Gruppeteori (28.07.08)

I historiske tilbakeblikk sier man ofte at gruppeteorien startet med Galois (1811-1832).

Men det første viktige teorem vi presenteres for i gruppeteorien er at hvis H er en undergruppe av en endelig gruppe G, så er ordenen for H en divisor i ordenen for G (orden = antall elementer).

Det er teoremet til Lagrange (1736-1813).

Likevel bør nok Galois fremheves fordi han viste at *gruppeteori er et sentralt verktøy i studiet av symmetriforhold* i andre matematiske strukturer.

For Galois var temaet polynomligninger, men etter hvert viste det seg f.eks. at *gruppeteorien gjorde det mulig å klassifisere alle mulige krystallformer.*
Gruppeteoretisk beskrivelse av symmetriforhold i andre deler av fysikken har bl.a. ledet til *forutsigelse av elementærpartikler*, som senere er påvist eksperimentelt.

Grupper som beskriver symmetririke “objekter” er også et hovedtema i det som følger!

Endelige simple grupper

H **er en *normal* undergruppe av *G* dersom, for alle $g \in G$**

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$$

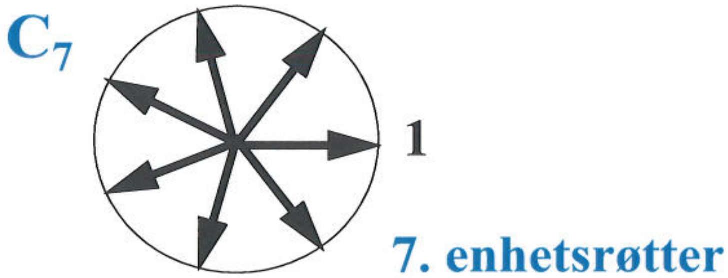
En gruppe *G* er *simpel* hvis den har nøyaktig to normale undergrupper: de trivielle {1} og *G*.

De endelige simple grupper er de grunnleggende bestanddeler som alle endelige grupper er bygget opp av. De er fullstendig klassifisert.

Vi nøyer oss med en *grovinndeling i 4 familier. De 3 første er uendelige*:

1 Gruppene C_p av primtallsorden p

Disse er sykliske og kan, som alle sykliske grupper, synliggjøres som multiplikative grupper av komplekse enhetsrøtter.



C_7 kan da også sees som rotasjonssymmetriene av en 7-kant!

2 De alternerende gruppene A_n for n>4

Disse består av alle n!/2 jamne permutasjoner av n objekter. A_5, av orden 60, er den minste simple gruppe av sammensatt orden. Simplisiteten forklarer at femtegradsligningen ikke kan løses med rottegn! A_5 kan visualiseres slik: En fotball sydd av 20 sekskanter og 12 femkanter har 60 *rotasjonssymmetrier*.

Se på rotasjonaksene!

6 akser $x \cdot 72^o$ 24 rotasjoner

10 akser $x \cdot 120^o$ 20 rotasjoner

15 akser 180^o 15 rotasjoner

Identiteten 1 "rotasjon"

Gruppens orden = 60

De 15 180^o-aksene danner 5 rettvinklede aksekors som selv permuteres av rotasjonene. Dermed gjenkjenner vi A_5!

3 Grupper av Lie-type, knyttet til Liealgebraer

Lie-familien deles ofte opp i underfamilier, f.eks. de ulike "klassiske" gruppene over endelige kropper. Den nestminste av alle simple grupper av sammensatt orden har orden 168, og er "klassisk". Den har også en kjent og kjær visualisering:

Fanoplanet består av 7 "punkt" A, B, C, D, E, F, G og like mange 3-punktsmengder kalt "linjer". Gruppen består av 168 *linjebevarende permutasjoner* av punktene. Eksempel:

Linjer: **{A,B,C}**; **{G,D,A}**; **{F,C,G}**; **{E,A,F}**; **{B,G,E}**; **{D,F,B}**; **{C,E,D}**

4 De sporadiske gruppene

De *26 sporadiske grupper* er simple men faller utenfor familiene 1, 2 og 3.

[Noen sier 27 fordi gruppen til Tits, av orden 17971200 = $2^{11}3^{3}5^{2}13$ er simpel og også, strengt tatt, faller utenfor. Men den er tilgjengelig som normal undergruppe i en gruppe som selv er av Lie-type og som har den dobbelte orden, $2^{12}3^{3}5^{2}13$.]

Mathieu oppdaget gruppene M_{11} og M_{12} i 1861 og deretter M_{22}, M_{23} og M_{24} i 1873, men en klar og nyttig presentasjon ble først gitt av Witt i 1938.

