.J., 2, pp.191-204.

- - (1850), Query, in Lady's and Gentleman's Diary, p.48.

KOCH J.(1982), Standard components of type $O^+(8,2)$, Ph.D.Thesis, Ohio State University.

KRAMER E.S.,MAGLIVERAS S.S.(1974) Some mutually disjoint Steiner systems. J.Comb.Theory(A), 17, pp.39-43.

KRAMER E.S.,MAGLIVERAS S.S.,MESNER D.M.(1980), Some resolutions of S(5,8,24), J.Comb.Theory(A), 29, pp.166-173.

- - (1981), t-designs from the large Mathieu groups, Discrete Math.. pp.171-189.

KRAMER E.S.,MESNER D.M.(1974), Intersection among Steiner systems. J.Comb.Theory (A), 16, pp.273-285.

- - (1976), t-designs on hypergraphs, Discrete Math.. 15, pp.263-296.

LANDROCK P.(1978), The non-principal 2-blocks of sporadic simple groups, Comm.Algebra, 6, pp.1865-1891.

LEECH J. (1964), Seme sphere packings in higher space, Canad.J. Math., 16,pp.657-682.

- - (1967), Notes on sphere packings, Canad.J.Math., 19, pp. 251-267.

- - (1969), A presentation of the Mathieu group M_{12}, Canad.Math. Bull., 12, pp.41-43.

LEECH J.,SLOANE N.J.A.(1971), Sphere packing and error-correcting codes, Canad.J.Math.,23,pp.718-745.

LEMPKEN W. (1978A), A 2-local characterization of Janko's simple group J_4, J.Algebra, 55, pp.403-445.

- - (1978B), The Schur multiplier of J_4 is trivial, Arch. Math.. 30,pp.267-270.

LEON J.,SIMS C.C.(1977), The existence and uniqueness of a simple group generated by {3,4}-transpositions, Bull.Amer.Math.Soc.,83, pp.1039-1040.

LEPOWSKY J.,MEURMAN A.(1982), An E_8-approach to the Leech lattice and the Conway group, J.Algebra, 77, pp. 484-504.

LINDNER C.C.,ROSA A.(ed.)(1980), Topics on Steiner systems, Annals of Discrete Math., 7, North-Holland, Amsterdam.

LINDSEY 11 J.H.(1970A), On a six-dimensiona1 projective representation of the Hall-Janko group, Pacific J.Math., 35, pp.175-186.

- - (1970B), On the Suzuki and Conway groups, Bull.Amer.Math. Soc.,76, pp.1088-1090.

- - (1971). A correlation between $PSU_4(3)$, the Suzuki group and the Conway group, Trans.Amer.Math.Soc., 157, pp.189-204.

VAN LINT J.H.(1971), Coding theory, Springer Lecture Notes in Math.201.

- - (1982), Introduction to Coding Theory, Springer Graduate Texts in Math.86.

LIST R.(1977), On the maximal subgroups of the Mathieu groups I: M_{24}, Lincei-Rend.Sc.fis.mat.e nat.,Vol.LXII, pp.432-438.

LÜNEBURG H.(1968), Über die Gruppen von Mathieu, J.Algebra, 10, pp.194-210.

- - (1969). Transitive Erweiterungen endlicher Permutationsgruppen, Springer Lecture Notes in Math.84.

MACWILLIAMS F.J.,SLOANE N.J.A.(1977), The Theory of Error-Correcting Codes, North-Holland. Amsterdam.

MAGLIVERAS S.S.(1971), The subgroup structure of the Higman-Sims simple group. Bull.Amer.Math.Soc., 77, pp.535-539.

- - (1974), On transitive extensions of the Higman-Sims group, J.Algebra, 30, pp.317-319.

- - (1976), The non-existence of rank-3 transitive extensions of the Higman-Sims simple group, in Proc.Utah Conference on Finite Groups, ed.W.Scott,F.Gross,Academic Press,pp. 457-469.

MAGLIVERAS S.S., LEAVITT D.W.(1982), Simple 6-(33,8,36) designs from $P\Gamma L_2(32)$, in Computational Group Theory, ed.M.D.Atkiusons, Proc. LMS Symp.Durham 1982, Academic Press 1984, pp.337-352.

MASON D.R.(1973), Finite simple groups with Sylow 2-subgroups of type PSL(4,q),q odd. J.Algebra, 26, pp.75-97.

