IDEAS IN FINITE GROUP THEORY

MARTINO GARONZI

Abstract. In this note I present some of the main ideas of finite group theory, starting with examples of non-abelian groups (groups of matrices and groups of permutations), going to Galois theory, i.e. the way polynomials and groups interact, and finally simple groups, solvable groups and their role in understanding when the roots of a polynomial can be expressed by starting with the coefficients and performing sums, differences, products, divisions and root extractions. After that I will present my research topic with examples and some results.

When dealing with operations there are two possible notations, the additive notation and the multiplicative notation. In the additive notation the operation between two group elements a, b is denoted $a+b$ and the identity element is denoted 0. In the multiplicative notation the operation between two group elements a, b is denoted $a \cdot b$ or simply ab and the identity element is denoted 1. Usually the additive notation is reserved for the abelian case. I will mostly use the multiplicative notation. I will assume the reader to be familiar with the basic properties of groups and fields. The notation $H \leq G$ means that H is a subgroup of G, and the notation $H \trianglelefteq G$ means that H is a normal subgroup of G.

The given bibliography provides good reference books for the theory of (finite) groups.

I will start by recalling the isomorphism theorem.

Theorem 1 (Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism and let $N := \ker(\varphi)$ be the kernel of φ, i.e. the set of elements $g \in G$ such that $\varphi(g) = 1$. Then $G/N \cong \varphi(G)$ via the canonical isomorphism $gN \mapsto \varphi(g)$.*

1. Some examples of groups

Usually abelian groups (commutative groups), i.e. groups in which any two elements a, b verify $ab = ba$ ("commute"), are familiar to every mathematician. Let us start with some examples of non-abelian groups.

1.1. **Matrices.** Invertible matrices form a group. Let F be any field (for example $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$). I denote by $GL(n, F)$ 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 group, which is non-abelian if $n \geq 2$. It is usually called the "General Linear Group". It is non-abelian because, as it is well-known, the row-column multiplication is not a commutative operation. The set $F - \{0\} = F^*$ is a group with respect to multiplication, and it is abelian, isomorphic to $GL(1, F)$. Taking the determinant provides a (surjective!) group homomorphism

$$GL(n, F) \to F^*, \qquad A \mapsto \det(A)$$

(indeed $\det(AB) = \det(A)\det(B)$ by Binet's theorem) whose kernel, $SL(n,F) := \{A \in GL(n,F) \ : \ \det(A) = 1\}$, is called the "Special Linear Group". It is a normal subgroup of $GL(n,F)$ (being the kernel of a homomorphism) and using the isomorphism theorem we see that the quotient $GL(n,F)/SL(n,F)$ is isomorphic to F^*.

1.2. **Permutations.** I will denote by $\mathrm{Sym}(X)$ the set of bijections $X \to X$ (also called the permutations of X). The operation of usual composition of functions gives $\mathrm{Sym}(X)$ the structure of group. It is called the "Symmetric Group" of X. It is an easy exercise to show that if X, Y are equipotent sets then $\mathrm{Sym}(X)$ and $\mathrm{Sym}(Y)$ are isomorphic groups. If $X = \{1, \dots, n\}$ I shall denote $\mathrm{Sym}(X)$ by $\mathrm{Sym}(n)$ or S_n. It is called the symmetric group of degree n. This group is non-abelian if and only if $n \geq 3$. 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 $n! = 1 \cdot 2 \cdots n$. I will use the standard cycle notation, which is best explained by means of examples:

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

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

Composition goes as follows:

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

Note that disjoint cycles always commute. The following calculation shows that $\mathrm{Sym}(n)$ is non-abelian for $n \geq 3$:

$$(12)(123) = (13), \qquad (123)(12) = (23).$$

Remark 1. *Every permutation can be written uniquely (up to reordering) as* ***product of disjoint cycles****.*

2-cycles are also called "transpositions". A permutation is called "even" (or "of sign 1") if it can be written as the product of an even number of transpositions, and "odd" (or "of sign -1") otherwise. For example $(12)(25)(13)(35)$ is even, $(13)(26)(43)$ is odd. The identity of $\mathrm{Sym}(n)$ (the identity function $\{1, \dots, n\} \to \{1, \dots, n\}$) is considered to be the product of zero transpositions, hence an even permutation.

Remark 2. *A product of disjoint cycles is an even permutation if and only if the number of cycles of even length is even.*

For example $(123)(4567)$, $(12)(3456)(78)$ are odd, $(123)(45)(67)$, $(123)(4567)(89)$ are even.

Definition 1. *The "cycle structure" of a permutation is the increasing sequence of the cycle lengths in the representation as a product of disjoint cycles. Cycles of length* 1 *are usually omitted.*

So for example $(123)(4567)$, $(12)(3456)(78)$, $(123)(45)(67)$, $(123)(4567)(89)$ have cycle structure respectively $(3,4)$, $(2,2,4)$, $(2,2,3)$, $(2,3,4)$. Remark 2 implies that the cycle structure of a permutation determines its sign. Hence all elements of cycle structure $(3,4)$, $(2,2,4)$ are odd, and all elements of cycle structure $(2,2,3)$, $(2,3,4)$ are even.