M_{24}, av orden 244823040,

inneholder de andre Mathieu-gruppene som undergrupper.

Først i 1965 oppdaget Janko en ny sporadisk gruppe, J_1, av orden 175560. Flere ble funnet noen år fremover, med svært ulike metoder. Klassifikasjonsteoremet gjør det klart det ikke er flere igjen å finne. 20 av de sporadiske gruppene finnes i den største av dem, nemlig *"Monsteret"*, av orden

808017424794512875886459904961710757005754368000000000 ≈ $8*10^{53}$.

Vi skal se på noen svært spesielle symmetririke objekter som gir opphav til mange av de sporadiske simple gruppene.

Den binære "utvidede" Golaykoden

En innfallsport til de fleste sporadiske gruppene er en av de feilkorrigerende kodene som ble funnet av Marcel Golay (1949). Betrakt vektorrommet F_2^{24}: vektorene har 24 koordinater hentet fra $F_2 = \{0,1\}$. Golaykoden utgjør et underrom av dimensjon 12 der vektorene parvis er ulike i minst 8 koordinater ("*Hammingdistanse*" $\geq$ 8).

I løpet av noen timer finner et leteprogram 4095 vektorer i tillegg til nullvektoren:

finne-nr	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X		lete-nr
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	8	255
2	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	8	3855
3	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	8	4080
4	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	8	13107
5	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0	8	13260
6	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	8	15420
7	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1	8	15555
31	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	16	65535
38	0	0	0	0	0	0	1	1	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	0	12	212842
4095	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	24	16777215

759 vektorer med 8 1-ere, 2576 med 12 1-ere, 759 med 16 1-ere.

Oktadene

De 579 kodevektorene med 8 1-ere kalles *oktader*; de noteres også som undermengder av 8 elementer i {A, B, C, D, E, ... , X} definert av 1-erne i kodevektoren. Linje 3 i forrige tabell viser oktaden {M, N, O, P, U, V, W, X}. [Det er 2576 *dodekader*.] To oktader kan høyst ha 4 elementer felles. Hvorfor?

Legg merke til at addisjonen av vektorene nr 2 og 3 i forrige tabell gir vektor 4:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
+	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
=	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0

Vektoraddisjon tilsvarer "symmetrisk differanse" mellom mengdene:

$$\{M,N,O,P,U,V,W,X\} \,\Delta\, \{Q,R,S,T,U,V,W,X\}$$
$$= \{M,N,O,P,Q,R,S,T\}$$

Hvis to oktader hadde 5 eller flere elementer felles, ville summen av dem ha fått mindre enn 8 1-ere!

De 759 oktadene utgjør et *Steinersystem*. Hva betyr det?

Steinersystemet (5, 8, 24)

En 5-bokstavsmengde kan altså ikke tilhøre mer enn én oktade! La oss telle:

I en oktade er det $\binom{8}{5} = \dfrac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 56$ **5-bokstavsmengder.**

Hvor mange 5-bokstavsmengder inneholder da alle oktadene til sammen?

$$759 \cdot \binom{8}{5} = (3 \cdot 23 \cdot 11) \cdot (8 \cdot 7) = 24 \cdot 23 \cdot 11 \cdot 7$$

$$= \frac{24 \cdot 23 \cdot (11 \cdot 2) \cdot (7 \cdot 3) \cdot (5 \cdot 4)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = \binom{24}{5}.$$

Vi har redegjort for alle 5-bokstavsmengdene! Altså

Hver 5-bokstavsmengde
tilhører nøyaktig én oktade!

Vi har allerede sett et Steinersystem (2,3,7), nemlig Fanoplanet.
Men systemet (5,8,24) har mye større symmetrigruppe!

Mathieugruppen M_{24}

Gruppen S_{24} består av alle de 24! permutasjonene av de 24 bokstavene [standardbasisvektorene] A, ... , X. Undergruppen M_{24} består av

de *permutasjonene som avbilder oktader på oktader*.