- - (1977), On the construction of the Steiner system S(5,8,24), J.Algebra, 47, pp.77-79.

MASON G.(1977), Some remarks on groups of type J_4, Arch.Math., 29, pp.574-582.

MATHIEU E.(1860), Mémoire sur le nombre des valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles, J.Math.Pures Appl., 5,pp.9-42.

(1861), Mémoire sur l'étude des fonctions de plusieurs quantités, sur la maniere de les former et sur les substitutions qui les laissent invariables, J.Math.Pures Appl., 6, pp.241-323.

(1873), Sur la fonction cinq fois transitive de 24 quantités, J.Math.Pures Appl.. 18, pp.24-46.

B.H.(1979A), Zur Konstruktion von Zahl-und Funktionen-Körpern mit vorgegebener Caloisgruppe, Habilitationschrift. Universität Karlsruhe.

(1979B). Konstruktion von Zahlkorpern mit der Galois-gruppe M_{11} über $Q(\sqrt{-11})$, Manuscripta math.. 27, pp.103-111.

(1983), Konstruktion von Zahlkorpern mit der Galois gruppe M_{12} über $Q(\sqrt{-5})$, 40, pp.245-254.

MAZET P . (1979), Sur le multiplicateur de Schur du groupe de Mathieu M_{22}, C.R.Acad.Sci.Paris, Sér.A-B, 289, pp.A659-A661.

- - (1982), Sur les multiplicateurs de Schur des groupesde Mathieu. J-Algebra, 77, pp.552-576.

MAZUROV V.D.(1966), On finite groups with a given Sylow 2-subgroup. Dokl.Akad.Nauk.SSSR.168, pp.519-521 (Soviet Math. Dokl.,7, pp.681-682.)

- - (1967), Finite groups with metacyclic Sylow 2-subgroups, Sibirsk Mat.Z.,8, pp.966-982.(Russo).

MCKAY J.(1972), A setting for the Leech Lattice, in Finite Groups '72, Proc.Gainesville Conference 1972, North-Holland 1973, pp. 117-118.

- - (1974), Computing with finite simple groups, in Proc. 2nd Intern. 'Conf.on the theory of groups, Canberra 1973, Springer Lecture Notes in Math. 372, pp.448-452.

MCKAY J., WALES D.(1971), The multiplier of the Higman-Sims simple group, Bull.London Math.Soc., 3, pp.283-285.

MCKAY J.. YOUNG K.C.(1979), The non-abelian simple groups $G, |G| < 10^6$-minimal generating pairs, Math.Comp., 33, pp.812-814.

MCLAUGHLIN J.(1969), A simple group of order 898,128,000, in Theory of Finite Groups - A Symposium (ed.Brauer-Sah), Benjamin, New York, pp.109-111.

MENDELSOHN N.S.(1970), A theorem on Steiner systems, Canad.J. Math.,22, pp.lOlO-1015.

MILLER G.A.(1898), On the supposed five-fold transitive function of 24 elements and 19!+48 values. Messenger of Math., 27, pp.187-190.

- - (1900). Sur plusieurs groupes simples. Bull.Soc.Math.Fr., 28, pp.266-267.

MILLS W.H. (1978). A new 5-design, Ars Combinatoria, 6, pp.193-195.

MIYAMOTO 1. (1974), Multiply transitive permutation groups and odd primes. Osaka Math J. 11, pp.9-13.

MOORI J.(1981), On certain groups associated with the smallest Fischer group. J.London Math.Soc.(2), 23, pp.61-67.

- - (1982), On the automorphism group of the group $D_4(2)$, to appear.

MORTIMER B.(1980), The modular permutation representations of the known doubly transitive groups,Proc.London Math.Soc. 41, pp.l-20.

MOSER W.O.J.(1959), Abstract definitions for the Mathieu groups Mll and M_{12}, Canad.Math.Bull.,2,pp.9-13.

NAGAO H.(1965), On multiply transitive groups.IV, Osaka J.Math.,2, pp.327-341.

- - (1966), On multiply transitive permutation groups.I, Nagoya Math.J., 27,pp.15-19.

- - (1968), On multiply transitive groups.V, J.Algebra, 9, pp. 240-248.

NAGAO H., OYAMA T. (1965), On multiply transitive groups.III, Osaka J.Math., 2, pp. 319-326.