Let us denote by C_2 the set $\{-1, 1\}$ with the operation given by multiplication: $1 \cdot 1 = (-1) \cdot (-1) = 1$ and $1 \cdot (-1) = (-1) \cdot 1 = -1$. Then C_2 is a commutative

group, it is a cyclic group (a group generated by one element) of order 2 (generated by -1), and it is isomorphic to $\mathrm{Sym}(2) = \{1, (12)\}$. Consider the map

$$\mathrm{sgn} : \mathrm{Sym}(n) \to \{-1, 1\} = C_2, \qquad \sigma \mapsto \mathrm{sgn}(\sigma)$$

which sends any permutation to its sign (1 if it is even, -1 if it is odd). Then sgn is a (surjective!) group homomorphism whose kernel, $\mathrm{Alt}(n) = A_n := \{\sigma \in \mathrm{Sym}(n) : \mathrm{sgn}(\sigma) = 1\}$ is called the "Alternating Group" of degree n. It is a normal subgroup of $\mathrm{Sym}(n)$ (being the kernel of a homomorphism) and using the isomorphism theorem we see that the quotient $\mathrm{Sym}(n)/\mathrm{Alt}(n)$ is isomorphic to C_2, in particular $|\mathrm{Alt}(n)| = n!/2$.

For example $\mathrm{Alt}(4) = \{1, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (234), (243), (134), (143)\}$.

2. Galois Theory

2.1. **The Galois group of a polynomial.** Let us talk about the reason why groups were invented.

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 the group defined as follows: if $a_1, \ldots, a_n \in \mathbb{C}$ denote the distinct roots of $f(X)$ then

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

where $\mathbb{Q}(a_1, \ldots, a_n)$ denotes the field generated by $a_1, \ldots, a_n$, i.e. the intersection of the subfields of $\mathbb{C}$ containing $a_1, \ldots, a_n$. That is, G_f is the group of field isomorphisms

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

that is, the group of such maps which are bijective and respect identity elements, sums, and products. It goes without saying that the operation in G_f is again the usual composition of functions. Suppose that a is a root of $f(X) \in \mathbb{Q}[X]$ (i.e. $f(a) = 0$) and $g \in G_f$. We can consider the element $g(a) \in \mathbb{C}$. Since g is a ring homomorphism, it fixes every element of $\mathbb{Q}$ (this is easy to show starting from the identity $g(n) = g(1 + \cdots + 1) = g(1) + \cdots + g(1) = 1 + \cdots + 1 = n$ for $n \in \mathbb{N}$) and also $g(a)$ is a root of f, indeed writing $f(X) = \sum_i c_i X^i$ with c_i elements of $\mathbb{Q}$ we have

$$\begin{aligned} f(g(a)) &= \sum_i c_i g(a)^i = \sum_i g(c_i) g(a^i) = \sum_i g(c_i a^i) = \\ &= g(\sum_i c_i a^i) = g(f(a)) = g(0) = 0. \end{aligned}$$

This implies that the group G_f **permutes the roots of** f. In other words, G_f can be described (or better, "represented") as a subgroup of $\mathrm{Sym}(n)$. Indeed, the function

$$G_f \to \mathrm{Sym}(\{a_1, \ldots, a_n\})$$

which sends $g \in G_f$ to the permutation given by $a_i \mapsto g(a_i)$ (which, as we saw above, is well-defined) is an injective (!) group homomorphism. Injectivity follows from the fact that the only element of G_f which fixes all the roots is the identity.

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 (unique!) field homomorphism $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ which sends $\sqrt{2}$ to $-\sqrt{2}$. The Galois group of X^2-2 is cyclic of order 2. $G_f \cong \mathrm{Sym}(2) \cong C_2$.

2.2. **Factorizations modulo prime numbers.** I now want to show how polynomials and groups interact. The usual "reduction modulo n" that we have for integers can be performed also in polynomial rings. It is an interesting fact that a polynomial might be irreducible over $\mathbb{Z}$ but reducible modulo some prime p. For example X^2-2 is irreducible over $\mathbb{Z}$ (its roots are not integers) but

$$X^2-2 \equiv X^2 \mod 2, \qquad X^2-2 \equiv (X-3)(X-4) \mod 7.$$

Still there are some primes for which the given polynomial might remain irreducible, for example X^2-2 is irreducible modulo 3.

For the following theorem see [7], Lemmas 1 and 2.

Theorem 2 (Frobenius-Dedekind)**.** *Let $f(X)$ be an irreducible polynomial of $\mathbb{Z}[X]$ of degree n. The following assertions are equivalent.*

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

This implies, for example, that an irreducible polynomial of degree n remains irreducible modulo some prime if and only if its Galois group, viewed as a subgroup of $\mathrm{Sym}(n)$, contains an n-cycle. Moreover, since every group contains the identity element, which has cycle structure $(1, \dots, 1)$, we deduce that given an irreducible polynomial there always exist primes p such that $P(X)$ splits into distinct linear factors modulo p (!). Such primes are infinitely many by Chebotarev's density theorem (cf. below).

There is a notion of "discriminant" valid for every polynomial. It is defined as $\prod_{i,j}^{n}(a_i - a_j)$ where $a_1, \dots, a_n$ are the roots of the polynomial. It is possible to show that the discriminant of a polynomial with integer coefficients is an integer. For small degrees it is reasonable to find a formula for the discriminant. For example,

- the discriminant of aX^2+bX+c is b^2-4ac,
- the discriminant of X^3+pX+q is $-4p^3-27q^2$.

A very useful property of the discriminant (which follows directly from its definition) is the following: given a polynomial $P(X)$, a prime number is ramified (i.e. $P(X)$ has multiple roots modulo that prime) if and only if it divides the discriminant of $P(X)$. In particular, there are only finitely many ramified primes.

