Groups and Galois Theory

Course Notes

Alberto Elduque

Departamento de Matemáticas
Universidad de Zaragoza
50009 Zaragoza, Spain

CONTENTS

SYLLABUS

This is a required course for Math Majors at the University of Zaragoza (School of Sciences). It consists of 6 credits. It is a sequel of (and relies heavily on) the course *Algebraic Structures*.

Lecturer: Alberto Elduque
Office: Math. Building. Second floor. Algebra Section. Office no. 2.
e-mail: elduque@unizar.es
http://personal.unizar.es/elduque

Course description: The goal of the course is to understand the basic properties of the groups, which form the basic algebraic structure to understand and measure the symmetry, and then to proceed to study the symmetry of the algebraic equations (Galois Theory). The peak of the course will be the proof of the impossibility to solve by radicals the algebraic equations of degree ≥ 5.

References:

There are many good references on Abstract Algebra, which include chapters devoted to Groups and to Galois Theory. Here are just a few of them:

- D.S. Dummit and R.M. Foote: *Abstract Algebra* (2^{nd} edition). John Wiley and Sons, 1999.
- J.J. Rotman: *A First Course in Abstract Algebra* (2^{nd} edition), Prentice Hall, 2000.
- R.B. Ash: *Abstract Algebra. The Basic Graduate Year*
  http://www.math.uiuc.edu/ r-ash/Algebra.html

Some more specific textbooks are the following:

- I. Stewart: *Galois Theory. 4th ed.*, CRC Press, 2015.
- J.P. Tignol: *Galois' Theory of Algebraic Equations*, World Scientific, 2001.
- J.S. Milne: *Group Theory* and *Fields and Galois Theory*,
  http://www.jmilne.org/math/CourseNotes/index.html

WHAT IS THIS COURSE ABOUT?

Symmetries of an equilateral triangle

Fix an equilateral triangle and consider the set

$$G = \{\text{isometries of } \mathbb{R}^2 \text{ fixing the triangle}\}$$

G consists of three reflections relative to the lines that pass through a vertex and the middle point of the opposite side (see Figure 1) together with the rotations of 0, 120 and 240 degrees. Thus G consists of 6 elements: $|G| = 6$.

Each isometry fixing the triangle permutes the vertices. The three reflections correspond to the transposition of two vertices. The rotations of 120 and 240 degrees correspond to the two cyclic permutations of the vertices.

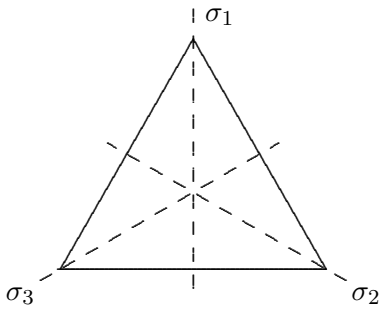


Figure 1: Symmetries of an equilateral triangle.

For us, the important property of this set G is that its elements can be composed (they are bijective maps!), and the composition of any two of its elements again belongs to G. Thus, for example, $\sigma_1\sigma_2$ is the clockwise rotation of 120 degrees.

These sets, endowed with a binary operation satisfying the usual properties of the composition of bijective maps, are called *groups*.

Solutions of equations by radicals

We are quite used to find the solutions of the degree 2 equations:

$$ax^2 + bx + c = 0,$$

which are given by the familiar formula:

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

In the course *Algebraic Structures* we learned how to solve the equations of degree 3 and 4, which involve the use of square and cubic roots.

The clue to deal with equations of degree ≥ 5 is to study the symmetries of the equation. These form a group, called the Galois group of the equation. Many properties of the equation, like its solvability by radicals, are determined by the structure of its Galois group.

The theory devoted to the study of the algebraic equations and their Galois groups is called *Galois Theory*.

This course is devoted to study the basic properties of groups and of the Galois Theory of algebraic equations.

CHAPTER 1

GROUPS

The purpose of this chapter is the study of those sets which, like the set of isometries preserving an equilateral triangle, are endowed with a binary operation satisfying the usual properties.

§ 1. Definitions and examples

1.1 Definition. A *group* is a nonempty set G endowed with a binary operation (usually called multiplication)

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\mapsto xy, \end{aligned}$$

which is associative ($(xy)z = x(yz)$ for any $x, y, z \in G$), there is a neutral element (which will usually be denoted by e: $ex = x = xe$ for any $x \in G$), and such that for any element $x \in G$ there exists an element, denoted by x^{-1} and called the inverse of x, such that $xx^{-1} = x^{-1}x = e$.

Moreover, if the multiplication is commutative ($xy = yx$ for any $x, y \in G$), then the group is said to be commutative or *abelian*.

1.2 Examples.

(i) Any ring R is an abelian group with the operation given by its addition. In particular we get the abelian groups $(\mathbb{Z}, +)$ or $(\mathbb{Z}/n\mathbb{Z}, +)$.

(ii) If R is a unital ring, the set of its units $R^\times = \{r \in R : \exists s \in R \text{ such that } rs = sr = 1\}$ is a group. The operation is given by the product of the ring.

(iii) **Classical groups:** For any natural number $n \in \mathbb{N}$ we have the following groups of matrices (the operation is the usual product):

- $GL(n,\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) : \det A \neq 0\}$ (general linear group),
- $SL(n,\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) : \det A = 1\}$ (special linear group),
- $O(n,\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) : AA' = I_n\}$ (orthogonal group),
- $SO(n,\mathbb{R}) = O(n,\mathbb{R}) \cap SL(n,\mathbb{R})$ (special orthogonal group).

(iv) Let Ω be an arbitrary set, then the set

$$S(\Omega) = \{f : \Omega \to \Omega : f \text{ is a bijective map}\}$$

is a group under the composition of maps. It is called the *group of permutations* of Ω.

The groups contained in $S(\Omega)$ are called *groups of transformations* of Ω.

The famous *Erlangen Program* (Felix Klein, 1872) proposed that Geometry is the study of invariants under the action of a group. Thus the euclidean geometry becomes the study of invariants under the isometry group (angles, distances, ..., are invarians), the affine (or projective) geometry becomes the study of invariants under the affine (or projective) group (for instance, the barycenter is an invariant), the topology becomes the study of invariants under the action of the group of homeomorphisms (compactness, connectedness, fundamental groups, ..., are invariants), ...

1.3 Remark. Thanks to the associativity of the product, there is no need to put parentheses in products $x_1x_2\cdots x_n$ $(n > 2)$. Also, we may define recursively the powers of an element of a group G as follows: $x^0 = e$, $x^{n+1} = x^n x$, $x^{-n} = (x^n)^{-1}$, for any $n \in \mathbb{N}$. The associativity of the product immediately gives the property $x^n x^m = x^{n+m}$ for any $x \in G$ and $n, m \in \mathbb{Z}$.

The associativity also implies the uniqueness of the inverse: If $xy = e = zx$, then

$$z = ze = z(xy) = (zx)y = ey = y.$$

As $(xy)(y^{-1}x^{-1}) = e$, it follows that $\boxed{(xy)^{-1} = y^{-1}x^{-1}}$.

1.4 Definition. Let G be a group and let H be a nonempty subset of G. H is said to be a *subgroup* of G if for any $x, y \in H$, both xy and x^{-1} belong to H. (It will be denoted by $H \leq G$.)

1.5 'Silly' properties. Let H be a nonempty subset of the group G.

- $H \leq G \implies e \in H$.
- $H \leq G \iff \forall x, y \in H,\ xy^{-1} \in H$.
- H is a subgroup of G if and only if H is closed under the multiplication in G, and it is a group with this multiplication.

1.6 Examples.

- $SO(n,\mathbb{R}) \leq SL(n,\mathbb{R}) \leq GL(n,\mathbb{R}), \quad O(n,\mathbb{R}) \leq GL(n,\mathbb{R})$.

- Let $\mathbb{H}$ be the ring of Hamilton quaternions, then $\mathbb{H}^\times = \{a+bi+cj+dk : a^2+b^2+c^2+d^2 \neq 0\}$. Consider the subset $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Then Q is a subgroup of $\mathbb{H}^\times$ consisting of 8 elements. It is called the *quaternion group*.

  Another subgroup of $\mathbb{H}^\times$ is given by the three-dimensional sphere:

$$S^3 = \{a + bi + cj + dk : a^2 + b^2 + c^2 + d^2 = 1\}.$$

- Any group G contains two trivial subgroups: $\{e\}$ and G. Any other subgroup is said to be a *proper subgroup* of G.

By abuse of notation, the trivial subgroup $\{e\}$ is usually denoted simply by 1 (or 0 if additive notation is being used).

Notation: Given a group G, its cardinal will be denoted by $|G|$. Thus, if G is finite, $|G|$ is the number of elements of G. This is called the *order* of G.

In general, multiplicative notation as above is used, unless we are dealing with abelian groups, like $(\mathbb{Z}, +)$; in this case, additive notation is used:

	Multiplicative notation	Additive notation
Neutral element	e or 1	0
operation	xy	$x + y$
inverse	x^{-1}	$-x$
powers	x^n	nx

§ 2. Cyclic groups. Generators

2.1 Definition. Let G be an arbitrary group and $g \in G$. Then $\{g^n : n \in \mathbb{Z}\}$ is a subgroup of G which is called the *cyclic subgroup* generated by g. It will be denoted by $\langle g \rangle$.

If there exists an element $g \in G$ such that $G = \langle g \rangle$, then G is said to be a *cyclic group*.

Note than any cyclic group is commutative, as $g^n g^m = g^{n+m} = g^m g^n$ for any $n, m \in \mathbb{Z}$.

2.2 Examples.

(i) $(\mathbb{Z}, +)$ is a cyclic group generated by 1 (and by -1).

(ii) Let P_n be a regular polygon of n sides on the euclidean plane, and let

$$G = \{\text{rotations of the plane which leave } P_n \text{ fixed}\}.$$

Then $G = \langle \varphi \rangle$, where φ is the rotation of angle $\frac{2\pi}{n}$ centered at the barycenter of the polygon.

Note that $G = \{id, \varphi, \varphi^2, \ldots, \varphi^{n-1}\}$ and $(\varphi^i)^{-1} = \varphi^{n-i}$ for any i.

2.3 Proposition. *Let G be a group and $g \in G$. Then:*

$$|\langle g\rangle| = \begin{cases} \infty, & \text{if } g^n \neq e \text{ for any } n \geq 1, \\ r = \min\{n \in \mathbb{N} : g^n = e\}, & \text{otherwise.} \end{cases}$$

In the first case, we say that the order *of g is infinite (and write $|g| = \infty$), while in the second case that g has* finite order r *(and write $|g| = r$).*

Proof. If $g^n \neq e$ for any $n \geq 1$ and there are $n \leq m \in \mathbb{Z}$ such that $g^n = g^m$, then multiply by g^{-n} to get $g^{m-n} = e$, so $n - m = 0$. Therefore, if $g^n \neq e$ for any $n \geq 1$, then the elements g^n, $n \in \mathbb{Z}$, are all different and $|\langle g\rangle| = \infty$.

On the contrary, if there exists a natural number n such that $g^n = 1$, take $r = \min\{n \in \mathbb{N} : g^n = e\}$. As before, it is easy to see that the elements $e, g, g^2, \ldots, g^{r-1}$ are all different. Moreover, for any $m \in \mathbb{Z}$, there are unique $q, s \in \mathbb{Z}$ with $0 \leq s < r$ such that $m = qr + s$. Then $g^m = (g^r)^q g^s = e^q g^s = g^s$, so that $\langle g\rangle = \{e, g, \ldots, g^{r-1}\}$ has order r. □

Note that the proof above shows that if the order of $g \in G$ is r, then $g^n = e$ for some $n \in \mathbb{Z}$ if and only if r divides n.