NEUMAIER A.(1982), Lattices of Leech type, SIAM J.Algebraic and Discrete Methods, to appear.

NEUMANN P.M.(1976), Transitive permutation groups of prime degree.IV: A problem of Mathieu and a theorem of Ito, Proc.London Math. Soc.,32, pp.52-62.

NIEMEIER H.V.(1968), Definite quadratische Formen der Dimension 24 und Diskriminante 1, Göttingen, Dissertation; pubbl. in J.Number Theory. 5,(1973), pp.142-178.

NODA R.(1967), On 6-fold transitive groups. Osaka J.Math., 4, pp. 257-260.

- - (1971), Doubly transitive groups in which the maximal number of fixed points of involutions in four, Osaka J.Math., 8, pp.77-90.

- - (1972), Steiner systems which admit block transitive automorphism groups of small rank. Math.Z., 125, pp. 113-121.

NODA R., OYAMA T. (1969), On multiply transitive groups.VI, J-Algebra, 11, pp.145-154.

NORMAN C.W. (1968). A characterization of the Mathieu group M_{11}, Math.Z., 106, pp. 162-166.

- - (1973). Hadamard designs with no non-trivial automorphisms, Geom.Dedicata. 2, pp.201-204.

NORTON S.(1980), The construction of J_4, in The Santa Cruz conference on finite groups, Santa Cruz 1979, Proc. Symp.Pure Math.. AMS, 37, pp.271-277.

- - (1982), A bound for the covering radius of the Leech lattice, Proc.Roy.Soc.London. A 380, pp.259-260.

O'NAN M.E.(1975), The norma1 structure of the point-stabilizer of a doubly transitive permutation group.I,II, Trans. Amer. Math. Soc., 214, pp.1-42, 43-74.

- - (1976A), Some characterizations by centralizers of elements of order three, in Proc.Utah Conference on Finite Groups, ed. W.Scott,F.Gross, Academic Press, pp.79-84.

- - (19768). Some evidence for the existence of a new simple group, Proc.London Math.Soc.(3), 32, pp.421-479.

O'NAN M.E.,SOLOMON R.(1976), Simple groups transitive on interna1 flags, J.Algebra, 39, pp.375-410.

OSTROM T.G.,WAGNER A.(1959), On projective and affine planes with transitive collineation groups. Math.Z.,71, pp.186-199.

OYAMA T.(1968), On multiply transitive groups.VII, Osaka J.Math., 5, pp.155-164.

- - (1969), On multiply transitive groups.VIII, Osaka J.Math., 6, pp.315-319.

- - (1970). On multiply transitive groups.IX, Osaka J.Math., 7, pp.41-56.

- - (1971), On multiply transitive groups.X, Osaka J.Math., 8, pp.99-130.

- - (1973), On multiply transitive groups.XI, Osaka J.Math., 10, pp.379-439.

- - (1974). On mult iply transitive groups.XII, Osaka J.Math., 11, pp.595-636.

- - (1976), On multiply transitive groups.XIII,Osaka J.Math., 13, pp.367-383.

- - (1978). On multiply transitive groups, XIV. Osaka J.Math., 15, pp.351-358.

PAHLINGS H.(1974), On the character tables of finite groups generated by 3-transpositions. Comm.Algebra, 2, pp.117-131.

PAIGE L.J.(1956), A note on the Mathieu groups. Canad.J.Math., 9, pp.15-18.

PALEY R.E.A.C.(1933), On orthogonal matrices, J.Math.Phys. Mass. Inst.Tech., 12, pp.311-320.

PARKER E.T.(1959), On quadruply transitive groups, Pacific J.Math., 9, pp.829-836.

PARROTT D.(1970), On the Mathieu groups M_{22} and Mll, J.Austral. Math.Soc., 11, pp.69-81.

- - (1981). Characterizations of the Fischer groups.I,II,III, Trans.Amer.Math.Soc.. 265, pp.303-347.

PARROTT D., WONG S.K. (1970). On the Higman-Sims simple group of order 44,352,000, Pacific J.Math., 32, pp.501-526.

PASINI A. (1980), Diagrams and Incidence Structures, rapp. 21 Ist.Mat.Università di Sien. pubbl. in J.Comb. Theory (A), 33 (1982), pp.186-194.

- - (1983A), Canonica1 linearization of Pure Geometries, J. Comb. Theory(A), 35, pp.10-32.