In the case of cubics (polynomials of degree 3) the discriminant determines the Galois group: it is possible to show that an irreducible polynomial of degree 3 over $\mathbb{Q}$ has Galois group Sym(3) if its discriminant is a square in $\mathbb{Q}$, it has Galois group Alt(3) otherwise.

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 $81 = 3^4$).

The following tables contain the reductions of these polynomials modulo various prime numbers.

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

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	$(X+53)(X+87)(X+114)$

Note that the factorization pattern $(1,2)$ shows up in the first table but does not in the second. This is explained by Frobenius theorem: Sym(3) (the Galois group of $X^3 + X^2 + X + 3$) contains permutations of cycle structure $(1,2)$ (2-cycles) but Alt(3) (the Galois group of $X^3 - 3X + 1$) does not! Indeed

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

Moreover, by a result known as "Chebotarev density theorem", the proportion of primes yielding a given factorization pattern equals the proportion of elements of the Galois group with the associated cycle structure. This is why, for example, the proportion of primes for which the second polynomial remains irreducible is about $2:1$: because in Alt(3) there are twice more 3-cycles than $(1,1,1)$-cycles.

2.3. **The Inverse Galois Problem.** The most famous open problem in group theory is probably the 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, cf. below for the definition), but the answer in general is not known.

3. Cauchy, Lagrange, Sylow, Cayley

Let us list the important results of "elementary" finite group theory. Given a subset X of a group G I will denote by $\langle X \rangle$ the **subgroup generated** by X in G, i.e. the intersection of the subgroups of G containing X. I will rather write $\langle x_1, \dots, x_n \rangle$ instead of $\langle \{x_1, \dots, x_n\} \rangle$.

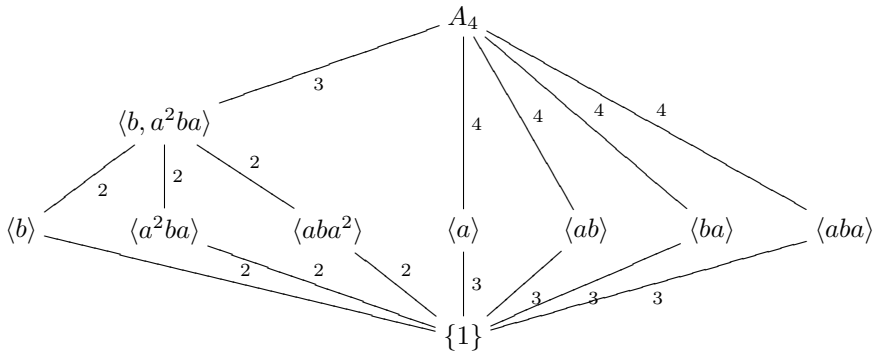
- the **"order" of an element** $g \in G$, denoted $o(g)$, is the smallest positive integer n such that the product of g with itself n times, $g^n = g \cdots g$ (n times), equals 1;
- the **"order" of a subgroup** $H \leq G$, denoted $|H|$, is its size.
- It turns out that $|\langle g \rangle| = o(g)$.

Theorem 3 (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 $|G|$ necessarily equals the size of a subgroup of G (cf. the example below), but...

Theorem 4 (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.*

Consider the following example: the alternating group of degree 4. $A_4 = \langle a, b \rangle$ where $a = (123)$ and $b = (12)(34)$. $|A_4| = 4!/2 = 12 = 2^2 \cdot 3$. Here is its subgroup lattice (the labelling numbers denote the indeces):



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

Note that although 6 divides 12, A_4 **has no subgroups of order** 6.

Although it is not true that there exist subgroups of G of order any given divisor of $|G|$, Cauchy's theorem implies that they exist if the given divisor is a prime. The next natural step is to ask what happens with prime-powers. Suppose $|G|$

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

Theorem 5 (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 $H \leq P$.*

Consider the following 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.

Finally, Cayley theorem says that every finite group can be found inside some symmetric group.

Theorem 6 (Cayley (1821 - 1895))**.** *Let G be a group. Then the map*

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

is an injective homomorphism.

In particular, G is isomorphic with a subgroup of $Sym(G)$.

Corollary 1. *Let G be a finite group. There exists a positive integer n such that G is isomorphic with a subgroup of $Sym(n)$.*

Cayley's theorem says that we may choose $n = |G|$. But sometimes we can choose a smaller n (cf. [8]).

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 $G_f \to \mathrm{Sym}(n)$.

4. Simple groups, solvable groups

A group G is said to be "simple" if the only normal subgroups of G are $\{1\}$ and G. Since every subgroup of an abelian group is normal, it is easy to show that

Remark 3 (Abelian simple groups)**.** *Abelian simple groups are the cyclic groups of prime order,*

$$C_p = \{g, g^2, \ldots, g^{p-1}, g^p = 1\} \cong (\mathbb{Z}/p\mathbb{Z}, +) = \{1, 2, \ldots, p-1, p = 0\}.$$

The following results provide infinite families of non-abelian simple groups.

Theorem 7 (Alternating Groups)**.** *If $n \geq 5$ is an integer, Alt(n) is a non-abelian simple group.*

Theorem 8 (Projective Linear Groups)**.** *Let F be a field, and let $GL(n, F)$ be the group of invertible matrices over 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 a 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 9 (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).*

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

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

Definition 2 (Solvable groups)**.** *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**". Let us give some examples.

