Ideas in finite group theory

Martino Garonzi
PhD student
Supervisor: Andrea Lucchini
University of Padova

Seminario Dottorato
February 27th 2013

Invertible matrices

Let F be a field (for example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$). Let

$$GL(n, F) \qquad \text{(General Linear Group)}$$

denote the set of $n \times n$ invertible matrices with entries in the field F. The usual row-column multiplication gives $GL(n, F)$ the structure of a (non-abelian!) group.

$F^* := F - \{0\}$ is a group with respect to multiplication.
It is abelian (commutative).

$\det : GL(n, F) \to F^*$ is a **group homomorphism**. Its kernel $\ker(\det)$ is denoted

$$SL(n, F) \qquad \text{(Special Linear Group).}$$

It consists of the $n \times n$ matrices with entries in F and determinant 1.

Permutations

The Symmetric Group: $\mathrm{Sym}(n) =$ the group of bijections

$$\{1,\dots,n\} \to \{1,\dots,n\}$$

with the operation given by the **composition**. An element of $\mathrm{Sym}(n)$ is called permutation of $\{1,\dots,n\}$. The order of $\mathrm{Sym}(n)$ (its size as a set) is $n! = 1 \cdot 2 \cdots n$. For example

$$(123)(4567): \qquad 1 \mapsto 2 \mapsto 3 \mapsto 1, \qquad 4 \mapsto 5 \mapsto 6 \mapsto 7 \mapsto 4.$$

$$(123\cdots k): \qquad 1 \mapsto 2 \mapsto 3 \mapsto \cdots \mapsto k \mapsto 1 \qquad k\text{-cycle}.$$

Composition goes as follows:

$$(12)(234)(13) = (234), \qquad (143)(1352)(4312) = (13)(45).$$

Note that disjoint cycles always commute.

$$(123)(4567) = (4567)(123).$$

Remark

Every permutation can be written uniquely (up to reordering) as **product of disjoint cycles**.

Definition

A permutation is called "even" if it can be written as the product of an even number of 2-cycles, and "odd" otherwise. For example $(12)(25)(13)(35)$ *is even,* $(13)(26)(43)$ *is odd.*
A product of disjoint cycles is an even permutation if and only if the number of cycles of even length is even.

Example:

$$(123)(4567), \qquad (12)(3456)(78) \qquad ODD,$$

$$(123)(45)(67), \qquad (123)(4567)(89) \qquad EVEN.$$

- All elements of cycle structure $(3,4)$, $(2,2,4)$ are odd.
- All elements of cycle structure $(2,2,3)$, $(2,3,4)$ are even.

Definition (Alternating group)

Even permutations are said to have sign 1.
$\sigma \in Sym(n)$ *is even if* $sgn(\sigma) = 1$.

Odd permutations are said to have sign -1.
$\sigma \in Sym(n)$ *is odd if* $sgn(\sigma) = -1$.

$sgn : Sym(n) \to \{-1, 1\} = C_2$ *is a group homomorphism.*

Its kernel $\ker(sgn)$ *is denoted* $Alt(n)$ *or* A_n*: it is the Alternating group of degree* n*. It is a normal subgroup of* $Sym(n)$*. Its order is* $n!/2$.

For **example** Alt(4) consists of the following elements.

$$\begin{array}{cccc} 1, & (12)(34), & (13)(24), & (14)(23), \\ (123), & (132), & (124), & (142), \\ (234), & (243), & (134), & (143). \end{array}$$

To each polynomial $f(X) \in \mathbb{Q}[X]$ without multiple roots can be attached a finite group G_f, called the Galois group of the polynomial (named after **Evariste Galois, 1811 - 1832**). It is defined as follows: if $a_1, \ldots, a_n \in \mathbb{C}$ denote the distinct roots of $f(X)$ then

$$G_f = \mathrm{Aut}(\mathbb{Q}(a_1, \ldots, a_n)).$$

That is, G_f is the group of ring isomorphisms

$$\mathbb{Q}(a_1, \ldots, a_n) \to \mathbb{Q}(a_1, \ldots, a_n).$$

The group G_f permutes the roots of f, and the only element of G_f which fixes all the roots is the identity. In other words, G_f can be described (or better, "represented") as a subgroup of $\mathrm{Sym}(n)$.

For **example** the Galois group of $X^2 - 2$ is the automorphism group of the field $\mathbb{Q}(\sqrt{2})$, so it consists of two elements: the identity and the automorphism $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ which sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$. The Galois group of $X^2 - 2$ is cyclic of order 2. $G_f \cong \mathrm{Sym}(2) \cong C_2$.

The Galois group encodes the factorization patterns modulo prime numbers.

Let us be more precise. Let $f(X)$ be an irreducible polynomial of $\mathbb{Z}[X]$ of degree n. According to a theorem of Frobenius,

- if for a prime p for which $f(X)$ mod p does not admit multiple irreducible factors (such prime is usually called "unramified") the factorization pattern of $f(X)$ mod p is $(n_1, \ldots, n_t)$ (meaning that there are t irreducible factors of degrees $n_1, \ldots, n_t$)
- then the Galois group of $f(X)$, seen as a (transitive) subgroup of $\mathrm{Sym}(n)$, contains an element of cycle structure $(n_1, \ldots, n_t)$.