- - (1983B), On the linearization of pure geometries in certain diagrams (cyclic diagrams and trees), to appear in Simon Stevin.

- - (1983C), Some results on covers, apartments and

intersection property. Rapp.Mat.n.81, Dipart.Mat.Univ.Siena.

PASSMAN D.S.(1968), Permutation Groups, Benjamin, New York.

PATTERSON N.(1974), On Conway's group ·0 and some subgroups, Ph.D.Thesis, University of Cambridge.

PERCSY N.(1981), Geometries uniquely embeddable in projective spaces, in Geometries and Groups (Proc.Berlin 1981). ed M.Aigner, D.Jungnickel, Springer Lecture Notes in Math. 893, pp.231-241.

PHAN K.W.(1969), A characterization of the finite simple group $U_4(3)$, J.Austral.Math.Soc., 10, pp.77-94.

- - (1970). A characterization of four dimensiona1 unimodular groups, J.Algebra, 15, pp.252-279.

- - (1971). A characterization of the unitary groups $PSU(4,q^2)$, q odd. J.Algebra, 17, pp.132-148.

PLESS V.(1968), On the uniqueness of the Golay codes, J.Comb. Theory, 5, pp.215-228.

- - (1972), Symmetry codes over GF(3) and new 5-designs, J.Comb.Theory, 12, pp.119-142.

- - (1975), Symmetry codes and their invariant subcodes, J.Comb.Theory(A), 18, pp.116-125.

- - (1982) Introduction to the theory of error-correcting codes, Wiley Inter-science Series in Discrete Math., New York.

PLESS V., SLOANE N.J.A.(1975), On the classification and enumeration of self-dual codes, J.Comb.Theory(A), pp.313-335.

POWELL M.B., HIGMAN G., ed.(1971), Finite Simple Groups, Academic Press, London.

RASALA R.(1976), Split codes and the Mathieu groups, J.Algebra, 42, pp.422-471.

RAY-CHALJDURI D.K., WILSON R.M.(1971), Solution of Kirkman's schoolgirls problem. in Combinatorics, Proc.Symp.Pure Math., AMS, 9, pp.187-203.

- - (1975). On t-designs. Osaka J.Math., 12, pp.737-744.

REIFART A.(1975), A characterization of the sporadic simple group of Suzuki, J.Algebra. 33, pp.288-305.

- - (1977A), Some simple groups related to M_{24}, J.Algebra. 45, pp.199-209.

- - (1977B), Another characterization of Janko's simple group J_4, J-Algebra, 49,pp.621-627.

- - (1977C), A remark on Conway's group ·1, Arch.Math., 29, pp.389-391.

- - (1978). A 2-local characterization of the simple groups M(24)', ·1, and J_4, J-Algebra, 50,pp.213-227.

ROBINSON D.J.S.(1982), A Course in the Theory of Groups, Graduate Texts in Math.80,Springer Verlag,Berlin.

RONAN M.(1982), Locally truncated buildings and M_{24}, Math.Z., 180, pp.489-501.

RONAN M.,SMITH S.D.(1980), 2-local geometries for some sporadic groups. in The Santa Cruz conference on finite groups. Santa Cruz 1979, Proc.Symp.Pure ath.. AMS, 37, pp. 283-289.

RONAN M.. STROTH G.(1982), On Sylow-2 geometries. to appear.

ROWLINSON P.(1972), Simple permutation groups in which an involution fixes a small number of points, J.London Math.Soc.(2), 4, pp.655-661.

- - (1973), Simple permutation groups in which an involution fixes a small number of points.II, Proc.London Math.Soc., 26, pp.463-484.

- - (1974). On (1,4)-groups.I, J.London Math. Soc.(2), 8,pp.493-498.

- - (1976), On (1,6)-groups, J.London Math. Soc.(2), 14, pp.481-486.

- - (1977), Certain multiply transitive setwise stabilizers, J-Algebra, 46, pp.481-496.

RUDVALIS A.(1975), Characters of the covering group of the Higman-Sims simple group, J.Algebra, 33, pp.135-143.

SANDLÖBES H.,SCHOENWAELDER U.(1979), The core-free groups of Sylow 2-type M_{24}, Math.Z., 167, pp.15-23.