Also note that $\langle g\rangle$ is the smallest subgroup containing the element g. In the same way, given a subset S of a group G, the *subgroup generated* by S is, by definition, the smallest subgroup of G containing S, and it is denoted by $\langle S\rangle$. In other words, $\langle S\rangle$ is the intersection of all the subgroups of G containing S (as the intersection of a family of subgroups is always a subgroup):

$$\langle S\rangle = \bigcap\{H : H \leq G \text{ and } S \subseteq H\}.$$

2.4 Proposition. *Given a subset S of a group G, the subgroup generated by S is the subset of G consisting of e and of all the possible products*

$$t_1 t_2 \cdots t_n$$

with $n \in \mathbb{N}$ and such that for any $1 \leq i \leq n$, either $t_i \in S$ or $t_i^{-1} \in S$.

2.5 Examples.

- $\langle G\rangle = G$, $\langle \emptyset\rangle = 1$ (trivial subgroups).
- Let Q be the quaternion group, then $Q = \langle i, j\rangle$.

2.6 Definition. A group G is said to be *finitely generated* if there exists a finite subset S of G such that $G = \langle S\rangle$.

Note that, in particular, any cyclic group is finitely generated.

2.7 Proposition. *Let G be a group, and let a, b be two elements of G such that $ab = ba$, $|a| = s$, $|b| = t$, with $s, t \in \mathbb{N}$ and $\gcd(s, t) = 1$. Then $\langle a, b\rangle = \langle ab\rangle$ is a cyclic group of order st.*

Proof. Obviously $ab \in \langle a, b\rangle$, so we get $\langle ab\rangle \subseteq \langle a, b\rangle$.

Let d be an element in $\langle a\rangle \cap \langle b\rangle$, then there are natural numbers i and j such that $d = a^i = b^j$. Thus,

$$b^{sj} = (b^j)^s = d^s = (a^i)^s = a^{is} = (a^s)^i = e^i = e.$$

Therefore t divides sj, and since $\gcd(s, t) = 1$, we conclude that t divides j, but then $d = b^j = e$. Hence $\langle a\rangle \cap \langle b\rangle = 1$.

Now, for any natural number n, we get

$$\begin{aligned}(ab)^n = e &\iff a^n b^n = e \text{ since } ab = ba,\\ &\iff a^n = b^{-n} \in \langle a\rangle \cap \langle b\rangle,\\ &\iff a^n = b^n = e,\\ &\iff \text{both } s \text{ and } t \text{ divide } n,\\ &\iff st \text{ divides } n \text{ (since } \gcd(s, t) = 1).\end{aligned}$$

Therefore $|ab| = st$ and $\langle ab\rangle$ is a cyclic group of order st.

Moreover, $\langle a, b\rangle = \{a^i b^j : 0 \le i \le s-1,\ 0 \le j \le t-1\}$, and hence the order of $\langle a, b\rangle$ is at most st. Since $\langle ab\rangle$ is contained in $\langle a, b\rangle$, and $|ab| = st$, we conclude that $\langle ab\rangle = \langle a, b\rangle$, as required. □

§ 3. Homomorphisms

3.1 Definition. Let G and H be two groups and let $\varphi : G \to H$ be a map. Then:

- φ is said to be a *group homomorphism* (or just a homomorphism) if for any $x, y \in G$, $\varphi(xy) = \varphi(x)\varphi(y)$.
- If φ is a group homomorphism, then its *kernel* is the subset $\ker\varphi = \varphi^{-1}(e)$ of G, while its *image* is the set $\operatorname{im}\varphi = \varphi(G)$.
- A group homomorphism is said to be a *monomorphism* if it is one-to-one, an *epimorphism* if it is surjective, and an *isomorphism* if it is a bijection. Moreover, the isomorphisms $\psi : G \to G$ are called *automorphisms*.

3.2 Examples.

- Let C_n be a cyclic group of order n. If g is a generator of C_n, then the map $\varphi : (\mathbb{Z}, +) \to G$ given by $\varphi(m) = g^m$ is an epimorphism with $\ker\varphi = n\mathbb{Z}$.
- Two cyclic groups are isomorphic if and only if they have the same order. To see this, note that if G is an infinite cyclic group, then the example above shows that G is isomorphic to $(\mathbb{Z}, +)$, while the same arguments show that C_n is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.
- The map $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, .)$, $\varphi(x) = e^x$, is an isomorphism. (Here $\mathbb{R}^+$ denotes the set of positive real numbers.)

- The map $\varphi : (\mathbb{R}, +) \to SO(2, \mathbb{R})$, $\varphi(t) = \left(\begin{smallmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{smallmatrix}\right)$, is an epimorphism with $\ker \varphi = 2\pi\mathbb{Z}$.
- The determinant map $\det : GL(n, \mathbb{R}) \to (\mathbb{R} \setminus \{0\}, .)$, $A \mapsto \det A$, is an epimorphism with $\ker \det = SL(n, \mathbb{R})$.
- Let G be a group and let $a \in G$. The map $I_a : G \to G$ given by $I_a(x) = axa^{-1}$ (*conjugation* by the element a) is an automorphism, which is called an *inner automorphism*.

  The set $\operatorname{Aut} G$ of automorphisms of G is a group under the composition of maps, and the map $I : G \to \operatorname{Aut} G$, given by $I(a) = I_a$ is a homomorphism, because $I_a I_b = I_{ab}$. Its image $\operatorname{im} I$ is the subgroup of inner automorphisms, denoted by $\operatorname{Int} G$, while its kernel is $\ker I = \{a \in G : I_a = id\} = \{a \in G : ax = xa \ \forall x \in G\}$, which is called the *center* of G (and denoted by $Z(G)$).

3.3 Properties. *Let $\varphi : G \to H$ be a group homomorphism. Then:*

(i) *$\varphi(e) = e$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$ for any $x \in G$,*

(ii) *$\operatorname{im} \varphi$ is a subgroup of H,*

(iii) *$\ker \varphi$ is a subgroup of G which satisfies the following extra condition: $\forall x \in \ker \varphi$, $\forall a \in G$, $axa^{-1} \in \ker \varphi$.*

This last property deserves a name:

3.4 Definition. Let G be a group and let N be a subgroup of G. Then N is said to be a *normal subgroup* of G if for any $x \in N$ and $a \in G$, the element axa^{-1} belongs to N. (This will be denoted by $N \trianglelefteq G$.)

Therefore the kernels of group homomorphisms are normal subgroups. The trivial subgroups 1 and the whole G are always normal subgroups of a group G. If G is abelian, then any subgroup is a normal subgroup.

Given a group G and a subgroup H, define the following relation among elements in G:

$$a \sim b \quad \text{if} \quad a^{-1}b \in H.$$

This is clearly an equivalence relation. The equivalence class of the element a is the subset

$$\{b \in G : a^{-1}b \in H\} = \{b \in G : \exists h \in H \text{ such that } b = ah\} =: aH,$$

which is called the *left coset of a modulo H*.

In the same vein we may define the equivalence relation where $a \sim b$ if $ab^{-1} \in H$, whose equivalence classes are the *right cosets modulo H* (the sets Ha for $a \in G$).

The set of left cosets modulo H (the quotient set by the equivalence relation) is denoted by G/H, and its cardinal by $[G : H]$, which is called the *index* of the subgroup H in G.

Note that the map $H = eH \to aH$, $h \mapsto ah$, is bijective, and hence all the left cosets modulo H have the same cardinal, equal to $|H|$. It follows that G is the disjoint union of the equivalence classes, and hence

$$|G| = [G : H]\,|H|.$$

3.5 Proposition. ***(Lagrange's Theorem)*** *The order of a finite group is a multiple of the order of any of its subgroups.*

3.6 Corollary.

(i) *The order of any element of a finite group divides the order of the group.*

(ii) *If the order of a group G is a prime number, then G is cyclic.*

In general, given a divisor of the order of a finite group, there may be no subgroup whose order is this divisor. However, for cyclic groups we have the following result:

3.7 Theorem. *Any subgroup of a cyclic group is cyclic. Moreover, the subgroups of $(\mathbb{Z}, +)$ are the subgroups $(m\mathbb{Z}, +)$ for $m \in \mathbb{N} \cup \{0\}$, and the subgroups of $(\mathbb{Z}/n\mathbb{Z}, +)$ are in one-to-one correspondence with the divisors of n.*

Proof. Let H be a subgroup of either $(\mathbb{Z}, +)$ or $(\mathbb{Z}/n\mathbb{Z}, +)$. Then for any $m \in \mathbb{Z}$ and $a \in H$, $ma = a + \cdots + a$ (m summands) if $m > 0$, while $ma = (-a) + \cdots + (-a)$ ($-m$ summands) if $m < 0$. In both cases, $ma \in H$ as H is closed under the operation (the sum) and the inverse (the opposite). It follows that H is an ideal of $\mathbb{Z}$ or of $\mathbb{Z}/n\mathbb{Z}$, and the result follows from the corresponding result in the course *Algebraic Structures*. (Anyway, it is very easy to provide a direct proof.) □

Using the fact that any cyclic group is isomorphic to either $(\mathbb{Z}, +)$ or to $(\mathbb{Z}/n\mathbb{Z}, +)$ for some $n \in \mathbb{N}$, we get the following consequence:

3.8 Corollary. *Let $G = \langle a \rangle$ be a cyclic group of order $q \in \mathbb{N}$ and let $d \in \mathbb{N}$ be a divisor of q. Then the subgroup of G of order d is (with additive notation) $H = \langle \frac{q}{d} a \rangle = \{b \in G : db = 0\}$.*

Let now N be a normal subgroup of a group G. Then the equivalence relation considered above ($a \sim b$ if $a^{-1}b \in N$) satisfies the following property:

$$a \sim b \text{ and } c \sim d \implies ac \sim bd,$$

because $(ac)^{-1}bd = c^{-1}a^{-1}bd = (c^{-1}(a^{-1}b)c)(c^{-1}d)$, and both $c^{-1}d$ and $c^{-1}(a^{-1}b)c$ are in N (the latter one because N is normal).

Therefore we may define a multiplication on the quotient set G/N as follows:

$$(aN)(bN) = (ab)N,$$

for any $a, b \in G$. This multiplication is associative, the element eN is its neutral element, and the inverse of aN is given by $a^{-1}N$. Hence, G/N is a group, called the *quotient group* of G modulo N.

With the same sort of arguments used for rings, the following results can easily be proved:

3.9 Theorem.

1. ***First Isomorphism Theorem:*** *Let $\varphi : G \to H$ be a group homomorphism, then the quotient group $G/\ker\varphi$ is isomorphic to* $\operatorname{im}\varphi$ *through the isomorphism*
$$\begin{aligned}\bar{\varphi} : G/\ker\varphi &\to \operatorname{im}\varphi\\ a\ker\varphi &\mapsto \varphi(a).\end{aligned}$$

2. *Let N be a normal subgroup of a group G, then the map $\pi : G \to G/N$, $a \mapsto aN$, is an epimorphism, called the* natural projection *of G over G/N. Besides,* $\ker\pi = N$. *In particular, this shows that any normal subgroup is the kernel of some homomorphism.*

3. *Let $\varphi : G \to H$ be a group homomorphism, then φ is a monomorphism if and only if* $\ker\varphi = 1$, *while φ is an epimorphism if and only if* $\operatorname{im}\varphi = H$.

4. ***Second Isomorphism Theorem:*** *Let H be a subgroup and N a normal subgroup of a group G. Then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G, N is a normal subgroup of HN, $H \cap N$ is a normal subgroup of H and the map*
$$\begin{aligned}H/H\cap N &\to HN/N\\ h(H\cap N) &\mapsto hN,\end{aligned}$$
is an isomorphism.

5. ***Third isomorphism theorem:*** *Let H and K be two normal subgroups of a group G with $H \subseteq K$, then K/H is a normal subgroup of G/H and the quotient groups $(G/H)/(K/H)$ and G/K are isomorphic.*

6. *Let N be a normal subgroup of a group G, then the map*
$$\begin{aligned}\{\textit{subgroups of } G \textit{ containing } N\} &\to \{\textit{subgroups of } G/N\}\\ H &\mapsto H/N,\end{aligned}$$
is a bijection. The inverse map is given by $\tilde{H} \leq G/N \mapsto H = \{g \in G : gN \in \tilde{H}\}$. The same result is valid changing subgroups for normal subgroups.