Let us consider the following **examples**:

- $X^3 + X^2 + X + 3$ (discriminant $-204 = -2^2 \cdot 3 \cdot 17$);
- $X^3 - 3X + 1$ (discriminant $81 = 3^4$).

p	X^3+X^2+X+3	p	X^3+X^2+X+3
2	$(X+1)^3$	53	$(X+43)(X^2+11X+5)$
3	$X(X+2)^2$	59	$(X+12)(X^2+48X+15)$
5	X^3+X^2+X+3	61	$(X+6)(X^2+56X+31)$
7	$(X+4)(X^2+4X+6)$	67	$(X+23)(X+52)(X+60)$
11	X^3+X^2+X+3	71	$(X+38)(X+52)(X+53)$
13	X^3+X^2+X+3	73	$(X+34)(X^2+40X+28)$
17	$(X+5)(X+15)^2$	79	$(X+74)(X^2+6X+31)$
19	X^3+X^2+X+3	83	$(X+45)(X^2+39X+72)$
23	X^3+X^2+X+3	89	$(X+32)(X^2+58X+14)$
29	$(X+11)(X+23)(X+25)$	97	$(X+59)(X^2+39X+28)$
31	$(X+15)(X^2+17X+25)$	101	$(X+75)(X^2+27X+97)$
37	$(X+25)(X^2+13X+9)$	103	X^3+X^2+X+3
41	X^3+X^2+X+3	107	X^3+X^2+X+3
43	X^3+X^2+X+3	113	X^3+X^2+X+3
47	$(X+31)(X^2+17X+38)$	127	X^3+X^2+X+3

$\mathrm{Sym}(3)=\{1,(12),(13),(23),(123),(132)\}$.

p	X^3-3X+1	p	X^3-3X+1
2	X^3+X+1	53	$(X+18)(X+39)(X+49)$
3	$(X+1)^3$	59	$X^3+56X+1$
5	X^3+2X+1	61	$X^3+58X+1$
7	X^3+4X+1	67	$X^3+64X+1$
11	X^3+8X+1	71	$(X+16)(X+25)(X+30)$
13	$X^3+10X+1$	73	$(X+14)(X+25)(X+34)$
17	$(X+3)(X+4)(X+10)$	79	$X^3+76X+1$
19	$(X+10)(X+12)(X+16)$	83	$X^3+80X+1$
23	$X^3+20X+1$	89	$(X+12)(X+36)(X+41)$
29	$X^3+26X+1$	97	$X^3+94X+1$
31	$X^3+28X+1$	101	$X^3+98X+1$
37	$(X+14)(X+28)(X+32)$	103	$X^3+100X+1$
41	$X^3+38X+1$	107	$(X+7)(X+40)(X+60)$
43	$X^3+40X+1$	113	$X^3+110X+1$
47	$X^3+44X+1$	127	$(X+53)(X+87)(X+114)$

$\mathrm{Alt}(3)=\{1,(123),(132)\}\subset \mathrm{Sym}(3)$.

The most famous open problem in group theory is probably the Inverse Galois Problem.

Inverse Galois Problem

Is it true that for any finite group G there exists a polynomial $f(X) \in \mathbb{Q}[X]$ with $G_f \cong G$?

This problem has been solved for abelian groups (even solvable groups), but the answer in general is not known.

Let us list the important results of "elementary" finite group theory.

- the **"order" of an element** $g \in G$, denoted $o(g)$, is the smallest positive integer n such that $g^n = 1$;
- the **"order" of a subgroup** $H \leq G$, denoted $|H|$, is its size.
- It turns out that $|\langle g \rangle| = o(g)$.

Theorem (Lagrange (1736 - 1813))

*Let G be a finite group, and let $H \leq G$. Then $|H|$ divides $|G|$. The integer $|G|/|H| = |G : H|$ is called the "**index**" of H in G.*

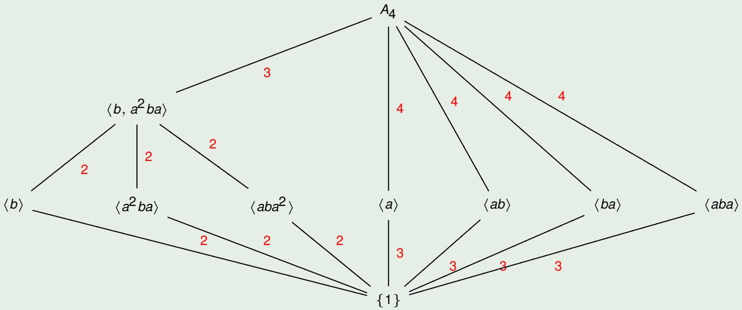
Not every divisor of $|G|$ equals the size of a subgroup of G, but...

Theorem (Cauchy (1789 - 1857))

Let G be a finite group, and let p be a prime dividing $|G|$. Then there exists $g \in G$ of order p.

Example: The alternating group of degree 4

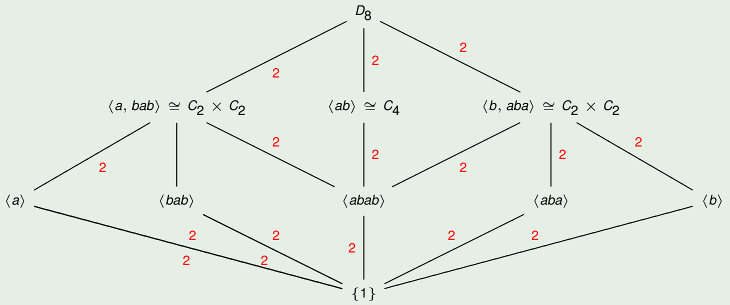
$A_4 = \langle a, b \rangle$ where $a = (123)$ and $b = (12)(34)$.
$|A_4| = 4!/2 = 12 = 2^2 \cdot 3$. Subgroup lattice:



$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (234), (243), (134), (143)\}$.
Note that A_4 has no subgroups of order 6.

Example: The dihedral group of order 8

$D_8 = \langle a, b \mid a^2 = b^2 = 1,\ (ab)^4 = 1 \rangle$. $|D_8| = 8 = 2^3$. Subgroup lattice:



Note that D_8 has subgroups of order $1, 2, 4, 8$.