SCHOENWAELDER U. (1974A), Finite groups with a Sylow 2-subgroup of type M_{24}, I,J.Algebra, 28, pp.20-45.

- - (1974B). Finite groups with a Sylow 2-subgroup of type M_{24}, II, J.Algebra, 28, pp.46-56.

SCOTT W.R.(1964), Group Theory. Prentice-Hall. Englewood Cliffs, N.Y..

SÉGUIER, J.de (1904). Théorie des Groupes Finis, Paris.

SEITZ G.M.(1973), Flag-transitive subgroups of Chevalley groups. Ann.of Math., 97, pp.27-56.

- - (1980), Standard subgroups in finite groups, in Finite Simple Groups II, Collins M.J. ed., Academic Press London, pp.41-62.

SERRE J.P.(1973), A Course in Arithmetic, Graduate Texts in Math. 7, Springer Verlag, Berlin.

SHAUGHNESSY E.P.(1971), Codes with simple automorphism groups, Arch.Math., 22, pp.459-466.

SHULT E.E. (1972). The graph extension theorem. Proc.Amer.Math. Soc., 33, pp.278-284.

- - (1981), Permutation groups with few fixed points, in Geometry-von Staudt's Point of View (Proc.NATO Advanced Study Inst.Bad Windsheim 1980). Plaumann. Strambach. ed., Reidel Publ.C., pp.275-311.

SHULT E.E., YANUSHKA A.(1980), Near n-gons and line systems, Geom.Dedicata, 9, pp.1-72.

SIMS C.C.(1967), Graphs and finite permutation groups.I, Math.Z., 95, pp.76-86.

- - (1968), Graphs and finite permutation groups.II, Math.Z., 103, pp.276-281.

- - (1969), On the isomorphism of two groups of order 44,352,000, in Theory of Finite Groups-A Symposium, (ed. Brauer-Sah).Benjamin. New York, pp.101-108.

SITNIKOV V.M.(1974), The Mathieu group M_{12}, Mat.Zametki, 15, pp.651-660.

SLOANE N.J.A.(1977), Binary codes, lattices and sphere packings, in Combinatorial Surveys: Proc.Sixt British Comb. Conf., P.J.Cameron ed., Academic Press, London, pp.117-164.

- - (1979). Self-dual codes and lattices, in Relations between combinatorics and other parts of mathematics. Proc.Symp.Pure Math., AMS, 34, pp.273-308.

SMITH F.L.(1974), A characterization of the $\mathbb{Z}_2$ Conway simple group. J-Algebra, 31, pp.91-116.

SMITH M.S.(1975), On rank 3 permutation groups, J.Algebra, 33, pp.22-42.

- - (1976A), On the isomorphism of two simple groups of order 44,352,000, J.Algebra. 41, pp.172-174.

- - (1976B), A combinatorial configuration associated with the Higman-Sims simple group, J.Algebra, 41, pp.175-195.

SMITH S.D.(1979), Large extraspecial subgroups of widths 4 and 6, J.Algebra. 58, pp.251-281.

(1980A), A characterization of orthogonal groups over GF(2), J.Algebra, 62, pp.39-60.

- - (1980B), A characterization of finite Chevalley and twisted groups of type E over GF(2), J.Algebra, 62, pp.101-117.

- - (1980C). The classification of finite groups with large extraspecial 2-subgroups, in The Santa Cruz conference on finite groups. Santa Cruz 1979. Proc.Symp. Pure Math.. AMS 37, pp.lll-120.

- - (1982A), Irreducible modules and parabolic subgroups, J.Algebra, 75, pp.286-289.

- - (1982B), Reconstructing M_{24} from its 2-local geometry, submitted to J.Algebra.

SNOVER S.L.(1973), The uniqueness of the Nordstrom-Robinson and the Golay binary codes, Ph.D.Thesis, Michigan State University.

SOLOMON R.(1974), Finite groups with Sylow 2-subgroups of type $\cdot 3$, J.Algebra, 28, pp.182-198.

STAFFORD R.M.(1979), A characterization of Janko's simple group J_4 by centralizers of elements of order 3, J.Algebra, 57, pp.555-566.

STANTON R.G.(1951), The Mathieu groups, Canad. J.Math., 3, pp.164-174.

STARK B.(1977), Another look at Thompson's quadratic pairs J.Algebra, 45, pp.334-342.

STEINBERG R.(1962), Generators for simple groups, Canad.J.Math., 14, pp.277-283.