§ 4. Symmetric group

We have already seen that given an arbitrary set Ω, the set $S(\Omega) = \{f : \Omega \to \Omega : f \text{ is a bijective map}\}$ is a group with the composition of maps.

Take $\Omega = \{1, 2, \ldots, n\}$, then the group $S(\Omega)$ is denoted by S_n and called the *symmetric group of degree n*.

The elements of S_n can be represented like this:
$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n\\ \pi(1) & \pi(2) & \ldots & \pi(n)\end{pmatrix}.$$
For obvious reasons, the elements of S_n are called *permutations*.

4.1 Example. Consider the symmetric group S_4 and its elements

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Then,

$$\sigma\tau = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \qquad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

4.2 Proposition. *The order of the symmetric group of degree n is $|S_n| = n!$. Its neutral element is the identity map: $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{smallmatrix}\right)$.*

Let us try to decompose any permutation into a product of simpler permutations:

4.3 Example. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 8 & 1 & 3 & 5 & 7 & 6 \end{pmatrix}$

Under the action of π, the elements are permuted as follows:

$$1 \mapsto 2 \mapsto 4 \mapsto 1, \quad 3 \mapsto 8 \mapsto 6 \mapsto 5 \mapsto 3, \quad 7 \mapsto 7.$$

There are thus three disjoint *cycles*. We will write then $\pi = (1\,2\,4)(3\,8\,6\,5)(7)$ or simply (omitting the cycles of length 1):

$$\pi = (1\,2\,4)(3\,8\,6\,5).$$

In general, given any permutation $\pi \in S_n$ and any $i \in \Omega = \{1, \ldots, n\}$, the *orbit* of the element i under the action of π is the set $\{i, \pi(i), \pi^2(i), \ldots\} \subseteq \Omega$. Sooner or later, there appear natural numbers $h < k$ with $\pi^h(i) = \pi^k(i)$, so that $\pi^{k-h}(i) = i$. Hence, if l is the lowest natural number such that $\pi^l(i) = i$, then the orbit of i is precisely $\{i, \pi(i), \ldots, \pi^{l-1}(i)\}$. This number l is then called the *length* of the orbit. The different orbits give a partition of Ω:

$$\Omega = \Omega_1 \cup \cdots \cup \Omega_p \quad \text{(disjoint union)}.$$

If $|\Omega_k| = l_k$, then for any $i \in \Omega_k$, $\Omega_k = \{i, \pi(i), \ldots, \pi^{l_k-1}(i)\}$. The permutation π acts independently on each orbit and hence π is the product $\pi = \pi_1 \cdots \pi_p$, where for each k,

$$\pi_k(i) = \begin{cases} \pi(i) & \text{if } i \in \Omega_k, \\ i & \text{otherwise.} \end{cases}$$

The permutations π_k are *cycles* of length l_k. In case $l_k = 1$, then $\pi_k = id$. Therefore we get the following result:

4.4 Theorem. *Any permutation in S_n different from the identity can be expressed uniquely as a product of "disjoint" cycles of length ≥ 2, up to the order of these cycles.*

4.5 Corollary. *Let π be an element of S_n expressed as a product $\pi = \pi_1 \cdots \pi_p$ of disjoint cycles of length ≥ 2. Let the length of π_k be l_k for $k = 1, \ldots, p$. Then the order of π is the lowest common multiple of the l_k's: $|\pi| = \mathrm{lcm}(l_1, \ldots, l_p)$.*

Proof. Since the π_k's are disjoint, they commute, so for any $n \in \mathbb{N}$,

$$\pi^n = \pi_1^n \cdots \pi_p^n,$$

and $\pi^n = 1$ if and only if $\pi_k^n = 1$ for any k, if and only if l_k divides n for any k, as required. (Note that the symbol 1 is used for the identity map.) □

4.6 Example. What are the possible orders of the elements of S_6?

Because of the previous Corollary, it is enough to see what are the different ways to decompose $\{1, 2, 3, 4, 5, 6\}$ into disjoint orbits. That is, the different ways of decomposing 6 as a sum of natural numbers:

Decomposition	example	order
1+1+1+1+1+1	id	1
2+1+1+1+1	(1 2)	2
2+2+1+1	(1 2)(3 4)	2
2+2+2	(1 2)(3 4)(5 6)	2
3+1+1+1	(1 2 3)	3
3+2+1	(1 2 3)(4 5)	6
3+3	(1 2 3)(4 5 6)	3
4+1+1	(1 2 3 4)	4
4+2	(1 2 3 4)(5 6)	4
5+1	(1 2 3 4 5)	5
6	(1 2 3 4 5 6)	6

4.7 Definition. A cycle of length 2 is called a *transposition.*

4.8 Proposition. *Any permutation can be expressed as a product of transpositions.*

Proof. It is enough to check that any cycle is a product of transpositions. For this just note the following:

$$(1\,2\,\cdots\,l) = (1\,l)(1\,l-1)(1\,l-2)\cdots(1\,3)(1\,2).$$ □

Note that the expression of a permutation as a product of transpositions is not unique in general. For instance, in S_4 we have:

$$(1\,2\,3) = (1\,3)(1\,2) = (2\,3)(1\,3) = (1\,3)(2\,4)(1\,2)(1\,4).$$

4.9 Proposition. *Given a natural number n, consider the map:*

$$\varphi : S_n \longrightarrow GL(n, \mathbb{R})$$

$$\sigma \mapsto \begin{pmatrix} E_{\sigma(1)} & \cdots & E_{\sigma(n)} \end{pmatrix}$$

where E_i denotes the column with a 1 in the i-th position, and 0's elsewhere. In other words, $\varphi(\sigma)$ is the matrix (a_{ij}) with $a_{ij} = 1$ if $i = \sigma(j)$ and $a_{ij} = 0$ otherwise.

Then φ is a group homomorphism.

Proof. For any $\sigma, \tau \in S_n$, consider $\varphi(\sigma) = (a_{ij})$, $\varphi(\tau) = (b_{ij})$ and $\varphi(\sigma\tau) = (c_{ij})$. Then, for any i, j:

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = a_{i\tau(j)}b_{\tau(j)j} = \begin{cases} 1 & \text{if } i = \sigma\tau(j), \\ 0 & \text{otherwise.} \end{cases}$$

Therefore $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$ and $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$. □

Since the determinant map $\det : GL(n, \mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism too, so is the composition $\det \circ\varphi$. Moreover, $\det \circ\varphi(\sigma) = \pm 1$, as the determinant of the matrix associated to any transposition is -1 (the corresponding matrix is the identity matrix with two columns permuted), and any σ is a product of transpositions.

4.10 Definition. The epimorphism $\operatorname{sgn} : S_n \to C_2 = \{1, -1\}$ (C_2 is the cyclic group of two elements) given by $\operatorname{sgn}(\sigma) = \det(\varphi(\sigma))$ is called the *signature homomorphism*. The value $\operatorname{sgn}(\sigma)$ is said to be the *signature* of the permutation σ. Its kernel is denoted by A_n and called the *alternating group* of degree n. The permutations in A_n are said to be *even*, while the permutations in $S_n \setminus A_n$ are said to be *odd*.

Note that A_n is a normal subgroup of S_n of index 2, as S_n/A_n is isomorphic to C_2.

4.11 Theorem. *Let π be a permutation in the symmetric group S_n.*

(i) *If $\pi = \tau_1\tau_2\cdots\tau_p$ for some transpositions τ_i, $i = 1, \ldots, p$, then $\operatorname{sgn}\pi = (-1)^p$.*

(ii) *If $\pi = \pi_1\pi_2\cdots\pi_q$ for some disjoint cycles π_i of length l_i, then $\operatorname{sgn}\pi = (-1)^{\sum_{i=1}^{q}(l_i-1)}$.*

Proof. For (i) just note that $\operatorname{sgn}\pi = \prod_{i=1}^{p}\operatorname{sgn}(\tau_i) = (-1)^p$, as the signature of any transposition is -1.

For (ii) note that the signature of a cycle of length l is $(-1)^{l-1}$, as $(1\,2\,\cdots\,l) = (1\,l)(1\,l-1)(1\,l-2)\cdots(1\,3)(1\,2)$ (a product of $l-1$ transpositions). Now (i) can be applied. □

Symmetric groups are quite important, partly because of the next result:

4.12 Cayley's Theorem. Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.

Proof. We may identify S_n with $S(G) = \{f : G \to G : f \text{ is a bijection}\}$. Consider the "left action":

$$\begin{aligned} L : G &\longrightarrow S(G) \\ a &\mapsto L_a : G \to G \\ &\qquad x \mapsto ax \end{aligned}$$

For any $a \in G$, L_a is bijective with inverse $L_{a^{-1}}$, and $L_{ab} = L_a \circ L_b$ for any $a, b \in G$. Thus, L is a group homomorphism. Moreover, if $a \in \ker L$, then $L_a = id$, that is $ax = x$ for any $x \in G$. In particular $a = ae = e$. Hence $\ker L = 1$, and $G \simeq \operatorname{im} G \leq S(G)$. □

§ 5. Group actions

Groups made their appearance as "groups of symmetries"; that is, their elements are symmetry maps on some object.

5.1 Definition. Let G be a group and Ω a set. An *action* of G on Ω (on the left) is a map

$$\begin{aligned} \Phi : G \times \Omega &\longrightarrow \Omega \\ (g, x) &\mapsto gx \end{aligned}$$

satisfying the following two properties:

(i) $ex = x$ for any $x \in \Omega$,

(ii) $(gh)x = g(hx)$ for any $g, h \in G$ and $x \in \Omega$.

Note that if Φ is a group action, then the map (which will be again denoted by Φ):

$$\begin{aligned} \Phi : G &\longrightarrow S(\Omega) \\ g &\mapsto \Phi_g : \Omega \to \Omega \\ & \qquad x \mapsto gx \end{aligned}$$

is a group homomorphism. And conversely, given any group homomorphism $\Phi : G \to S(\Omega)$, $g \mapsto \Phi_g$, the map $G \times \Omega \to \Omega$, given by $(g, x) \mapsto \Phi_g(x)$, is an action of the group G on Ω.

Therefore,

$$\{\text{Actions of } G \text{ on } \Omega\} \cong \{\text{Homomorphisms } G \to S(\Omega)\},$$

and an action of a group can be considered too as a homomorphism $\Phi : G \to S(\Omega)$.

5.2 Examples.

(i) Any subgroup of S_n acts on $\{1, 2, \ldots, n\}$ in a natural way.

(ii) In Cayley's Theorem we considered the action of a group on itself by left multiplication:

$$\begin{aligned} L : G &\longrightarrow S(G) \\ g &\mapsto L_g : G \to G \\ & \qquad x \mapsto gx \end{aligned}$$

which corresponds to the map $G \times G \to G$, $(g, x) \mapsto gx$.

(iii) Recall the definition of similar matrices in Linear Algebra. This corresponds to the action

$$\begin{aligned} GL(n, \mathbb{R}) \times \mathrm{Mat}_n(\mathbb{R}) &\longrightarrow \mathrm{Mat}_n(\mathbb{R}) \\ (A, B) \quad &\mapsto ABA^{-1}. \end{aligned}$$

5.3 Definition. Let $\Phi : G \to S(\Omega)$ be an action of a group G on a set Ω. Then:

- $\ker\Phi$ is said to be the *kernel* of the action. If $\ker\Phi = 1$, then the action is said to be *faithful*, and then G can be identified to a subgroup of $S(\Omega)$ through Φ.

- There appears the following equivalence relation on Ω:

$$x \sim y \iff \exists g \in G \text{ such that } gx = y.$$

  The equivalence classes are called the *orbits* of the action.
  The orbit of an element $x \in \Omega$ is denoted by $\mathrm{orb}(x)$ or simply by Gx. If there is just one orbit, then the action is called *transitive*. (This means that for any $x, y \in \Omega$, there is an element $g \in G$ such that $gx = y$.)