Suppose $|G|$ is divisible by a prime-power p^k. Can we always find a subgroup $H \leq G$ with $|H| = p^k$?

Theorem (Sylow (1832 - 1918))

Let G be a finite group and write $|G| = mp^n$ where p is a prime and m is not divisible by p.

- *G contains a subgroup P of order p^n. P is called "Sylow p-subgroup" of G.*
- *G contains a subgroup of order p^k for every $0 \leq k \leq n$.*
- *If P, Q are two Sylow p-subgroups of G then they are conjugated: there exists $g \in G$ such that $g^{-1}Pg = Q$.*
- *The number of Sylow p-subgroups of G is congruent to $1 \mod p$.*
- *If H is a subgroup of G such that $|H|$ is a power of p then there exists a Sylow p-subgroup P of G such that $H \leq P$.*

Example

Let $F = \mathbb{Z}/5\mathbb{Z}$ and let

$$G := \{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \ : \ a, b, c \in F, \ a, c \neq 0 \},$$

$$H := \{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G \ : \ b = 0 \},$$

$$K := \{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G \ : \ a = c = 1 \}.$$

- G is a group (with respect to multiplication) of order $4^2 \cdot 5 = 2^4 \cdot 5$,
- $|H| = 4^2 = 2^4 \Rightarrow H$ is a Sylow 2-subgroup of G and
- $|K| = 5 \Rightarrow K$ is a Sylow 5-subgroup of G.

Theorem (Cayley (1821 - 1895))

Let G be a group. Then the application

$$G \to \mathrm{Sym}(G), \qquad g \mapsto (x \mapsto gx)$$

is an injective homomorphism.
In particular, G is isomorphic with a subgroup of $\mathrm{Sym}(G)$.

Corollary

Let G be a finite group. There exists a positive integer n such that G is isomorphic with a subgroup of $\mathrm{Sym}(n)$.

Cayley's theorem says we may choose $n = |G|$. But sometimes we can choose a smaller n.

For **example**, if G_f is the Galois group of the polynomial $f(X) \in \mathbb{Q}[X]$ with n distinct roots, then the permutation action of G_f on the n roots gives an injective homomorphism $G_f \to \mathrm{Sym}(n)$.

Simple group G is **simple** if $\{1\}$ and G are the only normal subgroups of G.

Abelian simple groups

Abelian simple groups are the cyclic groups of prime order, $C_p = \{g, g^2, \ldots, g^{p-1}, g^p = 1\} \cong (\mathbb{Z}/p\mathbb{Z}, +) = \{1, 2, \ldots, p-1, p = 0\}$.

Alternating Groups

If $n \geq 5$ is an integer, $\mathrm{Alt}(n)$ is a non-abelian simple group.

Projective Linear Groups

Let F be a field, and let $GL(n, F)$ be the group of invertible matrices over the field F. Let $SL(n, F)$ be the subgroup of $GL(n, F)$ consisting of matrices of determinant 1. Let Z be the subgroup of $GL(n, F)$ consisting of scalar matrices. If $n \geq 2$ and $|F| \geq 4$, the quotient

$$PSL(n, F) := SL(n, F)/Z \cap SL(n, F)$$

(projective linear group) is an example of non-abelian simple group.

Given a finite group G, we can costruct longest possible chains of subgroups of the form

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_k = G.$$

Maximality of k implies that the factor groups G_i/G_{i-1} are all simple groups. Such chain is called "**composition series**" and its factors G_i/G_{i-1} are called "**composition factors**".

Theorem (Jordan-Holder)

Any two composition series of a given finite group have the same length and the same composition factors (up to reordering and isomorphism).

Cyclic groups

The composition factors of a cyclic group C_n correspond to the prime divisors of n, counted with multiplicity. If $n = 60 = 2^2 \cdot 3 \cdot 5$,

$$1 \lhd \langle g^{30} \rangle (\cong C_2) \lhd \langle g^{15} \rangle (\cong C_4) \lhd \langle g^5 \rangle (\cong C_{12}) \lhd \langle g \rangle = C_{60}.$$

Solvable group If the composition factors of the finite group G are all abelian (hence cyclic of prime order) then G is said to be **solvable**.

Evariste Galois proved that the zeros of a polynomial $f(X) \in \mathbb{Q}[X]$ can be expressed by starting from the elements of $\mathbb{Q}$ and performing sums, differences, products, divisions, and root extractions if and only if the Galois group G_f is solvable. In this case $f(X)$ is said to be "**solvable by radicals**".

Degrees $2, 3, 4$

Polynomials of degree 2, 3, 4 are solvable by radicals.

Indeed, all subgroups of Sym(4) are solvable.

Example

The Galois group of $f(X) = X^4 - 4X + 2 \in \mathbb{Z}[X]$ is S_4, so $f(X)$ is solvable by radicals. Indeed, S_4 is solvable:

$$\{1\} \xrightarrow{C_2} \langle (12)(34) \rangle \xrightarrow{C_2} O_2(S_4) \xrightarrow{C_3} A_4 \xrightarrow{C_2} S_4$$

The composition factors of S_4 are C_2 (three times) and C_3.
$|S_4| = 24 = 2^3 \cdot 3$.

Example

The symmetric group S_n is not solvable when $n \geq 5$:

$$\{1\} \xrightarrow{A_n} A_n \xrightarrow{C_2} S_n$$

The composition factors of S_n are A_n (not abelian) and C_2.

- Any subgroup of a solvable group is solvable.
- Any quotient of a solvable group is solvable.
- Any finite direct product of solvable groups is solvable.
- If $N \trianglelefteq G$ and G/N are solvable then G is solvable.

EXAMPLE

Abelian groups are solvable.

EXAMPLE

Suppose the order of the finite group G is a prime-power, $|G| = p^n$, where p is a prime. Then G is solvable.