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:

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

Arrows are inclusions. $O_2(S_4)$ denotes the intersection of the Sylow 2-subgroups of S_4: it is a normal subgroup of S_4 of order 4 isomorphic to the Klein group $C_2 \times C_2$. The composition factors of S_4 are C_2 (three times) and C_3. $|S_4| = 24 = 2^3 \cdot 3$. More generally, all polynomials of degree 2, 3, 4 are solvable by radicals. Indeed, all subgroups of Sym(4) are solvable. On the other hand, 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.

Let a, b, c be indeterminates over $\mathbb{Q}$. The roots of the polynomial $P(X) = aX^2 + bX + c$ are given by the well-known formula

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

It follows that $P(X)$ is solvable by radicals over $\mathbb{Q}(a, b, c)$. I want to consider now degrees larger than 2.

For the following discussion we refer the reader to [1, Theorem 4.15]. Let $a_0, \ldots, a_{n-1}$ be indeterminates over $\mathbb{Q}$. It is interesting to ask when the generic polynomial of degree n

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

is solvable by radicals over the field generated by its coefficients, $\mathbb{Q}(a_0, \ldots, a_{n-1})$. In other words, we ask when the roots of $P(X)$ can be expressed by starting from the coefficients $a_0, \ldots, a_{n-1}$ and performing sums, differences, products, divisions and root extractions. It turns out that $P(X)$ is irreducible in $\mathbb{Q}(a_0, \ldots, a_{n-1})[X]$, it has distinct roots (as does any irreducible polynomial in characteristic zero) and its Galois group over $\mathbb{Q}(a_0, \ldots, a_{n-1})$ is $\mathrm{Sym}(n)$. Since, as we have seen, $\mathrm{Sym}(n)$ is not a solvable group if $n \geq 5$, it follows that $P(X)$ is solvable by radicals if and only if $n \leq 4$.

As you might have noticed, above I used the expression "over the field generated by its coefficients". Let us clarify this. If F/K (to be read "F over K") is any **field extension** (meaning that F and K are fields and F contains K) then the Galois group of F/K, denoted $\mathcal{G}(F/K)$, is defined to be the set of all field automorphisms g of F such that (*) $g(a) = a$ for every $a \in K$. Note that if $K = \mathbb{Q}$ then condition (*) is automathic. The inclusion $K \subseteq F$ gives F a canonical structure of K-vector space. The extension F/K is said to be "finite" if F has finite dimension as K-vector space. The "degree" of the finite field extension F/K, usually denoted $[F : K]$, is the dimension $\dim_K(F)$. So for example $\mathbb{C}/\mathbb{R}$ is a finite field extension of degree 2 with Galois group C_2 (its two elements are the identity and the *complex conjugation* $a + ib \mapsto a - ib$). A finite extension F/K is said to be a *Galois extension* if

$$\{a \in F \ : \ g(a) = a \ \forall g \in \mathcal{G}(F/K)\} = K.$$

It turns out that an extension F/K is a Galois extension if and only if $[F : K] = |\mathcal{G}(F/K)|$, that is, the degree equals the size of the Galois group. For example, whenever $f(X)$ is a polynomial in $\mathbb{Q}[X]$, with roots $a_1, \ldots, a_n \in \mathbb{C}$, the extension $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}$ is a Galois extension. For example consider $f(X) = X^2+1 \in \mathbb{R}[X]$: since $\mathbb{C} = \mathbb{R}(i) = \mathbb{R}(i, -i)$, the extension $\mathbb{C}/\mathbb{R}$ is Galois.

Here is an example of an extension that is **not Galois**: $F/K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Indeed, the only K-automorphism of F is the identity, $\mathrm{id}_F : F \to F$ ($\sqrt[3]{2}$ is the only root of $X^3 - 2$ that belongs to F !), so $|\mathcal{G}(F/K)| = 1$, while the degree $[F : K]$ is 3: a K-basis is given by 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$. However, F is contained in a Galois extension of K: $\mathbb{Q}(a, b, c)/\mathbb{Q}$, where a, b, c are the three roots of $X^3 - 2$ in $\mathbb{C}$. It is an extension of degree 6 with Galois group isomorphic to $\mathrm{Sym}(3)$.

Here comes the main property of Galois extensions, which makes them very nice. If F/K is a finite Galois extension then the correspondences

$$H \mapsto \{a \in F \ : \ h(a) = a \ \forall h \in H\}$$

$$L \mapsto \{g \in \mathcal{G}(F/K) \ : \ g(a) = a \ \forall a \in L\}$$

provide inclusion-reversing bijections, inverses of each other, between the family of subgroups of $\mathcal{G}(F/K)$ and the family of fields L such that $K \subseteq L \subseteq F$ (*intermediate fields* of F/K). So, if you want to see how the intermediate field lattice of a Galois extension looks like just take the subgroup lattice of its Galois group and turn it upside-down (remember that inclusions are reversed).

I now spend some words on the classification of the finite simple groups. The starting point for the classification was the following beautiful result, which is known as the "odd order theorem". The proof is very long. Recently (September 2012) it was checked by the computer program Coq, essentially proving algorithmically that the proof is correct. This was achieved by a team led by Georges Gonthier (cf. http://ssr2.msr-inria.inria.fr/ $\sim$ jenkins/current/progress.html).