Se også på permutasjonene som lineære transformasjoner av vektorrommet F_2^{24} på seg selv; *de bevarer underrommet utspent av oktadene, altså det 12-dimensjonale underrommet av kodeord i Golay-koden.*

Antallet slike permutasjoner, dvs. ordenen for M_{24} er

$$244\,823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$$

M_{24} er 5-transitiv; det betyr at gitt to (ordnede) 5-tupler, f.eks

{A, B, C, D, E} og {R, X, P, C, B},

så finnes det en permutasjon λ i M_{24} slik at

$$\lambda:\ A \to R,\ B \to X,\ C \to P,\ D \to C,\ E \to B$$

Leechlatticen Λ

Latticen ble funnet av John Leech i 1965. Vektoren

$$(a_1, a_2, a_3, \dots, a_{24})$$

har *heltallskoordinater* og tilhører Λ hvis og bare hvis følgende krav er oppfylt:

1) *mod 8-kravene*:

$$4a_1 \equiv 4a_2 \equiv \dots \equiv 4a_{24} \equiv (a_1 + a_2 + \dots + a_{24}) \pmod 8$$

P.g.a mod 8-kravene er a_i jamn for alle i eller odde for alle i.

2) *Kodekravet*:

for $m=0,1,2,3$ vil $\{i \mid a_i \equiv m \pmod 4\}$ definere et element i Golaykoden.

Kodekravet er at en restklasse mod 4 har "støtte" i et kodeord.

Disse egenskapene gjør Leechlatticen lukket under addisjon og subtraksjon.

Leech-vektorene av minimal lengde, $4\sqrt{2}$

type	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	$4a_i,\Sigma$	a_i
I	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 (m8)	0,2(m4)
IIa	3	-1	-1	-1	-1	-1	-1	-1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4 (m8)	1,3(m4)
IIb	1	1	1	1	1	1	3	-1	1	1	-1	-1	-1	-1	-1	-1	1	-1	-1	1	-1	1	-1	1	4 (m8)	1,3(m4)
IIc	1	1	1	1	1	1	1	1	3	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	4 (m8)	1,3(m4)
IId	3	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	4 (m8)	3 (m4)
III	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0 (m8)	0 (m4)

Type I) 2-erne fyller en oktade og gis fortegn + eller -, et *jamnt* antall av hvert, på grunn av et mod 8-krav.

Subtotal $759*2^7$ = **97152**

Type II) Skriv 3 i en vilkårlig koordinat; velg et av de 2^{11} kodeord som bruker koordinaten, skriv -1 ellers i koordinatene for kodeordet og 1 i de øvrige koordinater. Vektoren kan så multipliseres med -1.

Subtotal $24*\ 2^{11}*2$ = **98304**

Type III) I to vilkårlige posisjoner står 4 eller -4 (altså 4 muligheter).

Subtotal $2^2*24*23/2$ = **1104**

Totalt antall nærmeste naboer til en Leech-vektor er 196560

M_{24} permuterer standardbasisvektorene og Leech-vektorene, men det skjer innenfor hver av disse typene og undertypene.

Conways gruppe Co_1

I 1967 studerte John H Conway Leechlatticen. Eksisterte ortogonale transformasjoner som "fusjonerte" alle typene av korteste vektorer?
Conway fant slike transformasjoner; dermed eksisterte symmetrier som fikk alle typene til å smelte sammen til én type. Ved sammensetninger av disse symmetriene redegjorde Conway for en simpel gruppe Co_1 av orden

$$(1/2) \cdot 8\,315553\,613086\,720000 =$$

$$(1/2) \cdot 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23.$$

Den store gruppen, Co_0, av orden $\approx 8 \cdot 10^{18}$, er analog til "fotballgruppen", men Co_0 har en normal undergruppe {I, -I} av orden 2. Inne i kvotienten Co_1 fant Conway og Thompson alle Mathieugruppene, fire av de andre sporadiske som til da var funnet, samt to tidligere ukjente, Co_2 og Co_3.

Omtrent samtidig hadde Bernd Fischer, med helt andre midler, funnet tre sporadiske grupper, Fi_{24}, Fi_{23}, Fi_{22} som også inneholdt Mathieugrupper.

Og etter hvert ble det grunn til å tro at det var mer igjen å finne!

“Monsteret”

Monsteret dukket først opp som en mulighet (Bernd Fischer og Robert Griess 1973). Man fant en rekke egenskaper Monsteret måtte ha - hvis det eksisterte og oppfylte visse hypoteser.

Griess klarte så (1980) å konstruere en reell, kommutativ, ikke-assosiativ **algebra av dimensjon 196884**, som har nettopp Monsteret som automorfigruppe, en gruppe av orden

$$2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Dimensjonstallets nærhet til **196560** = antallet minimale Leechvektorer [**196884 = 196560 + 324**] er ikke tilfeldig: Griessalgebraen kan konstrueres ved hjelp av Leechlatticen, som igjen var konstruert ved hjelp av den utvidede binære Golaykoden.