EXAMPLE

A direct product of finitely many groups of prime-power order is solvable.

A non-solvable polynomial

Consider the polynomial $f(X) = X^5 - 2X - 2$, irreducible in $\mathbb{Q}[X]$. Its discriminant is $41808 = 2^4 \cdot 3 \cdot 13 \cdot 67$.

- Reduction modulo 5: $(X+2)(X^4+3X^3+4X^2+2X+4)$.
- Reduction modulo 7: X^5+5X+5.
- Reduction modulo 17: $(X^2+X+6)(X^3+16X^2+12X+11)$.
- The Galois group G_f of $f(X)$ is a subgroup of $\mathrm{Sym}(5)$ containing elements of cycle structures (4), (5) and $(3,2)$.
- Deduce that $G_f = \mathrm{Sym}(5)$.
- $\mathrm{Sym}(5)$ contains the non-abelian simple group $\mathrm{Alt}(5)$, hence G_f is non-solvable.
- $f(X) = X^5 - 2X - 2$ is not solvable by radicals.

A finite group is said to be **nilpotent** if it is a direct product of finitely many groups of prime-power order. Equivalently, a finite group is nilpotent if and only if its Sylow subgroups are all normal.

- Cyclic groups are abelian. $C_2 \times C_2$ is abelian but not cyclic.
- Abelian groups are nilpotent. D_8 is nilpotent but not abelian.
- Nilpotent groups are solvable. S_3 is solvable but not nilpotent.
- A_5 is a non-abelian simple group. In particular it is not solvable.

Cyclic $\subset$ *Abelian* $\subset$ *Nilpotent* $\subset$ *Solvable*.

When facing a problem concerning finite groups, one usually goes through all these steps before dealing with the general case.

Feit and Thompson proved the following very deep result.

Theorem (Feit, Thompson, 1962-1963)

Any finite group of odd order is solvable.

This result is called the "Odd Order Theorem". It implies that **non-abelian finite simple groups have even order**.

With this as a starting point, all finite non-abelian simple groups have been classified:

Theorem

Let S be a non-abelian simple group. Then one of the following holds.

- $S \cong C_p$ *for some prime* p.
- $S \cong Alt(n)$ *for some integer* $n \geq 5$.
- S *is a group of Lie type.*
- S *is one of 26 sporadic groups.*

Consider the symmetric group $G = \mathrm{Sym}(n)$, and a subgroup $H \leq G$. G consists of permutations of $I_n = \{1, \ldots, n\}$, so if $g \in G$ and $i \in I_n$ it makes sense to consider $g(i) \in I_n$. Given $i \in I_n$ consider

$$O_H(i) := \{h(i) \ : \ h \in H\} \qquad \text{(The } H\text{-}\textbf{orbit} \text{ of } i\text{).}$$

If H has exactly one orbit it is called **transitive** (e.g. $\langle(1234)\rangle < S_4$), otherwise it is called **intransitive** (e.g. $\langle(12),(34)\rangle < S_4$).

If H has exactly two orbits then H is said to be "**maximal intransitive**". If $A \cap B = \emptyset$, $\mathrm{Sym}(A) \times \mathrm{Sym}(B) < \mathrm{Sym}(A \cup B)$.

We can easily establish wheter an element of G lies in an intransitive subgroup. For example $(123)(45)(67) \in \mathrm{Sym}(7)$ lies in the (maximal) intransitive subgroup whose orbits are $\{1,2,3,4,5\}$ and $\{6,7\}$, and also in the (maximal) intransitive subgroup whose orbits are $\{1,2,3\}$ and $\{4,5,6,7\}$. (1234567) does not lie in intransitive subgroups.

The elements of $\mathrm{Sym}(n)$ which do not lie in intransitive subgroups are precisely the n-cycles.

Note that **a maximal intransitive subgroup is determined by the choice of its two orbits**.
Therefore, there are exactly $\binom{n}{k}$ maximal intransitive subgroups with orbits of sizes k, $n-k$.

Suppose $n > 1$ is odd. The total number of maximal intransitive subgroups of $\mathrm{Sym}(n)$ is

$$\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{(n-1)/2} = 2^{n-1} - 1.$$

Since any n-cycle belongs to $\mathrm{Alt}(n)$ (n being odd), $\mathrm{Sym}(n)$ can be covered by 2^{n-1} proper subgroups. It turns out that it actually cannot be covered with less if $n \neq 9$. The case $n = 9$ is not known.

We express this by saying that if $n > 1$ is odd and $n \neq 9$ then the **covering number** of $\mathrm{Sym}(n)$ is 2^{n-1}: $\sigma(\mathrm{Sym}(n)) = 2^{n-1}$.

PROPOSITION

Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree $n > 1$. Suppose that $f(X)$ admits a root modulo every prime. Then $f(X)$ is reducible.

PROOF.

There is a correspondence between factorization patterns modulo unramified primes and cycle structures of elements of the Galois group of $f(X)$ viewed as a transitive subgroup of S_n.

If $f(X)$ admits a root modulo every prime then every $\sigma \in G_f \leq S_n$ has at least a fixed point in $\{1, \dots, n\}$. Since G_f is transitive, the point stabilizers are pairwise conjugated.

But **a finite group is never equal to the union of one single conjugacy class of subgroups**. $\square$

REMARK

No group is union of two proper subgroups.

THEOREM (SCORZA 1926)

A group G is union of three proper subgroups if and only if it there exists $N \trianglelefteq G$ such that $G/N \cong C_2 \times C_2$.

Remark

No group is union of two proper subgroups.

Theorem (Scorza 1926)

A group G is union of three proper subgroups if and only if it there exists $N \trianglelefteq G$ such that $G/N \cong C_2 \times C_2$.