Theorem 10 (Feit, Thompson, 1962-1963)**.** *Any finite group of odd order is solvable.*

It is easy to show that this is equivalent to say that every finite non-abelian simple group has even order (just look at a composition series). In particular, by Cauchy Theorem, any finite non-abelian simple group contains involutions (elements of order 2). Finite simple groups have been classified using the centralizers of the involutions. The centralizer of an element $x \in G$ is the set of elements which commute with x, $C_G(x) := \{g \in G \ : \ gx = xg\}$.

Proposition 1 ([2], (45.4))**.** *Let G be a finite simple group and let t be an involution in G, $n := |C_G(t)|$. Then $|G| \leq (2n^2)!$.*

An immediate corollary is:

Theorem 11 (Brauer-Fowler)**.** *Let H be a finite group. Then there exists at most a finite number of finite simple groups G with an involution t such that $C_G(t) \cong H$.*

This should clarify why the Feit-Thompson theorem is considered to be the starting point of the classification. The classification theorem is too long to be fully stated here, so I will give a short version of it. Groups of "Lie type" are particular groups of matrices over finite fields, as in the case of the projective special linear group $PSL(n, F)$.

Theorem 12 (Classification of the Finite Simple Groups)**.** *Let S be a finite 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.*

5. Some more beautiful results

The following result is one of the few results which guarantee the existence of subgroups of some order.

Theorem 13 (Schur-Zassenhaus)**.** *Let G be a finite group and let N be a normal subgroup of G. If $|N|$ and $|G:N|$ are coprime then G admits a subgroup of size $|G:N|$.*

The following result is a generalization of Sylow's Theorem in the case of solvable groups. If π is a set of prime numbers, a "Hall π-subgroup" of G is a subgroup H of G such that $|H|$ and $|G:H|$ are coprime and all prime divisors of $|H|$ belong to π.

Theorem 14 (Hall)**.** *Let G be a finite solvable group, and let π a set of prime numbers. Then G admits Hall π-subgroups, and any two Hall π-subgroups of G are conjugated.*

Classically this is proved using the Schur-Zassenhaus theorem.

6. Covering finite groups

Now I will say something about my own research. From now on all considered groups will be assumed to be finite.

6.1. **Sigma.** A "cover" of a group G is a family $\mathcal{H}$ of proper subgroups of G such that $\bigcup_{H\in\mathcal{H}} H = G$. It is easy to see that a group admits covers if and only if it is noncyclic. This follows from the equality $\bigcup_{g\in G}\langle g\rangle = G$ and the fact that a proper subgroup cannot contain the elements g such that $\langle g\rangle = G$.

Define $\sigma(G)$, the "**covering number**" of G, to be the smallest size of a cover of G. This notion was introduced in [9]. A cover of G of size $\sigma(G)$ will be called "minimal cover". If G is cyclic, set $\sigma(G) = \infty$ with the convention that $n < \infty$ for every integer n. It is obvious, but worth remarking, that if $\mathcal{H}$ is any cover of G then $\sigma(G) \leq |\mathcal{H}|$. The following basic result shows that if $N \trianglelefteq G$ then

$$\sigma(G) \leq \sigma(G/N).$$

Theorem 15 (Correspondence theorem)**.** *Let G be a group and let $N \trianglelefteq G$. The correspondences*

$$\varphi : H/N \mapsto \{g \in G \ : \ gN \in H/N\}, \qquad \psi : K \mapsto KN/N$$

provide canonical bijections, inverses of each other, between the family of subgroups of G/N and the family of subgroups of G containing N. Moreover, they both send normal subgroups to normal subgroups.

Indeed, if $\mathcal{H}$ is a cover of G/N then $\{\varphi(H) \ : \ H \in \mathcal{H}\}$ is a cover of G of size $|\mathcal{H}|$.

For example, if $n \neq 9$ is an odd integer larger than 1 then $\sigma(\mathrm{Sym}(n)) = 2^{n-1}$. A minimal cover of G is given by the following family:

$$(**)\{\mathrm{Alt}(n)\} \cup \{\mathrm{Sym}(a) \times \mathrm{Sym}(b) \ : \ 1 \leq a, b \leq n-1, \ a+b = n\}.$$

The subgroups of $\mathrm{Sym}(n)$ isomorphic to $\mathrm{Sym}(a)\times\mathrm{Sym}(b)$, for $a+b=n$, are obtained by considering partitions $\{1,\dots,n\} = A \cup B$ with $A \cap B = \emptyset$, $|A| = a$ and $|B| = b$. Indeed, for such a partition, it turns out that

$$\{g \in \mathrm{Sym}(n) \ : \ g(x) \in A \ \forall x \in A\} \cong \mathrm{Sym}(a) \times \mathrm{Sym}(b).$$

Such subgroups of $\mathrm{Sym}(n)$ are called "maximal intransitive". The reason why family (**) is a cover of $\mathrm{Sym}(n)$ is that n being odd, the n-cycles are even permutations, hence they belong to $\mathrm{Alt}(n)$, and all the other permutations belong to some maximal intransitive subgroup (they have nontrivial orbits - just look at the

cycle structure and group the cycles in two blocks). Family (**) is a cover also for $n = 9$ but it is still not known whether it is minimal or not in this case.

It is easy to show that a group cannot be written as the union of two proper subgroups. Therefore $\sigma(G) \geq 3$ always. What can be said about the groups G with $\sigma(G) = 3$?