- For any $x \in \Omega$, the *stabilizer* of x is the subgroup

$$G_x = \{g \in G : gx = x\}.$$

5.4 Proposition. *Let $\Phi : G \to S(\Omega)$ be an action of a group G on a set Ω. Then:*

(i) *For any $x \in \Omega$, $|Gx| = [G : G_x]$. In particular, if G is finite, the length (cardinal) of any orbit divides the order of G. Therefore, if $\{\Omega_i : i \in I\}$ is the set of orbits of the action, and $\{x_i : i \in I\}$ is a set of representatives of the orbits (that is, $x_i \in \Omega_i$ for any $i \in I$) then*

$$\boxed{|\Omega| = \sum_{i\in I} |\Omega_i| = \sum_{i\in I} [G : G_{x_i}]}$$

(ii) *Let $g \in G$ and $x, y \in \Omega$ be such that $gx = y$, then $G_y = gG_xg^{-1} = I_g(G_x)$.*

(iii) ***Cauchy-Frobenius:*** *If G is finite and for any $g \in G$ we consider $F(g) = \{x \in \Omega : gx = x\}$ (the set of fixed elements by g), then*

$$\boxed{\textit{number of orbits} = \frac{1}{|G|} \sum_{g\in G} |F(g)|}$$

Proof. For (i) just note that $gx = g'x$ if and only if $g^{-1}g' \in G_x$, if and only if $g' \in gG_x$. Hence the map $Gx \to G/G_x$, $gx \mapsto gG_x$ is well defined and bijective, so $|Gx| = [G : G_x]$.

Also note that if $gx = y$ and $hy = y$, then $hgx = gx$ or $g^{-1}hgx = x$, and conversely. Then $h \in G_y$ if and only if $g^{-1}hg \in G_x$, if and only if $h \in gG_xg^{-1}$, thus obtaining the result in (ii). Therefore, if x and y belong to the same orbit, then $|G_x| = |G_y|$ and $[G : G_x] = [G : G_y]$. From here, the last part of (i) follows.

Consider now the set $X = \{(g, x) \in G \times \Omega : gx = x\}$. We may count the elements of X in two ways:

$$|X| = \sum_{g\in G} |F(g)| \qquad \text{and} \qquad |X| = \sum_{x\in\Omega} |G_x|.$$

But because of (ii) we get:

$$\begin{aligned}|X| &= \sum_{x\in\Omega}|G_x| = \sum_{i\in I}|Gx_i||G_{x_i}| \\ &= \sum_{i\in I}|G| = |G|(\text{number of orbits}).\end{aligned}$$

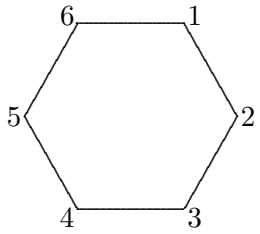
Hence

$$|G|(\text{number of orbits}) = |X| = \sum_{g\in G}|F(g)|,$$

as required. □

5.5 Example. A bracelet is made by stringing together six beads, two of them are green and the other four beads are red. How many different patterns are possible?

Let P_6 be the regular hexagon. We put the beads on the vertices of P_6.



There are $\binom{6}{2} = \binom{6}{4} = 15$ ways of doing this. However, two of these ways give the same pattern if there is a symmetry of P_6 which takes one to the other. Therefore, the number of different patterns is the number of orbits of the action of the group of symmetries of P_6 acting on the set of the 15 different possibilities.

The group of symmetries of the regular hexagon is the *dihedral* group D_6 of degree 6:

$$D_6 = \{id, \varphi, \varphi^2, \ldots, \varphi^5, s_{14}, s_{25}, s_{36}, s_{12}^{45}, s_{23}^{56}, s_{34}^{61}\}$$

where φ is the clockwise rotation of angle $\frac{2\pi}{6}$, s_{14} is the reflection relative to the axis which goes through the vertices 1 and 4, s_{12}^{45} is the reflection relative to the axis which goes through the middle points of the sides which join the vertices 1 and 2 and the vertices 4 and 5, and similarly for the other elements.

Now we compute the fixed elements in the set Ω of our 15 possibilities by each element of the group D_6, in order to apply Cauchy-Frobenius Theorem:

- $|F(id)| = 15$,
- $|F(\varphi)| = |F(\varphi^2)| = |F(\varphi^4)| = |F(\varphi^5)| = 0$,
- $|F(\varphi^3)| = 3$ (which correspond to the green beads in vertices 1 and 4, in 2 and 5, and in 3 and 6),

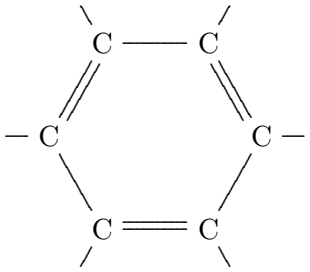
- $|F(s_{14})| = 3$ (which correspond to the green beads in 1 and 4, in 2 and 6 and in 3 and 5), and in the same vein $|F(s_{25})| = |F(s_{36})| = 3$,
- $|F(s_{12}^{45})| = 3$ (which correspond to the green beads in 1 and 2, in 3 and 6 and in 4 and 5), and in the same vein $|F(s_{23}^{56})| = |F(s_{34}^{61})| = 3$.

Therefore:

$$\text{number of patterns} = \frac{1}{12}\Big(15 + 3 + 3 \times 3 + 3 \times 3\Big) = \frac{36}{12} = 3.$$

Note that the result is clear: the green beads may be in adjacent vertices, or separated by one vertex, or in opposite vertices.

5.6 Example. How many different chemical compounds can be obtained adding radicals CH_3 or H to a benzene ring?



Here we have two possible colors (CH_3 or H) for each vertex of the hexagon. Hence there are $2^6 = 64$ different possibilities. A similar computation to the one performed before gives:

- $|F(id)| = 64$,
- $|F(\varphi)| = |F(\varphi^5)| = 2$,
- $|F(\varphi^2)| = |F(\varphi^4)| = 2^2$,
- $|F(\varphi^3)| = 2^3$,
- $|F(s_{14})| = |F(s_{25})| = |F(s_{36})| = 2^4$,
- $|F(s_{12}^{45})| = |F(s_{23}^{56})| = |F(s_{34}^{61}| = 2^3$.

And hence:

$$\text{number of compounds} = \frac{1}{12}\Big(64 + 2 \times 2 + 2 \times 2^2 + 2^3 + 3 \times 2^4 + 3 \times 2^3\Big) = 13.$$

§ 6. Conjugation. Translation

6.1. Action by conjugation

The action by conjugation of a group on itself is given by the homomorphism

$$\begin{aligned} \Phi : G &\longrightarrow \operatorname{Aut} G \leq S(G) \\ g &\mapsto I_g : G \to G \\ & \qquad x \mapsto gxg^{-1} \end{aligned}$$

We already know that its kernel is the center of G:

$$\ker \Phi = Z(G) = \{g \in G : gx = xg \ \forall x \in G\}.$$

The orbits of this action are called *conjugacy classes*:

$$\operatorname{orb}(x) = \{y \in G : \exists g \in G \text{ such that } y = gxg^{-1}\}.$$

The stabilizer of an element $x \in G$ is called the *centralizer* of x:

$$C_G(x) = \{g \in G : gx = xg\}.$$

Note that the orbit of x restricts to $\{x\}$ if and only if $C_G(x) = G$, if and only if $x \in Z(G)$. Therefore, if G is a finite group and $x_1, \ldots, x_r$ are representatives of the orbits containing at least two elements, then

$$\boxed{|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]},$$

which is called the *class equation* of the group G.

6.1 Corollary. *Let p be a prime number and let G be a finite p-group (that is, the order of G is a power of p). Then $Z(G) \neq 1$. Moreover, if $|G| = p^2$, then G is abelian ($G = Z(G)$).*

Proof. Consider the class equation of G, and note that since $[G : C_G(x_i)] \geq 2$, and it divides the order of G, $[G : C_G(x_i)]$ is a power of p for any i. It follows that p divides $|Z(G)|$, and hence $Z(G) \neq 1$.

Moreover, assume that G is a non abelian group with $|G| = p^2$. Take an element $x \in G \setminus Z(G)$. By the above $Z(G)$ is a subgroup of order p, and hence it is cyclic: $Z(G) = \langle y \rangle$. Then $\langle x, y \rangle$ is a subgroup, whose order is greater than p and divides the order of G. Since $|G| = p^2$, it follows that $G = \langle x, y \rangle$. But x and y commute as $y \in Z(G)$, so G is abelian, a contradiction. □

6.2 Example. (Conjugation in S_n)
Let π, σ be two permutations in S_n and assume that $\pi(i) = j$. Then

$$\sigma\pi\sigma^{-1}(\sigma(i)) = \sigma\pi(i) = \sigma(j).$$

That is, if we have $i \xrightarrow{\pi} j$, then $\sigma(i) \xrightarrow{\sigma\pi\sigma^{-1}} \sigma(j)$. Therefore, if π is expressed as a product of disjoint cycles:

$$\pi = (i_1 \ldots i_r)(j_1 \ldots j_s) \cdots,$$

then

$$\sigma\pi\sigma^{-1} = \big(\sigma(i_1)\dots\sigma(i_r)\big)\big(\sigma(j_1)\dots\sigma(j_r)\big)\cdots$$

Therefore, two elements of S_n are conjugate if and only if they have the same *cycle structure* (that is, they can be expressed as a product of disjoint cycles of the same length). The *type* of the permutation π is the sequence $(\alpha_1,\dots,\alpha_n)$, where α_i is the number of cycles of length i (the number of orbits of length i in the action of π on $\{1,2,\dots,n\}$). Note that $\alpha_1+2\alpha_2+\cdots+n\alpha_n = n$.

Thus, for example, for $n = 5$, the elements

$$1,\ (1\,2),\ (1\,2)(3\,4),\ (1\,2\,3),\ (1\,2\,3)(4\,5),\ (1\,2\,3\,4),\ (1\,2\,3\,4\,5),$$

form a representative system of the conjugacy classes in S_5.

The action by conjugation can be extended to an action of G on $\Omega = \{\text{subsets of } G\}$:

$$\begin{aligned}\tilde{\Phi} : G &\longrightarrow S(\Omega)\\ g &\mapsto I_g : \Omega \to \Omega\\ &\qquad S \mapsto gSg^{-1}\end{aligned}$$

Two subsets S and T are said to be conjugate if there is an element $g \in G$ such that $T = gSg^{-1}$.

Given a subgroup H of G, its stabilizer under this action is called the *normalizer* of H:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Note that H is a normal subgroup of its normalizer, and that H is normal if and only if $N_G(H) = G$. The length of the orbit of H is then $[G : N_G(H)]$.

6.2. Action by translation

The action by (left) translation of a group on itself is given by the homomorphism

$$\begin{aligned}L : G &\longrightarrow S(G)\\ g &\mapsto L_g : G \to G\\ &\qquad x \mapsto gx\end{aligned}$$

This action has already been used in Cayley's Theorem (4.12).

If H is a subgroup of G, this action L induces an action

$$\begin{aligned}L^H : G &\longrightarrow S(G/H)\\ g &\mapsto L_g^H : G/H \to G/H\\ &\qquad xH \mapsto gxH\end{aligned}$$

which is well defined, as $xH = yH$ if and only if $x^{-1}y \in H$, if and only if $(x^{-1}g^{-1})(gy) \in H$, if and only if $gxH = gyH$.

The kernel of this action is given by:

$$\begin{aligned}\ker L^H &= \{g \in G : gxH = xH \ \forall x \in G\} \\ &= \{g \in G : x^{-1}gx \in H \ \forall x \in G\} \\ &= \{g \in G : g \in xHx^{-1} \ \forall x \in G\} \\ &= \cap_{x\in G} xHx^{-1},\end{aligned}$$

which is the largest normal subgroup of G contained in H.