These considerations led Cohn in 1994 to define for every group G:

$\sigma(G)$ Covering number of G: the smallest cardinality of a covering of G, i.e. family of proper subgroups of G whose union equals G.

If G is cyclic we pose $\sigma(G) = \infty$.

Remark

No group is union of two proper subgroups.

Theorem (Scorza 1926)

A group G is union of three proper subgroups if and only if it there exists $N \trianglelefteq G$ such that $G/N \cong C_2 \times C_2$.

These considerations led Cohn in 1994 to define for every group G:

$\sigma(G)$ Covering number of G: the smallest cardinality of a covering of G, i.e. family of proper subgroups of G whose union equals G.

If G is cyclic we pose $\sigma(G) = \infty$.

Theorem (Neumann 1954)

*If G is an **infinite** group with finite covering number then there exists $N \trianglelefteq G$ such that G/N is finite and $\sigma(G) = \sigma(G/N)$.*

Cyclic groups do not admit coverings!

Proposition

A group G is cyclic if and only if G is not the union of its proper subgroups.

Proof.

Suppose G is cyclic generated by $g \in G$. Then

$$g \notin \bigcup_{H<G} H \qquad \Rightarrow \qquad \bigcup_{H<G} H \neq G.$$

Conversely, if G is not cyclic then

$$G = \bigcup_{g \in G} \langle g \rangle \subseteq \bigcup_{H<G} H \qquad \Rightarrow \qquad \bigcup_{H<G} H = G.$$

$\square$

A couple of easy remarks:

- If $\mathcal{H}$ is a covering of G then $\sigma(G) \leq |\mathcal{H}|$.
- If G is any non-cyclic group then $\sigma(G) < |G|$. Indeed, G is always covered by its non-trivial cyclic subgroups.
- If $N \trianglelefteq G$ and $\mathcal{H}$ is a covering of G/N then letting $\pi : G \to G/N$ be the canonical projection, the family

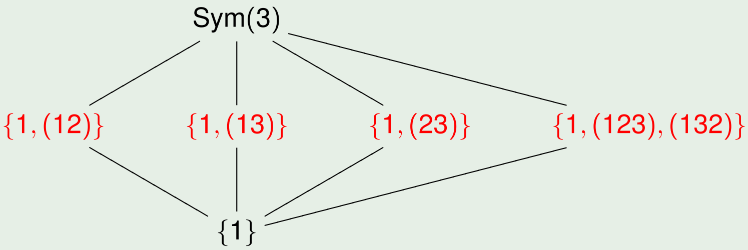
$$\{\pi^{-1}(H) \ : \ H \in \mathcal{H}\}$$

is a covering of G of size $|\mathcal{H}|$. It follows that $\sigma(G) \leq \sigma(G/N)$.
- Let $\Phi(G)$, **the Frattini subgroup of** G, be **the intersection of the maximal subgroups of** G. Then $\Phi(G) \trianglelefteq G$ and

$$\sigma(G) = \sigma(G/\Phi(G)).$$

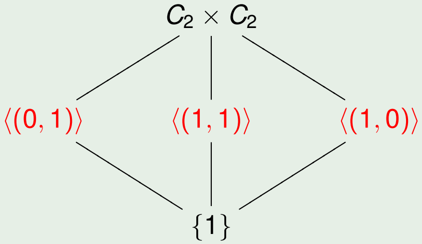
The symmetric group of degree 3

$\mathrm{Sym}(3) = \{1, (12), (13), (23), (123), (132)\}$. $\sigma(\mathrm{Sym}(3)) = 4$.
Subgroup lattice:



The Klein 4 group

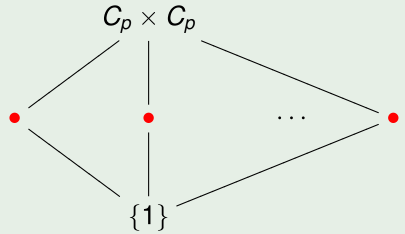
$C_2 \times C_2 = \{(a,b) \ : \ a,b \in C_2\}$. $\sigma(C_2 \times C_2) = 3$. Subgroup lattice:



Let us consider a very important **abelian** non-cyclic type of group.

The non-cyclic group of order p^2

Let p be a prime. $\sigma(C_p \times C_p) = p + 1$. Subgroup lattice:



Consider the following matrices of $GL(2,\mathbb{C})$.

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

The group they generate is **finite**. It has eight elements. It is called the quaternion group of order 8.

$$Q_8 = \langle 1, I, J, K \rangle = \{1, -1, I, -I, J, -J, K, -K\}.$$

We have the following relations:

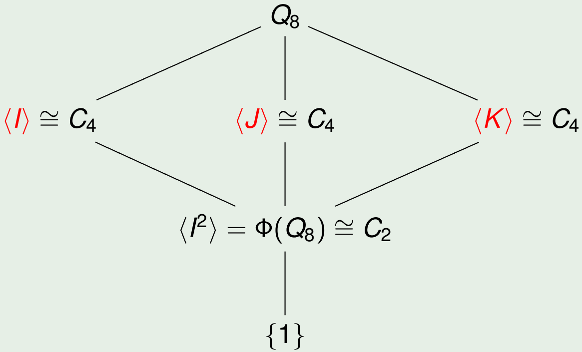
$$IJ = K = -JI, \qquad I^2 = J^2 = K^2 = -1.$$

The group Q_8 is an example of a finite **non-abelian group all of whose subgroups are normal** (Hamiltonian group).
Hamilton (1805 - 1865) was the discoverer of quaternions.

Hamiltonian groups have been classified. The finite Hamiltonian groups are precisely the groups of the form $Q_8 \times {C_2}^k \times A$ with $k \geq 0$ an integer and A an abelian group of odd order.