- - (1967), Lectures on Chevalley Groups. Yale University Mimeographed Notes.

STINGL V.(1976), Endliche. einfache Component-type Gruppen, deren Ordnung nicht durch 2^{11} geteilt wird, Dissertation, Mainz.

STRIKO J.K.(1976), A characterization of the finite simple groups M_{24}, He, and $L_5(2)$, J. Algebra, 43, pp.375-397.

STROTH G.(1975A), Über Gruppen. die in ähnlicher Beziehung zu M_{24} order $L_5(2)$ stehen, wie Sz zu He, und eine Kennzeichnung von M_{24} und $L_5(2)$.I, J.Algebra, 33, pp.206-223.

- - (1975B), Über Gruppen . . . .II, J.Algebra, 34, pp.331-364.

- - (1977A), Gruppen mit kleinen 2-lokalen Untergruppen, J.Algebra, 47, pp.441-454.

- - (1977B), Endliche einfache Gruppen mit einer zentralizatorgleichen elementar abelschen Untergruppe von der Ordnung 16, J.Algebra, 47, pp.480-523.

- - (1977C), Endliche einfache Gruppen mit einer 2-lokalen Untergruppe $E_{16}\,\Sigma_6$, J.Algebra, 47, pp.455-479.

- - (1978), An odd characterization of J_4, Israel J.Math., 31, pp.189-192.

- - (1979), A characterization of ·3, Acta Sci.Math. (Szeged). 41, pp.215-219.

- - (1980), Groups having a selfcentralizing elementary abelian subgroup of order 16. in The Santa Cruz conference on finite groups. Santa Cruz 1979, Proc.Symp.Pure Math., AMS. 37, pp.127-129.

SUZUKI M.(1966), Transitive extensions of a class of doubly transitive groups, Nagoya Math.J., 27, pp.159-169.

- - (1969), A simple group of order 448,345,497,600, in Theory of Finite Groups - A Symposium, (ed.Brauer-Sah), Benjamin, New York, pp.113-119.

- - (1982), Group Theory 1, Grundlehren der math.Wissenschaften, Band 247, Springer Verlag, Berlin.

SYSKIN S.A. (1980). Abstract properties of the simple sporadic groups, Uspekhi Mat . Nauk., 35:5, pp.181-212 (Russian Math. Surveys, 35:5, pp.209-246).

THOMPSON J.G.(1970), A note on quadratic pairs. in Act.Congr. Internat. Math. Nice 1970, Val. 1, Gauthier-Villars, Paris 1971, pp.375-376.

- - (1976). Finite groups and even lattices, J.Algebra, 38, pp. 523-524.

THWAITES G.N.(1973), A characterization of M_{12} by centralizer of involution. Quart.J.Math.Oxford(2), 24, pp.537-557.

TIETÄVAINEN A.(1973), On the non-existence of perfect codes over finite fields, SIAM J.Appl.Math., 24, pp.88-96.

TIMMESFELD F.(1970), Eine Kennzeichnung der linearen Gruppen iiber GF(2), Math.Ann., 189, pp.134-160.

- - (1973), A characterization of the Chevalley and Steinberg groups over F_2, Geom.Dedicata. 1, pp.269-321.

- - (1975A). Groups generated by root involutions.I.II, J.Algebra, 33, pp.75-134; 35, pp.367-441.

- - (1975B), Groups with weakly closed T.I. subgroups. Math.Z., 143, pp.243-278.

- - (1978). Finite simple groups in which the generalized Fitting group of the centralizer of some involut ion is extraspecial-, Ann.of Math., 107, pp.297-369. (Correction: Ann.of Math.,109, 1979. pp.413-414.)

TITS J. (1949). Généralisations des groupes projectifs.I,II,III, IV, Acad.Roy.Belg.Bull.Cl.Sci.(5), 35, pp.197-208, 224-233.568-589.756-773.

- - (1956), Sur les analogues algébriques des groupes semi-simples complexes, in Colloque d'Algèbre Supérieure du C.B.R.M. (Bruxelles 1956). 1957,pp.261-289.

- - (1959), Groupes algébriques semi-simples et géométr ies associées, in Proc.Coll.Algebraical and Topologica1 Foundat ions of Geometry (Utrecht 1959), Pergamon Press, London, 1962, pp.175-192.