6.3 Corollary.

(i) *If H is a subgroup of G of index n ($[G : H] = n$) and such that H does not contain any nontrivial normal subgroup of G, then $|G|$ divides $n!$.*

(ii) *If p is the lowest prime dividing the order of a finite group G, and if H is a subgroup of G with $[G : H] = p$, then H is a normal subgroup.*

Proof. For (i) note that $L^H : G \to S(G/H) \cong S_n$ is a monomorphism. For (ii) consider again the action L^H and its kernel $K = \ker L^H$. K is a normal subgroup of G contained in H, and $[G : K]$ divides $p! = |S(G/H)|$. But $[G : K] = [G : H][H : K] = p[H : K]$. Hence $[H : K]$ divides $(p-1)!$. However, the prime factors of $[H : K]$ are greater or equal than p. The only possibility is $[H : K] = 1$, or $H = K$, which is normal. □

§ 7. Sylow's Theorems

7.1 Definition. Let G be a finite group and let p be a prime number with $|G| = p^n m$ and $p \nmid m$. The subgroups of G of order p^n are called the *Sylow p-subgroups* of G.

The objective of this section is the proof of the following result:

7.2 Theorem. ***(Sylow, 1872)*** *Let G be a finite group and let p be a prime number with $|G| = p^n m$ and $p \nmid m$. Then:*

(i) *G contains Sylow p-subgroups,*

(ii) *Any two Sylow p-subgroups are conjugate,*

(iii) *The number of Sylow p-subgroups of G is congruent to 1 modulo p.*

A previous Lemma, due to Cauchy, is needed:

7.3 Lemma. *Let G be a finite group and let p be a prime number dividing the order of G. Then there are elements of G of order p.*

Proof. Assume first that G is abelian, and take a nontrivial element $g \in G$. If $p \,|\, |g|$, then $|g| = pr$ for some $r \in \mathbb{N}$, and g^r is an order p element. Otherwise, $H = \langle g \rangle$ is a normal subgroup of G (as G is abelian), and it can be assumed by an inductive argument that there is an element $xH \in G/H$ of order p. If $|x| = m$, then we have $(xH)^m = eH$, so $p = |xH|$ divides m, and again $x^{m/p}$ has order p.

If G is not abelian, consider its class equation $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$. If $p \,|\, |Z(G)|$, then there are elements of order p in the abelian subgroup $Z(G)$. Otherwise there is an i such that $p \nmid [G : C_G(x_i)]$. But then p divides $|C_G(x_i)|$, and an inductive argument finishes the proof. □

Proof of the Theorem. For part (i), consider again the class equation $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$. If $p \nmid |Z(G)|$, then again there is an i such that $p \nmid [G : C_G(x_i)]$, so that $|C_G(x_i)| = p^n m'$ for some m' (since $|G| = [G : C_G(x_i)]|C_G(x_i)|$). An inductive argument shows that there is a subgroup of $C_G(x_i)$ of order p^n, and this is a Sylow subgroup of G.

Otherwise $p \,|\, |Z(G)|$, so by Cauchy's Lemma, there is an element $z \in Z(G)$ of order p. Since z is central, $N = \langle z \rangle$ is a normal subgroup of G and $|G/N| = p^{n-1}m$. By an inductive argument there is a subgroup $P/N \leq G/N$ of order p^{n-1}, and hence $|P| = p^n$, so it is a Sylow p-subgroup.

We will prove an assertion which is stronger than (ii): Let P be a Sylow p-subgroup of G, and let Q be any p-subgroup of G, then we will check that Q is contained in a conjugate of P. Actually, consider the action

$$\begin{aligned} Q &\longrightarrow S(G/P) \\ g &\mapsto L_g^P : G/P \to G/P \\ &\qquad xP \mapsto gxP. \end{aligned}$$

Write $\Omega = G/P$, and let $\Omega_1, \ldots, \Omega_r$ be the orbits of this action. Since $|\Omega_i|$ divides $|Q|$ (a power of p) for any i and $m = |G/P| = |\Omega| = \sum_{i=1}^{r} |\Omega_i|$, and $p \nmid m$, it follows that there is an i such that $|\Omega_i| = 1$. That is, there is an element $x \in G$ such that $gxP = xP$ for any $g \in Q$. This means that $x^{-1}gx \in P$ for any $g \in Q$, or $Q \leq xPx^{-1}$.

As for (iii), let P be a Sylow p-subgroup, and let Ω be the set of Sylow p-subgroups of G, which is the set of subgroups conjugate to P. Consider the action by conjugation:

$$\begin{aligned} P &\longrightarrow S(\Omega) \\ g &\mapsto \Omega \to \Omega \\ &\qquad Q \mapsto gQg^{-1}. \end{aligned}$$

If an orbit of this action contains just one element Q, then $gQg^{-1} = Q$ for any $g \in P$, so that $P \leq N_G(Q)$, but then P and Q are Sylow p-subgroups of $N_G(Q)$, and hence they are conjugate in $N_G(Q)$. Since Q is a normal subgroup of $N_G(Q)$, it follows that $Q = P$. Therefore there is just one orbit consisting of one element, namely $\{P\}$. The length of any other orbit is a nontrivial divisor of $|P|$, and hence it is a power of p. We conclude that $|\Omega| = 1 + \sum(\text{powers of } p)$, and this is congruent to 1 modulo p. □

7.4 Remark. If P is a Sylow p-subgroup of a finite group G, then the number of Sylow p-subgroups is the number of subgroups conjugate to P, which is $[G : N_G(P)]$, and this is a divisor of $[G : P]$ and of $|G|$.

7.5 Corollary. *Let P be a Sylow p-subgroup of a finite group G, then P is the only Sylow p-subgroup of G if and only if P is a normal subgroup of G, if and only if P contains all p-subgroups of G.*

7.6 Example. Let p be a prime number, consider the following classical group:

$$G = SL(2,\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}_p,\ ad-bc = 1 \right\}.$$

We are going to compute the number of Sylow p-subgroups of G.

First, since $\det : GL(2,\mathbb{Z}_p) \to \mathbb{Z}_p^\times$ is a group epimorphism, and $SL(2,\mathbb{Z}_p)$ equals $\ker\det$, it follows that

$$|G| = \frac{|GL(2,\mathbb{Z}_p)|}{p-1} = \frac{(p^2-1)(p^2-p)}{p-1} = p(p^2-1).$$

On the other hand, it is clear that

$$P_1 = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z}_p \right\} \quad \text{and} \quad P_2 = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} : a \in \mathbb{Z}_p \right\}$$

are two Sylow p-subgroups. Hence P_1 is not a normal subgroup, so that $N_G(P_1) \neq G$. Also, for any $0 \neq b \in \mathbb{Z}_p$,

$$\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 1 & b^2a \\ 0 & 1 \end{pmatrix},$$

so that $H = \left\{ \left(\begin{smallmatrix} b & a \\ 0 & b^{-1} \end{smallmatrix} \right) : b \in \mathbb{Z}_p^\times, a \in \mathbb{Z}_p \right\}$ is a subgroup contained in $N_G(P_1)$. But $|H| = p(p-1)$, $N_G(P_1) \neq G$, and $[G : N_G(P_1)] = 1 + kp$ for some $k \geq 1$ (because of the "Third Sylow's Theorem"). The only possibility is $[G : N_G(P_1)] = p+1$ and $H = N_G(P_1)$. Therefore the number of Sylow p-subgroups of G is $p+1$.

§ 8. Direct products

8.1 Definition. Let $G_1, \ldots, G_n$ be groups, then the cartesian product $G = G_1 \times \cdots \times G_n$ is a group with the operation defined componentwise. It is called the *direct product* of the groups $G_1, \ldots, G_n$.

Note that if $G = G_1 \times \cdots \times G_n$ is a direct product, for each i the subset $H_i = \{(e, \ldots, x, \ldots, e) : x \in G_i\}$ (n-tuples with an element of G_i in the ith position, and the neutral element of the group G_j in the jth position for any $j \neq i$) is a normal subgroup of G isomorphic to G_i.

If each of the groups G_i is abelian, so is G. Moreover, if additive notation is used for the abelian groups, then the direct product is denoted by $G_1 \oplus \cdots \oplus G_n$.

8.2 Theorem. *Let G be a group, and let $H_1, \ldots, H_n$ be normal subgroups of G satisfying that $G = \langle H_1, \ldots, H_n \rangle$ and that for any $i = 1, \ldots, n$, $H_i \cap \langle H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_n \rangle = 1$. Then the map*

$$\begin{aligned} \varphi : H_1 \times \cdots \times H_n &\longrightarrow G \\ (h_1, \ldots, h_n) &\mapsto h_1 h_2 \cdots h_n \end{aligned}$$

is a group isomorphism.

Proof. For any $h_i \in H_i$ and $h_j \in H_j$, $i \neq j$,

$$h_i h_j h_i^{-1} h_j^{-1} = \begin{cases} (h_i h_j h_i^{-1}) h_j^{-1} \in H_j & \text{since } H_j \trianglelefteq G, \\ h_i (h_j h_i^{-1} h_j^{-1}) \in H_i & \text{since } H_i \trianglelefteq G, \end{cases}$$

so that, as $H_i \cap H_j = 1$, it follows that $h_i h_j h_i^{-1} h_j^{-1} = e$, or $h_i h_j = h_j h_i$. This shows that φ is a group homomorphism.

Moreover, $H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i \ \forall i\}$ is then a normal subgroup of G which contains all the H_i's. Hence $G = \langle H_1, \ldots, H_n \rangle = H_1 H_2 \cdots H_n$, and hence φ is an epimorphism.

Finally, if $(h_1, h_2, \ldots, h_n) \in \ker \varphi$, then $h_1 h_2 \cdots h_n = e$, so that for any i, $h_i = h_1^{-1} \cdots \hat{\imath} \cdots h_n^{-1} \in H_i \cap \langle H_1, \ldots, \hat{\imath}, \ldots, H_n \rangle = 1$, and this shows that φ is a monomorphism. □

In the situation of the theorem above, G is said to be the *inner direct product* of the subgroups $H_1, \ldots, H_n$. Any element of G can be written in a unique way as a product $h_1 h_2 \cdots h_n$, with $h_i \in H_i$, $i = 1, \ldots, n$.

The case $n = 2$ of the previous theorem asserts that if H and K are two normal subgroups of a group G with $HK = G$ and $H \cap K = 1$, then G is isomorphic, in a natural way, to the direct product $H \times K$.

If we only assume that H is a normal subgroup of G, but K is just a subgroup, and again $HK = G$ and $H \cap K = 1$, then G is called the *semidirect product* of the normal subgroup H by the subgroup K. In this case note that for $h_1, h_2 \in H$ and $k_1, k_2 \in K$:

$$(h_1 k_1)(h_2 k_2) = \big(h_1 (k_1 h_2 k_1^{-1})\big)(k_1 k_2) = \big(h_1 I_{k_1}(h_2)\big)(k_1 k_2),$$

and note that we have a natural homomorphism $K \to \operatorname{Aut} H$, given by $k \mapsto I_k|_H$.

Conversely, assume that H and K are two groups, and that $\varphi : K \to \operatorname{Aut} H$, $x \mapsto \varphi_x$, is a group homomorphism. On the cartesian product $H \times K$ define a product by:

$$(a, x)(b, y) = (a \varphi_x(b), xy),$$

for any $a, b \in H$ and $x, y \in K$. With this product $H \times K$ is a group (CHECK THIS!), denoted by $H \rtimes_\varphi K$, and called the *outer semidirect product* of H and K with respect to φ. This semidirect product has two distinguished subgroups, the normal subgroup $\{(h, e) : h \in H\}$ isomorphic to H, and $\{(e, k) : k \in K\}$ isomorphic to K.

§ 9. Finitely generated abelian groups

Throughout this section, additive notation will be used.

9.1 Definition. Let A be an abelian group. The subgroup

$$\begin{aligned} \operatorname{tor} A &= \{x \in A : \exists n \in \mathbb{N} \text{ such that } nx = 0\} \\ &= \{x \in A : |x| < \infty\} \end{aligned}$$

is called the *torsion subgroup* of A. The group A is said to be *torsion free* in case $\operatorname{tor} A = 0$.