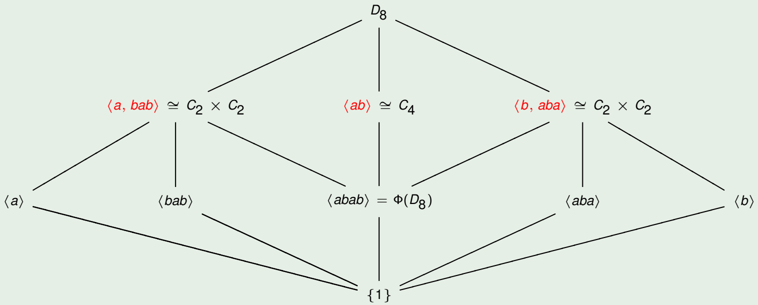
The Quaternion group of order 8

$Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ with $IJ = K = -JI$, $I^2 = J^2 = K^2 = -1$.
$|Q_8| = 8$. $\sigma(Q_8) = 3$. Subgroup lattice:



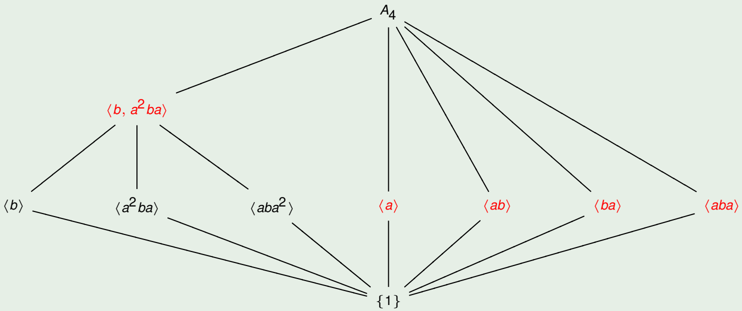
The dihedral group of order 8

$D_8 = \langle a, b \mid a^2 = b^2 = 1,\ (ab)^4 = 1 \rangle$. $\sigma(D_8) = 3$. Subgroup lattice:



The alternating group of degree 4

$A_4 = \langle a, b \rangle$ where $a = (123)$ and $b = (12)(34)$. $|A_4| = 4!/2 = 12$.
$\sigma(A_4) = 5$. Subgroup lattice:



$A_4 = \{1, (12)(34), (13)(24), (14)(23), (123), (132),$
$(124), (142), (234), (243), (134), (143)\}$.

Let us prove a very easy lower bound.

Proposition (The Minimal Index Lower Bound)

Let G be a non-cyclic group, and write $G = H_1 \cup \cdots \cup H_n$ as union of $n = \sigma(G)$ proper subgroups. Let $\beta_i := |G : H_i| := |G|/|H_i|$ for $i = 1, \dots, n$. Then $\min\{\beta_1, \dots, \beta_n\} < \sigma(G)$.

Proof.

We may assume that $\beta_1 \leq \cdots \leq \beta_n$. Since $1 \in H_1 \cap \ldots \cap H_n$ the union $H_1 \cup \ldots \cup H_n$ is not disjoint and hence

$$|G| < \sum_{i=1}^{n} |H_i| = |G| \sum_{i=1}^{n} \frac{1}{\beta_i} \leq \frac{|G|n}{\beta_1}.$$

Therefore $\beta_1 < n$. $\square$

p-groups

Consider the group $G = {C_p}^n = C_p \times \cdots \times C_p$ ($n \geq 2$ times), where p is a prime. $|G| = p^n$.

- G projects onto $C_p \times C_p$, so $\sigma(G) \leq \sigma(C_p \times C_p) = p + 1$.
- By the minimal index lower bound, $p < \sigma(G)$.

It follows that $\sigma(G) = p + 1$.

Let $d(G)$ denote the smallest number of generators of the group G. If G is any finite p-group then

$$\sigma(G) = \sigma(G/\Phi(G)) = ({C_p}^{d(G)}) = p + 1$$

as long as G is non-cyclic, i.e. $d(G) > 1$.

Nilpotent groups (direct products of finitely many groups of prime-power order).

Proposition

If A and B are two finite groups of coprime order then

$$\sigma(A \times B) = \min\{\sigma(A), \sigma(B)\}.$$

It follows that if G is a nilpotent group $P_1 \times \cdots \times P_t$, where $P_1, \ldots, P_t$ are finite groups of prime-power pairwise coprime order, then

$$\sigma(G) = \min\{\sigma(P_1), \ldots, \sigma(P_t)\}.$$

We can re-state this as follows:

Proposition

Let G be a finite nilpotent group.
Then $\sigma(G) = p + 1$ where p is the smallest prime divisor of G such that the Sylow p-subgroup of G is non-cyclic.

A "**chief factor**" of a group G is a minimal normal subgroup of a quotient of G.

If $K \trianglelefteq G$ and H/K is a chief factor of G, a complement of the chief factor H/K is a subgroup M/K of G/K such that $(M/K) \cap (H/K) = K/K$ and $(M/K)(H/K) = G/K$.

Solvable groups were considered by Tomkinson in 1994.

Theorem (Tomkinson, [4])

Let G be a finite solvable group. Then

$$\sigma(G) = |H/K| + 1$$

where H/K is the smallest chief factor of G with more than one complement in G/K.

In particular, if G is solvable then $\sigma(G) - 1$ is always a prime power. This is false for non-solvable groups, for example $\sigma(S_6) - 1 = 12$.

Lemma (Intersection argument)

Let K be a maximal subgroup of a group G and let $\mathcal{H}$ be a minimal cover of G consisting of maximal subgroups.
If $\sigma(G) < \sigma(K)$ then $K \in \mathcal{H}$.
Equivalently, if $K \notin \mathcal{H}$ then $\sigma(K) \leq \sigma(G)$.