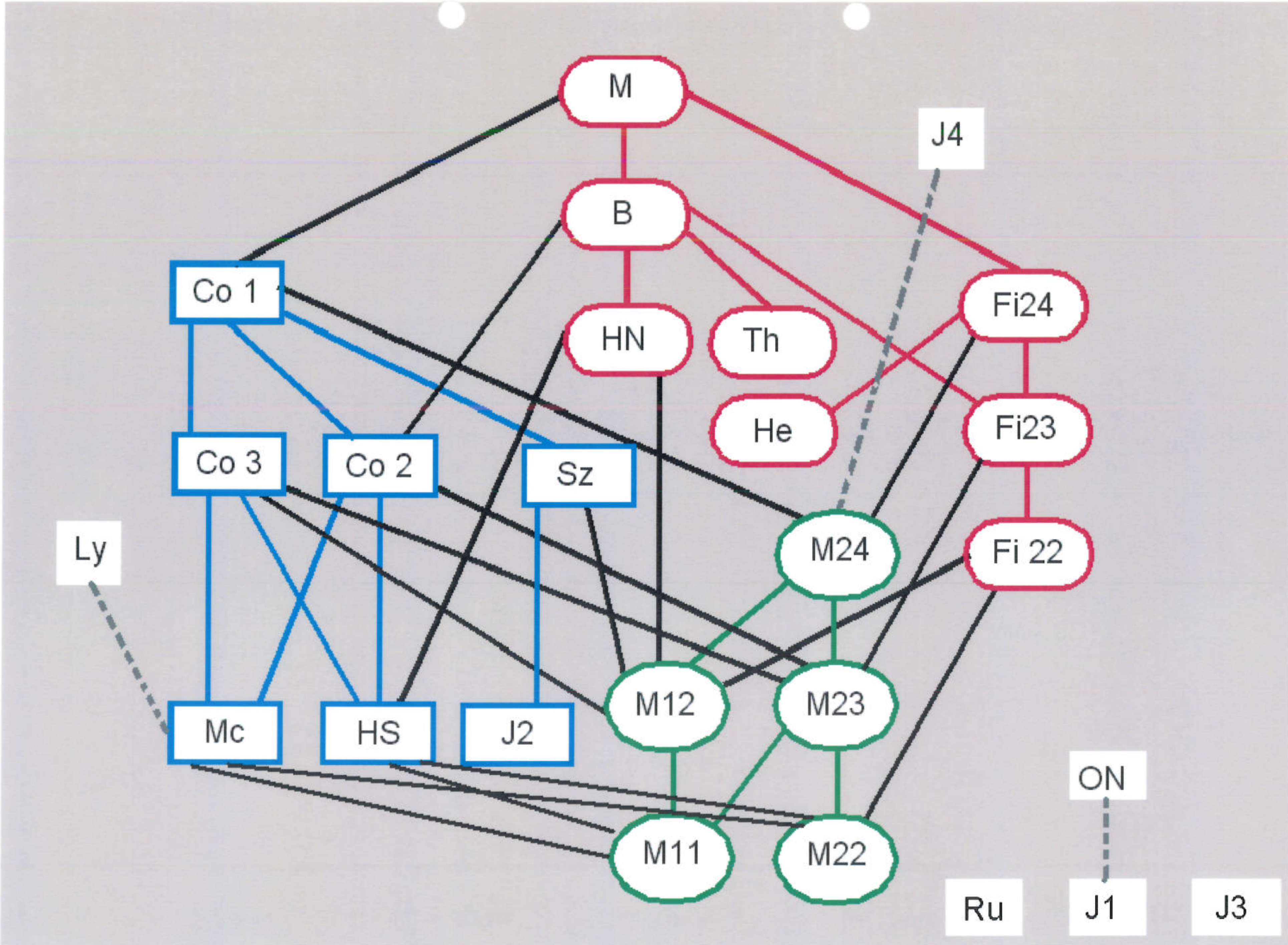
Et tilbakeblikk

Vi har beskrevet en utviklingslinje:

fra Mathieus observervasjoner av 5 sporadiske grupper,
via *Steinersystemet* og *Golaykoden*
som gjorde dem tilgjengelige, så via nye oppdagelser,
først av *Leech-latticen* og Conway-gruppene,
og videre via indikasjoner om eksistens frem til
til *Griessalgebraen* som bekreftet at Monsteret eksisterer.

Griess omtaler Monsteret som "The Friendly Giant" og de 20 sporadiske gruppene i den som "The Happy Family", delt i 1., 2. og 3.generasjon!

Og der starter en ny fortelling, om Monsterets relasjon til modulære funksjoner, hyperbolsk geometri og teoretisk fysikk.



Fra Mark Ronan: *Symmetry and the Monster*