Theorem 16 (Scorza, 1926)**.** *Let G be a group. Then $\sigma(G) = 3$ if and only if G admits a normal subgroup N such that $G/N \cong C_2 \times C_2$.*

Note that the implication $\Leftarrow$ is easy: if $G/N \cong C_2 \times C_2$ then $\sigma(G) \leq \sigma(G/N) = \sigma(C_2 \times C_2) = 3$. On the other hand $\sigma(G) \geq 3$ (this is always true), so $\sigma(G) = 3$. The reason why $\sigma(C_2 \times C_2) = 3$ is that $C_2 \times C_2$ has only three nontrivial proper subgroups, and they have size 2. In general if p is any prime number then $C_p \times C_p$ has precisely $p+1$ proper nontrivial subgroups, and they are all cyclic of order p (so they are both minimal and maximal subgroups). It follows that $\sigma(C_p \times C_p) = p+1$. Indeed, any nontrivial element of $C_p \times C_p$ determines the proper subgroup in which it is contained: it is the subgroup which it generates. So in this case in order to cover the group all proper nontrivial subgroups have to be considered.

I now argue that whenever G is a noncyclic group and $|G|$ is a power of a prime p (i.e. G is a "p-group") we have $\sigma(G) = p + 1$.

Lemma 1 (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 $i = 1, \ldots, n$. Then $\min\{\beta_1, \ldots, \beta_n\} < \sigma(G)$.*

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 $\beta_1 < n$. □

Let us apply this to the case $|G| = p^n$. The index of any subgroup of G is a divisor of $|G|$ (Lagrange Theorem) so if a subgroup of G is proper then its index is at least p. It follows that $p < \sigma(G)$ so $p + 1 \leq \sigma(G)$. We are left to prove that $\sigma(G) \leq p+1$, and for this it is enough to find a normal subgroup N of G such that $G/N \cong C_p \times C_p$ (indeed $\sigma(G) \leq \sigma(G/N)$ and $\sigma(C_p \times C_p) = p+1$). This follows from the following fact, which I will state without proof (the proof is a bit technical). Recall that a subgroup H of G is called "maximal" if it is not properly contained in a subgroup of G, and the "Frattini subgroup" of a group G is the intersection of the maximal subgroups of G, denoted $\Phi(G)$. It is a normal subgroup of G. Moreover, denote by $d(G)$ the least integer d such that there exist d elements $x_1, \ldots, x_d \in G$ with $\langle x_1, \cdots, x_d \rangle = G$.

Proposition 2. *Let G be a p-group and let $d = d(G)$. Then $G/\Phi(G) \cong {C_p}^d$.*

Now if the p-group G is not cyclic, i.e. if $d > 1$, then ${C_p}^d$ clearly admits a quotient isomorphic to $C_p \times C_p = {C_p}^2$, therefore $\sigma(G) \leq \sigma(G/\Phi(G)) = \sigma({C_p}^d) \leq \sigma(C_p \times C_p) = p + 1$.

Using this we can deduce the value of $\sigma(G)$ whenever G is an abelian group. We first need a lemma.

Lemma 2. *If A, B are two groups of coprime order then $\sigma(A\times B) = \min\{\sigma(A), \sigma(B)\}$.*

Proof. Since $|A|$ and $|B|$ are coprime, the subgroups of $A \times B$ are of the form $H \times K$ with $H \leq A$ and $K \leq B$. With this in mind, the proof becomes technical. I will omit the details. □

Indeed, by the structure theorem of finite abelian groups (and the Chinese Remainder Theorem), any finite abelian group is a direct product of cyclic groups of prime power order, so

Proposition 3. *Let G be a noncyclic abelian group, and write $G = \prod_{i=1}^{k} C_{p_i^{n_i}}$. Then $\sigma(G) = p + 1$ where p is the smallest prime number such that there exist two distinct $i, j \in \{1, \dots, k\}$ with $p_i = p_j = p$.*

6.2. **Direct products.** Lemma 2 deals with direct products of groups A, B of coprime order. Let us give an example in which $A = B$. I will compute $\sigma(S \times S)$ when S is a nonabelian simple group. I will prove that $\sigma(S \times S) = \sigma(S)$. This will give me the opportunity to discuss more general facts.

Lemma 3 (Intersection argument)**.** *Let K be a maximal subgroup of a group G and let $\mathcal{H}$ be a minimal cover of G. If $\sigma(G) < \sigma(K)$ then $K \in \mathcal{H}$. Equivalently, if $K \notin \mathcal{H}$ then $\sigma(K) \leq \sigma(G)$.*

Proof. We have

$$K = K \cap G = K \cap \bigcup_{H \in \mathcal{H}} H = \bigcup_{H \in \mathcal{H}} (K \cap H)$$

therefore, if $\sigma(G) < \sigma(K)$, this union cannot consist of proper subgroups of K, thus there exists $H \in \mathcal{H}$ such that $K \cap H = K$, i.e. $K \subseteq H$. Since K is maximal it follows that $K = H \in \mathcal{H}$. □

Corollary 2. *Let M be a maximal subgroup of G, not normal, such that $\sigma(G) < \sigma(M)$. Then $|G : M| < \sigma(G)$.*

Proof. Using standard arguments of group actions, it is possible to prove that the number of conjugates of $H \leq G$ equals the index in G of the "normalizer" $N_G(H) := \{g \in G \ : \ g^{-1}Hg = H\}$ of H in G. We always have $H \subseteq N_G(H)$ and $N_G(H) = G$ if and only if H is normal in G. Now, M being maximal and not normal in G, $N_G(M) = M$ therefore M has $|G : M|$ conjugates in G. Since $\sigma(G) < \sigma(M)$, they all belong to every minimal cover of G by the intersection argument. In particular $\sigma(G) \geq |G : M|$. Now, the $|G : M|$ conjugates of M cover less than $|G| = |M| \cdot |G : M|$ group elements (they all contain the identity element), so we get the strict inequality $\sigma(G) > |G : M|$. □