9.2 Remark. Let A be any abelian group. Then $A/\operatorname{tor} A$ is a torsion free group. (Why?)

9.3 Theorem. *Let A be a nonzero finitely generated abelian group. Then there are a natural number $n \in \mathbb{N}$, an integer $r \in \mathbb{Z}$ with $0 \leq r \leq n$, natural numbers $m_1, \ldots, m_r \geq 2$, and a system of generators $\{a_1, \ldots, a_n\}$ of A such that:*

- *$A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$ is the inner direct sum of the $\langle a_i \rangle$'s.*
- *$|a_i| = m_i$ for any $i = 1, \ldots, r$, $|a_i| = \infty$ for $r+1 \leq i \leq n$, and $m_1 \,|\, m_2 \,|\, \cdots \,|\, m_r$.*

Moreover, the numbers $n, r, m_1, \ldots, m_r$ are uniquely determined by A, $n - r$ is called the Betti number *of A, and $m_1, \ldots, m_r$ the* invariant factors *of A.*

9.4 Remark. Note that the Theorem implies that A is isomorphic to the group $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z} \oplus \overset{n-r}{\cdots} \oplus \mathbb{Z}$.

Proof. Let n be the minimal number of generators of A. First we will show the existence of the decomposition in the Theorem by induction on n, and we will check also that there appear exactly n summands.

If $n = 1$ A is cyclic, so it is either isomorphic to $\mathbb{Z}$ or to $\mathbb{Z}_m$ for some m and we are done.

Assume the result is true for $n-1$. If there is a generating system $\{a_1, \ldots, a_n\}$ such that $q_1 a_1 + \cdots + q_n a_n = 0$ for $q_1, \ldots, q_n \in \mathbb{Z}$ implies $q_1 = \cdots = q_n = 0$, then it is clear that $|a_i| = \infty$ and $A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle \simeq \mathbb{Z} \oplus \overset{n}{\cdots} \oplus \mathbb{Z}$ (because for any i $\langle a_i \rangle \cap \Big(\langle a_1 \rangle + \cdots + \langle a_{i-1} \rangle + \langle a_{i+1} \rangle + \cdots + \langle a_n \rangle \Big) = 0$). Otherwise the set Ω of those natural numbers $x \in \mathbb{N}$ such that there exists a generating system $\{b_1, \ldots, b_n\}$ of A and integers $x_2, \ldots, x_n \in \mathbb{Z}$ such that $x b_1 + x_2 b_2 + \cdots + x_n b_n = 0$ is not empty. Let m_1 be the minimum of Ω and let $\{b_1, \ldots, b_n\}$ be a generating system and $s_2, \ldots, s_n \in \mathbb{Z}$ integers such that $m_1 b_1 + s_2 b_2 + \cdots + s_n b_n = 0$. For any $i = 2, \ldots, n$, let $q_i, r_i \in \mathbb{Z}$, with $0 \leq r_i < m_1$ be the unique integers satisfying $s_i = q_i m_1 + r_i$. Then

$$m_1(b_1 + q_2 b_2 + \cdots + q_n b_n) + r_2 b_2 + \cdots + r_n b_n = 0.$$

Since $\{a_1 = b_1 + q_2 b_2 + \cdots + q_n b_n,\ b_2, \ldots, b_n\}$ is a generating system of A, and m_1 is the minimum of Ω, it follows that $r_2 = \cdots = r_n = 0$. Therefore $m_1 a_1 = 0$ and, by minimality, $|a_1| = m_1$. Moreover, A is the inner direct sum $A = \langle a_1 \rangle \oplus \langle b_2, \ldots, b_n \rangle$, as otherwise there would exist a nonzero element $r a_1 \in \langle a_1 \rangle \cap \langle b_2, \ldots, b_n \rangle$ with $0 < r < m_1$. But then $r \in \Omega$ and $r < m_1$, a contradiction.

By the induction argument, $\langle b_2, \ldots, b_n \rangle = \langle a_2 \rangle \oplus \cdots \oplus \langle a_n \rangle$, for some elements $a_2, \ldots, a_n$ such that $|a_i| = m_i < \infty$ for $i = 2, \ldots, r$ and $|a_i| = \infty$ for $r \leq i \leq n$, for some r and m_i's, with $m_2 \,|\, \cdots \,|\, m_r$.

Finally, the division algorithm gives us integers q, s with $m_2 = q m_1 + s$ and $0 \leq s < m_1$. Then

$$\begin{aligned} 0 &= m_1 a_1 + m_2 a_2 + 0 a_3 + \cdots + 0 a_n \\ &= m_1(a_1 + q a_2) + s a_2 + 0 a_3 + \cdots + 0 a_n, \end{aligned}$$

and since $\{a_1 + q a_2, a_2, \ldots, a_n\}$ is a generating system, it follows that $s \in \Omega$ unless $s = 0$. Since $s < m_1$, the only possibility left is $s = 0$, so that $m_1 \,|\, m_2$.

Let us prove the uniqueness now. Note that

$$\operatorname{tor} A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle,$$

and

$$B = A/\operatorname{tor} A \cong \langle a_{r+1} \rangle \oplus \cdots \oplus \langle a_n \rangle \cong \mathbb{Z} \oplus \overset{n-r}{\cdots} \oplus \mathbb{Z}.$$

Hence

$$B/2B \cong \mathbb{Z}_2 \oplus \overset{n-r}{\cdots} \oplus \mathbb{Z}_2,$$

which contains 2^{n-r} elements. Therefore we obtain:

$$n - r = \log_2 \left(|(A/\operatorname{tor} A)/2(A/\operatorname{tor} A)| \right).$$

Now $\operatorname{tor} A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle$ and hence m_r is the maximum of the orders of the elements in $\operatorname{tor}(A)$:

$$m_r = \max\{|x| : x \in \operatorname{tor}(A)\}.$$

Also, for any $j = 1, \ldots, r-1$ and $d \in \mathbb{N}$ with $d \,|\, m_{j+1}$, we have

$$d \operatorname{tor}(A) = \oplus_{i=1}^{r} \langle d a_i \rangle$$

and

$$|d \operatorname{tor}(A)| = \prod_{i=1}^{r} |d a_i| = \left(\prod_{i=1}^{j} |d a_i| \right) \cdot \left(\prod_{i=j+1}^{r} \frac{m_i}{d} \right).$$

Hence $|d \operatorname{tor}(A)| = \frac{1}{d^{r-j}} (m_{j+1} \cdot \cdots \cdot m_r)$ if and only if $d a_i = 0$ for any $i = 1, \ldots, j$, if and only if m_j divides d. Therefore we get:

$$m_j = \min\{d \in \mathbb{N} : d \,|\, m_{j+1} \text{ and } |d \operatorname{tor}(A)| = \frac{1}{d^{r-j}} (m_{j+1} \cdot \cdots \cdot m_r)\}.$$

We conclude that $m_1, \ldots, m_r$ are uniquely determined by $\operatorname{tor}(A)$, and hence by A. □

9.5 Corollary. *Let $0 \neq A$ be a finite abelian group. Then there are natural numbers $r, m_1, \ldots, m_r$ with $m_1 \geq 2$ and $m_1 \,|\, m_2 \,| \cdots | \, m_r$, uniquely determined by A, such that $A \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$.*

9.6 Lemma. *Let $m = p_1^{s_1} \cdots p_r^{s_r}$ be the prime factorization of a natural number $m \geq 2$ ($p_1, \ldots, p_r$ are different prime numbers and $s_1, \ldots, s_r \in \mathbb{N}$). Then the abelian group $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{s_r}}$.*

Proof. Actually, the Chinese Remainder Theorem shows us that there is a ring isomorphism $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{s_r}}$. This isomorphism is, in particular, a group isomorphism. □

9.7 Example. If A is a finite abelian group with invariant factors 6 and 18. Then we get:

$$A \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{18} \cong \Big(\mathbb{Z}_2 \oplus \mathbb{Z}_3 \Big) \oplus \Big(\mathbb{Z}_2 \oplus \mathbb{Z}_9 \Big) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9.$$

On the other hand, if an abelian group B is isomorphic to, say, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, then again by the previous Lemma B is isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{36}$. By the uniqueness of the Theorem above, we conclude that its invariant factors are 3, 6 and 36.

The arguments in this example give the following result:

9.8 Corollary. *Any nonzero finite abelian group is isomorphic to a direct sum of cyclic groups whose orders and powers of prime numbers. These powers are uniquely determined by the group (and are called the* elementary divisors *of the group).*

9.9 Example. How many abelian groups of order 180 do exist, up to isomorphism?
Since $180 = 2^2 \cdot 3^2 \cdot 5$, there are the following possibilities for the elementary divisors:

$$\begin{aligned} 2,2,3,3,5: &\quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{30}, \\ 4,3,3,5: &\quad \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{60}, \\ 2,2,9,5: &\quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{90}, \\ 4,9,5: &\quad \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{180}. \end{aligned}$$

§ 10. Solvable groups

The solvable groups are the ones that will appear as groups of symmetries of the algebraic equations which are solvable by radicals.

10.1 Definition. Let G be a group and let $x, y \in G$.

- The element $[x, y] = xyx^{-1}y^{-1}$ is called the *commutator* of x and y.
- The subgroup generated by the commutators: $G' = \langle [a, b] : a, b \in G \rangle$, is called the *derived subgroup* of G.

Note that $[x, y] = e$ if and only if $xy = yx$, and hence a group G is abelian if and only if $G' = 1$. In a way, G' measures how far the group G is from being abelian.

10.2 Example. For any x, y in the symmetric group S_n,

$$\operatorname{sgn}[x, y] = \operatorname{sgn} x \operatorname{sgn} y (\operatorname{sgn} x)^{-1} (\operatorname{sgn} y)^{-1} = 1,$$

so that the derived subgroup of S_n is contained in the alternating group A_n. Moreover,

$$[(i\,j), (i\,k)] = (i\,j)(i\,k)(i\,j)(i\,k) = (i\,j\,k),$$

and hence all the 3-cycles are in S_n'. But, for different i, j, h, k:

$$\begin{aligned} &(i\,j)(i\,k) = (i\,k\,j), \\ &(i\,j)(h\,k) = (i\,j)(i\,h)(i\,h)(h\,k) = (i\,h\,j)(h\,k\,i), \end{aligned}$$

and hence any even product of transpositions is a product of 3-cycles. Therefore we get

$$A_n \subseteq \langle \text{cycles of length } 3 \rangle \subseteq S_n' \subseteq A_n,$$

and we conclude that the alternating group A_n is the derived subgroup of the symmetric group S_n, and it is generated by the cycles of length 3.

10.3 Proposition. *Let G be a group.*

(i) *If K is a normal subgroup of G, then so is K'. In particular G' is a normal subgroup of G.*

(ii) *The quotient group G/G' is abelian, and if K is a normal subgroup of G with G/K abelian, then G' is contained in K.*

(iii) *Any subgroup of G containing G' is normal.*

Proof. For (i) note that $\forall g \in G$ and $\forall x, y \in K$, $I_g([x,y]) = [I_g(x), I_g(y)] \in K'$, since I_g is an automorphism. Therefore $I_g(K') \subseteq K'$ for any $g \in G$ and K' is a normal subgroup.

For (ii) it is enough to note the following equation in the quotient group G/G' valid for any $x, y \in G$:

$$(xG')(yG') = (xy)G' = (xy)[y^{-1}, x^{-1}]G' = yxG' = (yG')(xG').$$

Hence G/G' is abelian. Besides, if G/K is abelian, then $xyK = yxK$ for any $x, y \in G$, and this is equivalent to $[x,y] \in K$. Thus $G' \subseteq K$.

Finally, if $G' \subseteq K \subseteq G$, and $x \in K$, $g \in G$, $gxg^{-1} = [g,x]x \in K$, because $[g,x] \in G' \subseteq K$, so K is a normal subgroup. □

We already have two subgroups related to the commutativity of a group G:

$$G \text{ is abelian} \iff G' = 1 \iff Z(G) = G.$$

Define recursively the following normal subgroups of a group G:

- $G^{(0)} = G$, $G^{(n+1)} = \left(G^{(n)}\right)'$,
- $Z_0 = 1$, $Z_{n+1}/Z_n = Z(G/Z_n)$.