- - (1964). Sur les systèmes de Steiner associés aux trois "grands" groupes de Mathieu, Rend.Mat.e Appl.. 25, pp.166-184.

- - (1969), Le groupe de Janko d'ordre 604.800, in Theory of Finite Groups - A Symposium, (ed.Brauer-Sah), Benjamin, New York, pp.91-95.

- - (1970), Groupes finis simples sporadiques, Sém.Bourbaki 1969/70 n.375, Springer Lecture Notes in Math. 180.

- - (1974) Buildings of spher ical type and finite BN-pairs, Springer Lecture Notes in Math. 386.

- - (1975) Sur certains groupes dont l'ordre est divisible par 23, Bull.Soc.Math.Belg., 27, pp.325-332.

- - (1976), Classification of buildings of spherical type and Moufang polygons - A survey. Atti Convegni Lincei, 17, pp.229-2[illegible].

- - (1978A), Four presentations of Leech's lattice, in Finite Simple Groups 11, Collins M.J.ed., Academic Press, London 1980, pp.303-307.

- - (1978B), Résumé d e Cours, Annuaire d u Collège de France, 1977/78, pp.80-81.

- - (1978C), Buildings and Buekenhout geometries, in Finite Simple Groups 11, Collins M.J.ed., Academic Press, London 1980, pp.309-320.

- - (1979), A loca1 approach to buildings. in The Geometric Vein (Proc. o f the Coxeter Symposium, Toronto 1979). Springer Verlag, Berlin, 1981.

- - (1980), Quaternions over Q($\sqrt{5}$), Leech lattice and the sporadic group of Hall-Janko, J.Algebra, 63, pp.66-75.

TODD J.A. (1933). A combinatoria1 problem, J.Math.Phys.Mass.Inst. Tech., 12, pp.321-333.

- - (1959), O n representations of the Mathieu groups as collineation groups, J.London Math.Soc., 34, pp.406-416.

- - (1966), A representation of the Mathieu group M_{24} as a collineation group, Ann.di Mat.Pura e Appl., 71, pp.199-238.

- - (1970), Abstract definitions for the Mathieu groups, Quart.J.Math.Oxford (2), 21, pp.421-424.

TRAN VAN TRUNG(1980), Eine Kennzeichnung der endlichen ainfachen Gruppe J_4 von Janko durch eine 2-lokale Untergruppe, Rend.Sem.Mat.Univ.Padova, 62, pp.35-45.

TURYN R.J.(1966), A simple construction of the binary Golay code, A note produced under Contract AF19(628)-5998 of the Office of Aerospace Research at the Air Force Cambridge Research Labs.(USA).

VENKOV B.B. (1980), On the classification of integral even unimodular 24-dimensional quadratic forms. Proc.Steklov. Inst.Math., 4, pp.63-74.

WAGNER A.(1980), Determination of the finite primitive reflection groups over an arbitrary field of characteristic not two.I, Geom.Dedicata, 9, pp.239-253.

- - (1981), Determination of . . . .II,III, Geom.Dedicata. 10, pp.191-203,475-523.

WALES D.B.(1969A), Uniqueness of the graph of a rank 3 group, Pacific J.Math., 30, pp.271-276.

- - (1969B), The uniqueness of the simple group of order 604.800 as a subgroup of SL(6,4), J.Algebra, 11, pp.455-460.

WARDH.N. (1972). Representations of symplectic groups, J. Algebra, 20, pp. 185-195.

- - (1975). A form for Mll, J.Algebra, 37, pp.340-361.

WHITELAW J.A.(1966), On the Mathieu group of degree twelve, Proc. Camb.Phil.Soc., 62, pp.351-364.

WIELANDT H.(1960), Über den Transitivität von Permutations Gruppen, Math.Z.,74, pp.297-298.

- - (1964), Finite Permutat ion Groups, Academic Press, New York.

WILSON R.A. (1982), Maximal subgroups of some finite simple groups, Ph.D.Thesis, University of Cambridge.

WITT E. (1938A), Die 5-fach transitiven Gruppen von Mathieu, Abh.Math.Sem.Univ.Hamburg. 12, pp.256-264.

- - (1938B), Über Steinersche Systeme, Abh.Math.Sem.Univ. Hamburg. 12, pp.265-275.

WONG S.K. (1977), A characterization of the Fischer group M(23) by a 2-local subgroup, J.Algebra, 44, pp.143-151.