This is actually the main argument used in [10] and in my Ph.D thesis. Let me be more precise about this. Recall that if A, B are two subgroups of a group G then the product AB is defined as $AB := \{ab \ : \ a \in A, \ b \in B\}$. It turns out that $|AB| = |A| \cdot |B|/|A \cap B|$ (nice exercise). A **supplement** of the normal subgroup $N \trianglelefteq G$ is a subgroup $H \leq G$ such that $HN = G$. A **complement** of N is a supplement H of N such that $H \cap N = \{1\}$. In this case we also say that H complements N in G. If H complements N then $|G| = |HN| = |H| \cdot |N|$, so $|G : N| = |H|$. The above corollary implies the following.

Proposition 4 (The Maximal Complement Argument)**.** *Let N be a nonsolvable normal subgroup of the group G and suppose that there exists a maximal subgroup M of G that complements N. Then $\sigma(G) = \sigma(G/N)$.*

This is the argument that allows to produce results about the structure of σ-elementary groups (cf. the following subsection). The proof is a bit technical but I hope that by writing it down I will give some ideas about the kind of arguments needed in this kind of analysis.

Proof. Thanks to nonsolvability of N we may assume that N does not contain nontrivial central elements of G (i.e. elements g lying in the center of G). Indeed if $g \in N$ and $g \in Z(G)$ we may consider the quotient $G/\langle g \rangle$ and proceed by induction on $|G|$. As a consequence of the classification of finite simple groups, N does not have fixed-point-free automorphisms (recall that an automorphism φ of N, i.e. a group isomorphism $N \to N$, is said to be fixed-point-free if $\varphi(x) \neq x$ whenever $x \in N$ and $x \neq 1$). It follows that the family $\{C_G(x) \ : \ 1 \neq x \in N\}$ covers G, where $C_G(x) = \{g \in G \ : \ gx = xg\}$. Indeed, if $g \in G$ then the map $N \to N$, $x \mapsto g^{-1}xg$ is an automorphism of N. Since N does not contain nontrivial central elements, $C_G(x) \neq G$ for every $1 \neq x \in N$. Therefore $\{C_G(x) \ : \ 1 \neq x \in N\}$ is a cover of G of size $|N| - 1$, so $\sigma(G) \leq |N| - 1$.

Now, M is not normal in G, otherwise $G \cong N \times M$ and maximality of M would imply that $|N| = |G : M| = p$ is a prime, contradicting the nonsolvability of N. Therefore Corollary 2 implies that $|N| = |G : M| < \sigma(G)$. This contradicts the fact that $\sigma(G) \leq |N| - 1$. □

Let us show how this implies that $\sigma(S \times S) = \sigma(S)$ whenever S is a nonabelian simple group. The following is a standard fact and a nice exercise.

Proposition 5. *Let G be a group. Then G is simple if and only if*

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

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

It follows that Δ_S is a maximal subgroup of $S \times S$ that complements $S \times \{1\}$, and we may apply the Maximal Complement Argument. Actually in this case much less is needed: since $S \times S \to S$, $(x, y) \mapsto x$ is a surjective homomorphism with kernel $\{1\} \times S$, by the Isomorphism Theorem (Theorem 1) and the fact that S being noncyclic, it admits as a cover the family of its nontrivial cyclic subgroups, it follows that

$$\sigma(S \times S) \leq \sigma(S) \leq |S| - 1,$$

and now since $|S \times S : \Delta_S| = |S|$ Corollary 2 yields a contradiction.

A result I obtained in a joint work with A. Lucchini is a generalization of this fact to all direct products:

Theorem 17 (Lucchini A., G 2010 [12])**.** *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* $\sigma(G) = p + 1$.

6.3. **σ-elementary groups.** Suppose we want to compute $\sigma(G)$ for a given group G. If there exists $N \trianglelefteq G$ such that $\sigma(G) = \sigma(G/N)$ then we may consider the group G/N instead of G. This gives a sort of reduction and leads to the following definition.

Definition 3 (σ-elementary groups)**.** *A group* G *is called* σ*-elementary if* $\sigma(G) < \sigma(G/N)$ *whenever* $\{1\} \neq N \trianglelefteq G$. G *is called* n*-elementary if* G *is* σ*-elementary and* $\sigma(G) = n$.

This notion was introduced in [9] and thoroughly studied in [10] (there these groups are called σ-primitive).

For example:

- If G is any group then there exists a normal subgroup N of G such that G/N is σ-elementary and $\sigma(G) = \sigma(G/N)$ (just choose a proper normal subgroup N of G such that $\sigma(G) = \sigma(G/N)$ and proceed by induction on $|G|$).
- If p is any prime number, $C_p \times C_p$ is $(p + 1)$-elementary (the nontrivial proper quotients are all cyclic of size p).
- The only 3-elementary group is $C_2 \times C_2$ (Scorza's Theorem).
- 6.2 implies that if S is a nonabelian simple group then $S \times \cdots \times S = S^m$ is σ-elementary if and only if $m = 1$.
- If $n \geq 3$ is an integer and $n \neq 4$ then $\mathrm{Sym}(n)$ is σ-elementary: its only nontrivial proper quotient is C_2. $\mathrm{Sym}(4)$ is not σ-elementary: it admits $\mathrm{Sym}(3)$ as homomorphic image (quotient) and $\sigma(\mathrm{Sym}(4)) = \sigma(\mathrm{Sym}(3)) = 4$.
- 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 $I \rtimes \mathrm{Alt}(p)$ 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, the action is the usual one on the p coordinates.