$\sigma(\mathrm{Sym}(6)) = 13$

For example let $G = \mathrm{Sym}(6)$, K a subgroup of G isomorphic to $\mathrm{Sym}(5)$. Since $\sigma(\mathrm{Sym}(5)) = 2^{5-1} = 16$ and G can be covered with 13 subgroups (Alt(6) together with the twelve subgroups isomorphic to Sym(5)) we have $\sigma(G) \leq 13 < 16 = \sigma(\mathrm{Sym}(5)) = \sigma(K)$.

Applying the lemma we find that $\mathcal{H}$ contains the twelve subgroups of G isomorphic to Sym(5). Since they are not enough to cover G and $\sigma(G) \leq 13$, we find $\sigma(G) = 13$.

- If $A, B \leq G$ let $AB := \{ab \ : \ a \in A, \ b \in B\}$.
- Let $N \trianglelefteq G$. A **complement** of N in G is $H \leq G$ such that

$$NH = G \qquad \text{and} \qquad N \cap H = \{1\}.$$

- If H complements N in G then $G/N \cong H$.

Example

Any two 1-dimensional vector subspaces of $\mathbb{R}^2$ complement each other as additive groups.

Example

Consider the group G of isometries of the plane $\mathbb{R}^2$. We certainly have the subgroup T of translations and the subgroup O of linear isometries. T is a normal subgroup of G complemented by O.

Proposition (Maximal Complement Argument)

If a maximal subgroup M of G complements a non-solvable normal subgroup N of G then $\sigma(G) = \sigma(G/N)$.

Proposition

Let G be a group. Then G is simple if and only if

$$\Delta_G := \{(g, g) \mid g \in G\}$$

is a maximal subgroup of $G \times G$.

$\sigma(S \times S) = \sigma(S)$

Let S be a non-abelian simple group. Note that $S \times \{1\}$ is a non-solvable normal subgroup of $S \times S$ and that Δ_S is a complement of $S \times \{1\}$. It follows from the Maximal Complement Argument that

$$\sigma(S \times S) = \sigma(S).$$

One of the main results in my thesis is the following.

Theorem (Lucchini A., G 2010 [5])

Let $\mathcal{M}$ be a minimal cover of a direct product $G = H_1 \times H_2$ of two finite groups. Then one of the following holds:

1. $\mathcal{M} = \{X \times H_2 \mid X \in \mathcal{X}\}$ *where* $\mathcal{X}$ *is a minimal cover of* H_1. *In this case* $\sigma(G) = \sigma(H_1)$.
2. $\mathcal{M} = \{H_1 \times X \mid X \in \mathcal{X}\}$ *where* $\mathcal{X}$ *is a minimal cover of* H_2. *In this case* $\sigma(G) = \sigma(H_2)$.
3. *There exist* $N_1 \trianglelefteq H_1$, $N_2 \trianglelefteq H_2$ *with* $H_1/N_1 \cong H_2/N_2 \cong C_p$ *and* $\mathcal{M}$ *consists of the maximal subgroups of* $H_1 \times H_2$ *containing* $N_1 \times N_2$. *In this case* $\sigma(G) = p + 1$.

Suppose we want to compute $\sigma(G)$. If $N \trianglelefteq G$ is such that $\sigma(G) = \sigma(G/N)$ then we are reduced to compute $\sigma(G/N)$.

Definition (σ-elementary groups)

A non-cyclic group G is said to be σ-elementary if $\sigma(G) < \sigma(G/N)$ whenever $\{1\} \neq N \trianglelefteq G$.

It is easy to prove that:

Proposition

Let G be a finite non-cyclic group. Then there exists $N \trianglelefteq G$ such that:

- $\sigma(G) = \sigma(G/N)$;
- *G/N is σ-elementary.*

Examples

- Non-abelian simple groups are σ-elementary.
- If p is a prime, $C_p \times C_p$ is σ-elementary.
- The dihedral group D_{2p} of order $2p$ is σ-elementary.
- If S is a non-abelian simple group and $n \geq 1$ is an integer such that S^n is σ-elementary then $n = 1$. Indeed, $\sigma(S^n) = \sigma(S)$.
- If $n \geq 3$ is an integer and $n \neq 4$ then S_n is σ-elementary: its only proper quotient is C_2. S_4 is not σ-elementary: it admits S_3 as homomorphic image (quotient) and $\sigma(S_4) = \sigma(S_3) = 4$.
- If G/N is cyclic whenever $\{1\} \neq N \trianglelefteq G$ then G is σ-elementary. The converse is true for solvable groups but false in general. An example is $I \rtimes A_p$ where $I = \{(x_1, \ldots, x_p) \in \mathbb{F}_2^p : \ \sum_{i=1}^p x_i = 0\}$ and p is a prime not of the form $\frac{q^n-1}{q-1}$ with q a prime power.

Proposition

Let G be a σ-elementary group.

- *Since $\sigma(G) = \sigma(G/\Phi(G))$, $\Phi(G) = \{1\}$.*
- *If G is non-abelian then it has trivial center: $Z(G) = \{1\}$.*
- *If G is abelian then $G \cong C_p \times C_p$ for some prime p.*
- *Scorza's theorem: if $\sigma(G) = 3$ then $G \cong C_2 \times C_2$.*
- *Scorza's theorem revisited: if $\sigma(G) = p + 1$ with p the smallest prime divisor of $|G|$ then $G \cong C_p \times C_p$.*
- *Let n be a positive integer. There are only finitely many σ-elementary groups G with $\sigma(G) = n$.*
- *If $H_1 \times H_2$, a direct product of two non-trivial groups, is σ-elementary then $H_1 \cong H_2 \cong C_p$ for some prime p.*
- *If G is σ-elementary, $\{1\} \neq N \trianglelefteq G$ and G/N is solvable then G/N is cyclic. In particular G/G' is cyclic.*

Theorem (G 2009)

All σ-elementary groups G with $\sigma(G) \leq 25$ are known.