WONG W.J.(1964A), On finite groups whose 2-Sylow subgroups have cyclic subgroups of index 2, J.Austral .Math.Soc. ,4, pp.90-112.

- - (1964B), A characterization of the Mathieu group M_{12}, Math.Z.,84, pp.378-388.

YAMAKI H.(1975), Finite groups with Sylow 2-subgroups of type A_{16}, J-Algebra, 33, pp.523-566.

YOSHIDA T.(1974), A characterization of Conway's group C_3, Hokkaido Math.J., 3, pp.232-242.

- - (1977), A characterization of the $\cdot 2$ Conway simple group. J.Algebra, 46, pp.405-414.

YOSHIZAWA M.(1977), Quadruply-transitive permutation groups whose four-point stabilizer is a Frobenius group, Proc.Jap.Acad.(A), 53, pp.20-22.

- - (1978A), 5-fold transitive permutation groups in which the stabilizer of five points has a normal Sylow-2-subgroup, Osaka J.Math., 15, pp.343-350.

- - (1978B), On 2p-fold transitive permutation groups. Tokyo J.Math., 1, pp.263-267.

- - (1979A), On multiply transitive permutation groups.I, Osaka J.Math.,16, pp.775-795.

- - (19798). Remarks on multiply transitive permutation groups, Osaka J.Math.,16, pp.31-34.

- - (1980). On 2p-fold transitive permutation groups, 11, Proc.Jap.Acad.(A), 56, pp.45-49.

ZAPPA G.(1970), Fondamenti di Teoria dei Gruppi, Vol.II, Cremonese, Roma.

ZASSENHAUS H.(1935), Über transitive Erweiterungen gewisser Gruppen aus Automorphismen endlicher mehrdimensionaler Geometrien, Math.Ann.,111, pp.748-759.

- - (1936), Kennzeichnung endl icher 1 inearer Gruppen als Permutations-gruppen. Abh.Math.Sem.Univ.Hamburg, 11, pp.17-40.

ASCHBACHER M., GURALNICK R. (1984), Some applications of the first cohomology group, J-Algebra. 90, pp.446-460.

COLLINS M.J.(1984), Some subgroups of M_{24}, unpublished.

CONWAYJ.M.(1982), Mexacode and Tetracode - MOG and MINIMOG, in "Computational Group Theory", ed. M.D.Atkinson, Proc.LMS Symp.Durham 1982, Academic Press 1984, pp.359-365.

CURTIS R.T.(1982), The Steiner system S(5,6,12), the Mathieu group M_{12} and the "Kitten". in Computational Group Theory", ed. M.D. Atkinson, Proc. LMS Symp. Durham 1982, Academic Press 1984, pp.353-358.

DALLA VOLTA F. (1984). Gruppi sporadici generati da tre involuzioni, in corso di stampa su Rend.Ist.Lomb.

GILLIO A., TAMBURINI M.C. (1982), Alcune classi di gruppi generati da tre involuzioni, in corso di stampa su Rend. 1st. Lomb.

GORENSTEIN D.(1983), The classification of finite simple groups. Volume 1: Groups of Noncharacteristic 2 Type, The University Series in Math.. Plenum Press, New York.

HUMPHREYS J.F. (1983), Projective character tables for the finite simple groups of order less than one million, Comm. Algebra, 11(7), pp.725-751.

KADIR G.A., KEY J.D.(1984), The Steiner system S(5.8.24) constructed from dual affine planes. Preprint.

KANTOR W.M.(1983), Homogeneous designs and geometric lattices, Preprint.

KRAMER E.S., LEAVITT D.W., MAGLIVERAS S.S.(1984), Construction procedures for t-designs and the existence of new simple 6-designs, Preprint.

LEMPKEN W. (1984). The maximal subgroups of J_4. Dissertation, Mainz.

WAGNER A. (1978), The nimimal number of involutions generating some three-dimensiona1 groups, Boll.Un.Mat.Ital.. 15-A, pp.431-439.

WILSON R.A.(1983), The complex Leech lattice and the maximal subgroups of the Suzuki group. J. Algebra, 84, PP. 151-188.

Ricevuto il 28/7/1984

Indirizzo dell'Autore: Dipartimento di Matematica "F.Enriques"
Università
Via C. Saldini, 50
20133 MILANO