10.4 Definition. Let G be a group.

- The descending chain of normal subgroups $G = G^{(0)} \supseteq G' = G^{(1)} \supseteq G^{(2)} \supseteq \cdots$ is called the *derived series* of G.
- The ascending chain of normal subgroups $1 = Z_0 \subseteq Z(G) = Z_1 \subseteq Z_2 \subseteq \cdots$ is called the *upper central series* of G.
- The group G is said to be *solvable* if there is an $n \in \mathbb{N}$ such that $G^{(n)} = 1$.
- The group G is said to be *nilpotent* if there is an $n \in \mathbb{N}$ such that $Z_n = G$.

10.5 Example. The symmetric group S_2 is the cyclic group of order 2, which is abelian, and hence solvable.

The symmetric group S_3 satisfies that its derived subgroup is A_3, which is cyclic of order 3. Hence its derived chain is $S_3 \trianglerighteq A_3 \trianglerighteq 1$ and S_3 is solvable too.

The symmetric group S_4 satisfies that its derived subgroup is A_4 of order 12. Consider the so called *Klein four group*

$$V = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

It is straightforward to check that this is a subgroup, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and it is normal as any conjugate of a product of two disjoint transpositions is a product of two disjoint transpositions. Note that V is contained in A_4 and A_4/V has order 3, and hence it is cyclic. Hence $(A_4)' \subseteq V$. But $[(1\,2\,3),(1\,2\,4)] = (1\,2)(3\,4)$. It follows that the derived series of S_4 is $S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq 1$. Again S_4 is solvable.

10.6 Proposition.

(i) *Any p-group (p a prime number) is nilpotent.*

(ii) *A group G is solvable if and only if there is chain of subgroups $G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$, with each factor G_i/G_{i+1} being abelian.*

(iii) *Any nilpotent group is solvable.*

(iv) *If N is a normal subgroup of a group G, then G is solvable if and only if so are both N and G/N.*

Proof. **(i)** If G is a p-group: $|G| = p^n$, we know (see 6.1 Corollary) that $Z_1 = Z(G)$ is not trivial ($1 \subsetneqq Z_1$). Now, if $Z_1 \neq G$, then G/Z_1 is a p-group too, so $1 \neq Z_2/Z_1 = Z(G/Z_1)$ and hence $Z_1 \subsetneqq Z_2$. Continuing in this way we get $1 \subsetneqq Z_1 \subsetneqq Z_2 \subsetneqq \cdots$. Since G is finite, it turns out that $G = Z_n$ for some n.

(ii) One implication is clear, because if G is solvable, its derived series is a chain with abelian consecutive factors. Conversely, if $G \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$ is a descending chain with abelian consecutive factors, then we may prove inductively that $G^{(i)} \subseteq G_i$ for any $i = 0, 1, 2, \ldots$ (with $G_0 = G$). Indeed, this is trivial for $i = 0$, and if $G^{(i)} \subseteq G_i$, then since G_i/G_{i+1} is abelian, $G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i' \subseteq G_{i+1}$, as desired.

(iii) If G is nilpotent, the chain $G = Z_n \trianglerighteq Z_{n-1} \trianglerighteq \cdots \trianglerighteq Z_0 = 0$ is a descending chain with abelian consecutive factors, and hence G is solvable.

(iv) Note that if N is a normal subgroup of a solvable group G with $G^{(n)} = 1$, then[1] $N^{(n)} \subseteq G^{(n)} = 1$, and also $\left(G/N\right)^{(n)} \subseteq G^{(n)}N/N = N/N = 1$. Hence both N and G/N are solvable. Conversely, if both N and G/N are solvable, we may join any descending chains with consecutive abelian factors of both N and G/N to get such a chain for G: $N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_r = 1$ and $G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq \cdots \trianglerighteq G_s/N = N/N = 1$ give the descending chain $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_s = N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_r = 1$.

□

10.7 Proposition. *Let p, q and r be three different prime numbers. Then the groups of order p^n ($n \geq 1$), pq, p^2q, p^2q^2 and pqr are all solvable.*

Proof. We have already proved in the previous proposition that any p-group is nilpotent, and hence solvable.

pq : We may assume $p > q$. If $|G| = pq$, the number of Sylow p-subgroups of G is N_p, and $N_p \,|\, q$, since $N_p = [G : N_G(P)] \,|\, [G : P]$ for a fixed Sylow subgroup P of G, while $N_p \equiv 1 \pmod{p}$.

[1] This is valid even for a non normal subgroup and shows that any subgroup of a solvable group is solvable

The only possibility is $N_p = 1$, and hence there is a unique (normal) Sylow p-subgroup P. Then $|P| = p$, so P is cyclic (and hence abelian and solvable) and $|G/P| = q$ and hence G/P is solvable too. Thus, G is solvable.

p^2q : If $p > q$ the same argument as before gives that there is a unique Sylow p-subgroup P which, as any p-group, is nilpotent and hence solvable, while G/P is cyclic, and the result follows. If $p < q$, then the number of Sylow q-subgroups N_q divides p^2 and is $\equiv 1 \pmod q$. Then either $N_q = 1$ and, as before, G is solvable, or $N_q = p^2$. In this case, there are exactly p^2 Sylow q-subgroups, and each of them is cyclic of order q, so there are $p^2(q-1)$ elements of order q in G. But $|G| = p^2q = p^2(q-1) + p^2$, so there is room for a unique Sylow p-subgroup, and this implies again that G is solvable.

p^2q^2 : We may assume that $p > q$ and, as before, either $N_p = 1$ or $N_p = q^2$. In the first case we are done. In the second case, as $N_p \equiv 1 \pmod p$, $p \,|\, q^2 - 1 = (q-1)(q+1)$, so $p \,|\, q+1$ and $p = q+1$ as $p > q$. The only possibility is $q = 2$ and $p = 3$. Thus we have $N_3 = 4$. Let P be a Sylow 3-subgroup of G, then G acts by left multiplication on the quotient G/P: $\Phi : G \to S(G/P) \simeq S_4$. But $|S_4| = 24$ and $|G| = 36$. Thus $\ker\Phi$, which is the largest normal subgroup contained in P is not trivial. We conclude that $\ker\Phi$ has order 3, and hence it is solvable, while $G/\ker\Phi$ has order 12 and hence it is solvable too.

pqr : We may assume $p > q > r$ and $N_p, N_q, N_r > 1$. Since $N_p \mid qr$, $N_p \equiv 1 \pmod p$, and $p > q, r$, we conclude that $N_p = qr$, and hence there are $(p-1)qr$ elements of order p in G. Also $N_q \,|\, pr$ and $N_q \equiv 1 \pmod q$ so $N_q \geq p$ and there are at least $p(q-1)$ elements of order q. But $(p-1)qr + p(q-1) = pqr + (p(q-1) - qr) > pqr = |G|$, a contradiction.

□

There are two deep results of Group Theory which we mention here without proofs:

10.8 Burnside's Theorem (1904). Let p and q be two different prime numbers and let $n, m \in \mathbb{N}$. Then any group of order p^nq^m is solvable.

10.9 Feit-Thompson's Theorem (1963). Any finite group of odd order is solvable.

§ 11. Simple groups

11.1 Definition. A nontrivial group G is said to be *simple* if it contains no proper normal subgroup.

11.2 Proposition. *Let G be a solvable group. Then G is simple if and only if it is cyclic of prime order.*

Proof. It is clear that any cyclic group of prime order is simple. Conversely, given a simple solvable group G, as $G' \trianglelefteq G$, and $G' \neq G$, it follows that $G' = 1$, so G is abelian. Then for any element $1 \neq x \in G$, we have $\langle x\rangle \trianglelefteq G$, so that $G = \langle x\rangle$ is cyclic. But if $|x| = nm$, with $n, m > 1$, then $\langle x^m\rangle$ is a proper normal subgroup of G. Hence G is cyclic of prime order. □

Our purpose now is to show that the alternating groups A_n for $n \geq 5$ are simple.

11.3 Lemma. *Assume $n \geq 3$.*

(i) *The alternating group A_n is generated by the cycles of length 3.*

(ii) *If a normal subgroup of A_n contains a cycle of length 3, then it is the whole A_n.*

Proof. Part (i) is already known (see 10.2). Now, if $N \trianglelefteq A_n$ and $(a\,b\,c) \in N$, then a simple computation gives $(a\,b\,d)(a\,b\,c)^2(a\,b\,d)^{-1} = (b\,c\,d) = (d\,b\,c) \in N$. In this way we may show that any cycle of length 3 lies in N, and hence $N = A_n$. □

11.4 Theorem. *The alternating group A_n is simple for any $n \geq 5$.*

Proof. Let N be a normal subgroup of A_n, $N \neq 1$. It is enough to check that N contains a cycle of length 3. Let $1 \neq \sigma \in N$ and let r be the greatest length of the cycles involved in the cycle decomposition of σ.

If $r \geq 4$, then $\sigma = (a_1\,a_2\,\ldots\,a_r)\tau$, where τ is "disjoint" to $(a_1\,a_2\,\ldots\,a_r)$. Then, as $[\sigma,\gamma] = \sigma(\gamma\sigma^{-1}\gamma^{-1}) \in N$ for any $\gamma \in A_n$, we get

$$\begin{aligned}[\sigma,(a_1\,a_2\,a_3)] &= \sigma(a_1\,a_2\,a_3)\sigma^{-1}(a_1\,a_2\,a_3)^{-1} = (\sigma(a_1)\,\sigma(a_2)\,\sigma(a_3))(a_1\,a_3\,a_2)\\ &= (a_2\,a_3\,a_4)(a_1\,a_3\,a_2) = (a_1\,a_4\,a_2) \in N.\end{aligned}$$

If $r = 3$ and σ contains at least two disjoint cycles of length 3, then $\sigma = (a\,b\,c)(d\,e\,f)\tau$, then

$$[\sigma,(a\,b\,d)] = (\sigma(a)\,\sigma(b)\,\sigma(d))(a\,d\,b) = (b\,c\,e)(a\,d\,b) = (a\,d\,c\,e\,b) \in N,$$

and the argument for $r \geq 4$ works.

If $r = 3$ and σ contains exactly one cycle of length 3: $\sigma = (a\,b\,c)\tau$ and $\tau^2 = 1$, then $\sigma^2 = (a\,c\,b) \in N$.

Finally, if $r = 2$, then $\sigma = (a\,b)(c\,d)\tau$, where τ is a product of an even number (possibly 0) of transpositions. Then

$$[\sigma,(a\,b\,c)] = (\sigma(a)\,\sigma(b)\,\sigma(c))(a\,c\,b) = (b\,a\,d)(a\,c\,b) = (a\,c)(b\,d) \in N,$$

and since $n \geq 5$,

$$[(a\,c\,e),(a\,c)(b\,d)] = (c\,e)(b\,d)(a\,c)(b\,d) = (a\,e\,c) \in N.$$ □

11.5 Corollary. *The symmetric group S_n, for $n \geq 5$, is not solvable.*

Proof. We know that $S_n' = A_n$. Since A_n is simple and it is not abelian, its derived subgroup is $A_n' = A_n$. And hence the derived series of S_n is just $S_n \trianglerighteq A_n$. □

Exercises

1. Let G be a *semigroup*, that is, a nonempty set with a binary operation which is associative. Assume that the following two conditions hold:
   (a) There exists an element $e \in G$ such that $ex = x$ for any $x \in G$ (a left neutral element),
   (b) For any $x \in G$ there is an element $y \in G$ such that $yx = e$ (a left inverse).
   Prove that G is a group.

2. Let G be a semigroup containing a left neutral element e and such that any element has a right inverse (relative to e). Is G a group?

3. Let G be a group such that $g^2 = 1$ for any $g \in G$. Prove that G is abelian.

4. Let S be the subgroup of the cyclic group of order 154: $C_{154} = \langle x \rangle$, generated by $\{x^{28}, x^{88}\}$. Find a natural number n such that $S = \langle x^n \rangle$.

5. Let $G = \langle x \rangle$ be an infinite cyclic group. Prove that any nontrivial subgroup of G is an infinite cyclic group of finite index generated by x^n for some $n \in \mathbb{N}$.