3	$C_2 \times C_2$
4	$C_3 \times C_3, \mathrm{Sym}(3)$
5	$\mathrm{Alt}(4)$
6	$C_5 \times C_5, D_{10}, AGL(1,5)$
7	$\emptyset$
8	$C_7 \times C_7, D_{14}, 7:3, AGL(1,7)$
9	$AGL(1,8)$
10	$3^2:4, AGL(1,9), \mathrm{Alt}(5)$
11	$\emptyset$
12	$C_{11} \times C_{11}, 11:5, D_{22}, AGL(1,11)$
13	$\mathrm{Sym}(6)$
14	$C_{13} \times C_{13}, D_{26}, 13:3, 13:4, 13:6, AGL(1,13)$
15	$SL(3,2)$
16	$\mathrm{Sym}(5), \mathrm{Alt}(6)$
17	$2^4:5, AGL(1,16)$
18	$C_{17} \times C_{17}, D_{34}, 17:4, 17:8, AGL(1,17)$
19	$\emptyset$
20	$C_{19} \times C_{19}, AGL(1,19), D_{38}, 19:3, 19:6, 19:9$
21	$\emptyset$
22	$\emptyset$
23	M_{11}
24	$C_{23} \times C_{23}, D_{46}, 23:11, AGL(1,23)$
25	$\emptyset$

Definition (Minimal normal subgroups)

A minimal normal subgroup of a group G is a non-trivial normal subgroup N of G which does not contain any non-trivial normal subgroup of G different from N.

Examples

- If p is a prime, $C_p \times C_p$ has $p+1$ minimal normal subgroups.
- If S is a simple group, it is its unique minimal normal subgroup.
- If $n \geq 3$ is an integer and $n \neq 4$ then the unique minimal normal subgroup of S_n is A_n.
- The unique minimal normal subgroup of S_4 is $V = \{1, (12)(34), (13)(24), (14)(23)\}$.
- If $k \geq 1$ is an integer and S is a non-abelian simple group then the minimal normal subgroups of $S \times \cdots \times S = S^k$ are its k direct factors, $S \times \{1\} \times \cdots \times \{1\}, \ldots, \{1\} \times \cdots \times \{1\} \times S$.
- If F is a field with at least 4 elements and $n \geq 2$, the unique minimal normal subgroup of $PGL(n, F)$ is $PSL(n, F)$.

Given a finite group G denote by $mn(G)$ the **number of minimal normal subgroups** of G.

The main problem I dealt with in my Ph.D thesis is the following.

Conjecture (A. Lucchini, E. Detomi)

Let G be a non-abelian σ-elementary group. Then $mn(G) = 1$.

If $mn(G) = 1$ we usually say that G is monolithic.

Here is what I can say when the covering number is “small”.

Theorem

Let G be a non-abelian σ-elementary group such that $\sigma(G) \leq 56$. Then G is monolithic. Moreover, its minimal normal subgroup is either simple or abelian.

$\sigma(A_5 \wr C_2) = 57$, $A_5 \wr C_2$ is monolithic and its minimal normal subgroup is $A_5 \times A_5$, not simple and not abelian.

Here is what I can say when I “block” pieces of the group.

Theorem

Let H be a non-abelian σ-elementary group, and suppose that whenever S is a non-abelian simple subgroup of H and there exists a chain

$$\{1\} \lhd S \lhd H_2 \lhd \cdots \lhd H_n = H,$$

S is isomorphic to an alternating group $Alt(n)$ with n large enough and even. Then H is monolithic.

R.A. Bryce, V. Fedri, L. Serena, Subgroup coverings of some linear groups; Bull. Austral. Math. Soc., 60(1999), 227–238.

D. Berend, Y. Bilu, Polynomials with roots modulo every integer; Proc. Amer. Math. Soc. 124 (1996), no. 6, 1663Ű1671.

J. H. E. Cohn, On n-sum groups; Math. Scand. 75 (1) (1994) 44–58.

B. H. Neumann, Groups covered by permutable subsets; J. London Math. Soc. 29, 236-248 (1954).

E. Detomi and A. Lucchini, On the structure of primitive n-sum groups; Cubo 10 (2008), no. 3, 195–210.

M. J. Tomkinson, Groups as the union of proper subgroups; Math. Scand. 81 (2) (1997) 191–198.

L. C. Kappe, J. L. Redden, On the Covering Number of Small Alternating Groups; Contemp. Math., 511, Amer. Math. Soc., Providence, RI, 2010.

M. Garonzi, A. Lucchini, Direct products of groups as unions of proper subgroups; Archiv der Mathematik, ISSN: 0003-889X

M. Garonzi, Finite Groups that are Union of at most 25 Proper Subgroups; Journal of Algebra and its Applications, ISSN: 0219-4988.

M. S. Lucido, On the covers of finite groups; Groups St. Andrews 2001 in Oxford. Vol. II, 395Ű399, London Math. Soc. Lecture Note Ser., 305, Cambridge Univ. Press, Cambridge, 2003.

A. Maróti, M. Garonzi, Covering certain wreath products with proper subgroups; Journal of Group Theory, ISSN: 1433-5883.

A. Maróti, Covering the symmetric groups with proper subgroups; J. Combin. Theory Ser. A, 110(1) (2005), 97–111.

M. Garonzi, Covering certain monolithic groups with proper subgroups; Communications in Algebra, ISSN: 0092-7872.

A. Abdollahi, F. Ashraf, S. M. Shaker, The symmetric group of degree six can be covered by 13 and no fewer proper subgroups; Bull. Malays. Math. Sci. Soc. (2) 30 (2007), no. 1, 57–58.