Let us list the known facts concerning σ-elementary groups. Recall that $\Phi(G)$, the Frattini subgroup of G, is the intersection of the maximal subgroups of G, $Z(G)$, the center of G, is the subgroup $\{g \in G \ : \ xg = gx \ \forall x \in G\}$, and G', the derived subgroup of G, is the intersection of the normal subgroups N of G such that G/N is abelian.

Proposition 6. *Let* G *be a* σ*-elementary group.*

- $\Phi(G) = \{1\}$.
- *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 (this follows from Theorem 17).*
- *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.*

A result I obtained is the determination of all n-elementary groups with $n \leq 25$.

Theorem 18 (G 2009 [11])**.** *All σ-elementary groups G with $\sigma(G) \leq 25$ are known.*

$\sigma(G)$	G
3	$C_2 \times C_2$
4	$C_3 \times C_3, Sym(3)$
5	$Alt(4)$
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	$3^2:4, AGL(1,9), Alt(5)$
11	$\emptyset$
12	$C_{11} \times C_{11}, 11:5,$ $D_{22}, AGL(1,11)$
13	$Sym(6)$
14	$C_{13} \times C_{13}, D_{26}, 13:3,$ $13:4, 13:6, AGL(1,13)$

$\sigma(G)$	G
15	$SL(3,2)$
16	$Sym(5), Alt(6)$
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	$\emptyset$

Scorza's Theorem can be read off from the top left line of the above table. Also, we see that there are some numbers n such that $\sigma(G) \neq n$ for every group G (7, 11, 19, 21, 22, 25). The following is an open question: are there infinitely many such n?

6.4. **A conjecture.**

Definition 4 (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.*

Let us give some 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 $\mathrm{Sym}(n)$ is $\mathrm{Alt}(n)$.
- The unique minimal normal subgroup of $\mathrm{Sym}(4)$ 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 known examples of σ-elementary groups either are abelian isomorphic to $C_p \times C_p$ or admit only one minimal normal subgroup. The main problem I dealt with in my Ph.D thesis is the following conjecture, still open.

Conjecture 1 (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". In the following result the **wreath product** $\mathrm{Alt}(5) \wr C_2$ is the semidirect product $(\mathrm{Alt}(5) \times \mathrm{Alt}(5)) \rtimes C_2$ where the action is given by the exchange of the two coordinates.

Theorem 19. *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. Moreover $\sigma(Alt(5) \wr C_2) = 57$, $Alt(5) \wr C_2$ is monolithic and its minimal normal subgroup is $Alt(5) \times Alt(5)$, not simple and not abelian.*

A subgroup H of a group G is said to be **subnormal** if there exists a chain $H \lhd H_2 \lhd \cdots \lhd H_n = G$. Subnormal subgroups are not necessarily normal, for example in Sym(4), $\langle (12)(34) \rangle \lhd V$ and $V \lhd \mathrm{Sym}(4)$ but $\langle (12)(34) \rangle$ is not normal in Sym(4). A **minimal subnormal subgroup** is a subnormal subgroup which does not properly contain nontrivial subnormal subgroups of G. Note that minimal subnormal subgroups are always simple groups. Here is another result I proved in my Ph.D thesis.

Theorem 20. *Let G be a non-abelian σ-elementary group, and suppose that every minimal subnormal subgroup of G is isomorphic to an alternating group $Alt(n)$ with n large enough and even. Then G is monolithic.*

References

[1] N. Jacobson, Basic Algebra 1 (second edition); W. H. Freeman and Company.
[2] M. Aschbacher, Finite Group Theory; Cambridge Studies in Advanced Mathematics.
[3] M. Isaacs, Finite Group Theory; Graduate Studies in Mathematics.
[4] D. Gorenstein, Finite Groups; American Mathematical Society.
[5] P. J. Cameron, Permutation Groups; London Mathematical Society.
[6] D. J. S. Robinson, A Course in the Theory of Groups; Springer.
[7] R. Brandl, Integer polynomials that are reducible modulo all primes, Amer. Math. Monthly 93, (1986) 286-288.
[8] D. Easdown, C. Praeger, On Minimal Faithful Permutation Representations of Finite Groups.
[9] J.H.E. Cohn, On n-sum groups; Math. Scand., 75(1) (1994), 44–58.
[10] E. Detomi, A. Lucchini, On the Structure of Primitive n-Sum Groups; CUBO A Mathematical Journal Vol.10 n. 03 (195–210), 2008.
[11] M. Garonzi, Finite Groups that are the union of at most 25 proper subgroups; Journal of Algebra and Its Applications Vol. 12, No. 4 (2013) 1350002.
[12] M. Garonzi, A. Lucchini, Direct products of groups as unions of proper subgroups; Archiv der Mathematik, ISSN: 0003-889X
[13] A. Maróti, M. Garonzi, Covering certain wreath products with proper subgroups; J. Group Theory 14 (2011), no. 1, 103-125.
[14] Garonzi Martino, Covering certain monolithic groups with proper subgroups; Communications in algebra, 41:2, 471–491