6. Let $G \neq 1$ be a group containing no subgroup different from 1 and G. Prove that G is cyclic of prime order.

7. Let G be a cyclic group of order n. Compute the number of generators of G (that is, compute $|\{g \in G : \langle g \rangle = G\}|$).

8. Let G be a finite abelian group of order n, and let $m = \max\{|g| \mid g \in G\}$.
   (a) Prove that m divides n and that G is cyclic if and only if $m = n$.
   (b) Show that the order of any element of G divides m.
   (c) Let p be a prime number, prove that the multiplicative group $\mathbb{Z}_n^\times$ is cyclic.

9. Let C_n be a cyclic group of order n and let $m \in \mathbb{N}$. Prove that the map $\alpha_m : C_n \to C_n$ such that $x \mapsto x^m$ for any $x \in C_n$ is an automorphism if and only if $\gcd(m, n) = 1$. Prove that $\operatorname{Aut} C_n$ is an abelian group of order $\phi(n)$. Compute $\operatorname{Int} C_n$.

10. Consider the elements $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ in $GL_2(\mathbb{Z})$. Prove that A has order 4, B has order 3, while the order of AB is infinite.

11. Give an example of a nonabelian finite group such that all its proper subgroups are cyclic (respectively normal).

12. Consider the additive group $\mathbb{Q}$ of the rational numbers.
   (a) Is it cyclic?
   (b) Take any two elements $x, y \in \mathbb{Q}$, is $\langle x, y \rangle$ cyclic?

[9] Recall that $\phi(n)$ denotes the Euler map: $\phi(n) = |\{1 \leq m \leq n : \gcd(m, n) = 1\}|$.

(c) What is the answer to the two previous questions if we substitute $\mathbb{Q}$ by the multiplicative group $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$?

13. Let x, y, z be elements of a group G. Are the following assertions true? Why?
    (a) The elements x, x^{-1}, $x^y = yxy^{-1}$ have the same order.
    (b) xy and yx have the same order.
    (c) xyz and zyx have the same order.

14. Prove that, up to isomorphism, the only groups of order 4 are C_4 and $C_2 \times C_2$.

15. Let G be a group such that $G/Z(G)$ is cyclic. Prove that G is abelian.

16. Let G be an abelian group. Prove that the set of finite order elements of G is a subgroup of G.

17. Let H and K be two subgroups of a group G.
    (a) Prove that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.
    (b) Let $HK = \{xy : x \in H,\, y \in K\}$. Give an example showing that, in general, HK is not a subgroup of G.
    (c) Prove that HK is a subgroup of G if and only if $HK = KH$.

18. Prove that the set of matrices $\left\{ \begin{pmatrix} \lambda & -\mu \\ \mu & \lambda \end{pmatrix} : \lambda, \mu \in \mathbb{R},\ (\lambda, \mu) \neq (0,0) \right\}$ is a multiplicative group isomorphic to $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

19. Prove, without the use of group actions, that any index two subgroup of a group G is normal.

20. Let $\Phi : G_1 \to G_2$ be a group homomorphism, and let N be a normal subgroup of G_1 and K a subgroup of G_2.
    (a) Is $\Phi(N)$ a normal subgroup of G_2?
    (b) Is $\Phi^{-1}(K) = \{x \in G_1 : \Phi(x) \in K\}$ a subgroup of G_1?
    (c) If K is normal, is $\Phi^{-1}(K)$ a normal subgroup of G_1?

21. Find the order of H, where:
    (a) H is the subgroup of S_3 generated by $\{(1\,2), (1\,3)\}$.
    (b) H is the subgroup of S_5 generated by $\{(1\,2), (1\,3)(4\,5)\}$

22. Prove that S_n is generated by $(1\,2)$ and $(1\,2\,\ldots\,n)$.

23. Find abelian and nonabelian order 6 subgroups of S_6.

24. Prove that for any $n \geq 3$, the center of S_n is trivial.

25. Compute the centralizer of the element $(1\,2\,3\,4)$ in S_4. How many conjugates does this element have in S_4?

26. Compute the center of $GL_2(\mathbb{Z})$ $(= \{A \in \mathrm{Mat}_2(\mathbb{Z}) : \exists B \in \mathrm{Mat}_2(\mathbb{Z}) \text{ such that } AB = I_2 = BA\})$.

27. Consider the dihedral group D_6 of isometries of the euclidean plane which fix a regular hexagon.

    (a) Prove that this group is generated by the clockwise rotation x of angle $\frac{\pi}{3}$ and by the reflection y through two opposite vertices.

    (b) Show that $x^6 = 1 = y^2$ and $yx = x^{-1}y$.

    (c) Show that $D_6 = \{x^n y^m : 0 \leq n < 6,\ 0 \leq m < 2\}$.

28. Let G be a finite group generated by two different elements of order 2. Prove that G is isomorphic to $C_2 \times C_2$ or to D_n for some $n \geq 3$.

29. Compute $\mathrm{Aut}\, D_n$ $(n \geq 3)$.

30. Prove that the multiplicative group $G_n = \left\{ \left(\begin{smallmatrix} \pm 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right) : \lambda \in \mathbb{Z}_n \right\}$ is isomorphic to D_n.

31. Prove that the only groups of order 6 are, up to isomorphism, C_6 and D_3.

32. Prove that the only nonabelian groups of order 8 are, up to isomorphism, D_4 and the quaternion group.

33. Prove that A_4 has no order 6 subgroups.

34. How many different bracelets can be done with 3 red beads and 4 green beads?

35. Let the order of a group G be a product of two prime numbers $p > q$. Prove that either G is abelian or $q \,|\, p - 1$.

36. Let G be a group with order $2p$ for an odd prime number p. Prove that either G is cyclic or isomorphic to the dihedral group D_p.

37. Compute, up to isomorphism, the groups of order 21.

38. Compute, up to isomorphism, the groups of order 12.

39. Let G be a nonabelian group of order p^3 for a prime number p. Prove that G' equals $Z(G)$.

---

[27] It can be checked that any equation satisfied by x and y is a consequence of the equations in (ii). This allows us to write

$$D_6 = \langle x, y : x^6 = y^2 = 1,\ yx = x^{-1}y \rangle.$$

This is a *presentation by generators and relations* of D_6. These presentations constitute a very useful way to define groups.

The formal definition of these presentations require the definition of *free groups*, which will not be given in this course.

[28] Let u and v be the two order 2 generators. If $uv = vu$, then show that $G \cong C_2 \times C_2$. Otherwise, show that G is generated by $x = uv$ and $y = v$, and that these elements satisfy the relations of the generators of a dihedral group.

40. For $n \geq 3$, let $D_n = \langle x, y : x^n = y^2 = 1,\ yx = x^{-1}y \rangle$ be the dihedral group of degree n.
    (a) Prove that $Z(D_n) = 1$ for odd n, but $Z(D_n) = \langle x^{\frac{n}{2}} \rangle$ for even n.
    (b) Prove that $D_n' = \langle x^2 \rangle$ (which is equal to $\langle x \rangle$ for odd n).

41. Let H be a subgroup of a simple nonabelian group G of index $m \geq 5$. Prove that G is isomorphic to a subgroup of A_m.

42. Let G be a finite group of order $2m$ for an odd $m > 1$. Prove that G is not simple.

43. Prove that there are no simple groups of order 56, 80, 84, 132, 300 or 1000.

44. Prove that, up to isomorphism, the only simple nonabelian group of order ≤ 60 is A_5.

45. Prove the following relations in any group G:

$$[x, y]^{-1} = [y, x],\ [x, yz] = [x, y](y[x, z]y^{-1}),\ [xy, z] = (x[y, z]x^{-1})[x, z].$$

46. Let H and K be subgroups of a group G. Define the commutator subgroup $[H, K]$ as

$$[H, K] = \langle [h, k] : h \in H,\ k \in K \rangle.$$

    Prove that $[H, K] = [K, H]$ and that H is a normal subgroup of G if and only if $[G, H] \leq H$.

47. The *lower central series* of a group G is defined by means of $L_0 = G$, $L_{n+1} = [G, L_n]$ for $n \geq 0$.
    (a) Prove that L_n is a normal subgroup of G for any n.
    (b) Show that we have indeed a descending series: $L_0 \trianglerighteq L_1 \trianglerighteq L_2 \trianglerighteq ....$
    (c) Prove that for any n, $L_n/L_{n+1} \leq Z(G/L_{n+1})$.
    (d) Prove that the group G is nilpotent if and only if $L_n = 1$ for some n.

48. Prove that subgroups, quotients and finite direct products of solvable (respectively nilpotent) groups are solvable (respectively nilpotent).

49. Give an example of a nonnilpotent group G with a normal subgroup N such that both N and G/N are nilpotent.

50. Give examples of nilpotent nonabelian groups and of solvable nonnilpotent groups.

51. Consider the following two groups:

$$G_1 = \langle x, y : x^5 = 1 = y^4,\ yx = x^3y \rangle,$$
$$G_2 = \langle x, y, z : x^{11} = 1 = z^3,\ [x, y] = 1,\ zx = yz,\ zy = x^{-1}y^{-1}z \rangle.$$

[42] Otherwise G would be isomorphic, through the action by left translation, to a subgroup of A_{2m}. Then argue with the possible expressions as a product of disjoint cycles of an order 2 element x of G, taking into account that the left multiplication by x does not fix any element of G.

(a) Compute their orders and the number of its Sylow subgroups.

(b) Describe these groups as semidirect products.

(c) Compute the derived subgroups, the centers, and the corresponding quotient groups.

(d) How many conjugacy classes do they contain?

(e) Study the solvability and nilpotency of these groups.

[51] The groups G_1' and G_1/G_1' are cyclic. The subgroup of G_1 generated by x and y^2 is a dihedral group. These facts, together with the number of Sylow subgroups, allows you to conclude that G_1 contains 5 elements of order 2 and that its center is trivial.
For G_2 consider the subgroup H generated by x and y, which is normal and abelian. Compute $[x, z]$ and $[y, z]$ and deduce from here G_2' and G_2/G_2'. Argue that $Z(G_2)$ cannot contain order 3 or 11 elements. Using Sylow subgroups, check that G can only contain elements of order 1, 3 or 11.

CHAPTER 2

GALOIS THEORY

We will start this chapter by recalling in the first section some concepts you should already know.

§ 1. Algebraic extensions

1.1. Let F be a field with unity $1_F = 1$. Consider the map:

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow F \\ n &\mapsto n1 = 1 + \overset{n}{\cdots} + 1 \quad (n \in \mathbb{N}) \\ 0 &\mapsto 0 \\ -n &\mapsto -n1 = (-1) + \overset{n}{\cdots} + (-1) \quad (n \in \mathbb{N}) \end{aligned}$$

Then φ is a ring homomorphism and there are two possibilities:

1. $\ker \varphi = 0$ (that is, φ is a monomorphism). Then φ extends to a monomorphism

$$\begin{aligned} \psi : \mathbb{Q} &\longrightarrow F \\ \frac{m}{n} &\mapsto \varphi(m)\varphi(n)^{-1} \end{aligned}$$

since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. In this case, it is said that the *characteristic of F is* 0 and $\mathbb{Q}$ is identified with its image under ψ, which is the smallest subfield of F and it is called the *prime subfield* of F.

2. $\ker \varphi = p\mathbb{Z}$ for some $p \in \mathbb{N}$, so that φ induces a monomorphism

$$\begin{aligned} \bar{\varphi} : \mathbb{Z}/p\mathbb{Z} &\longrightarrow F \\ n + p\mathbb{Z} &\mapsto \varphi(n) = n1. \end{aligned}$$

Since F has no zero divisors, neither does $\mathbb{Z}/p\mathbb{Z}$, so that p is a prime number, which is called the *characteristic* of F. In this case the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is identified with its image under $\bar{\varphi}$, which again is the smallest subfield of F and called the *prime subfield* of F.
Notice that p is the smallest natural number such that $p1 = 0$ and that for any $\alpha \in F$

$$p\alpha = \alpha + \overset{p}{\cdots} + \alpha = (1 + \overset{p}{\cdots} + 1)\alpha = 0\alpha = 0$$

1.2 Examples.

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields of characteristic 0.
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, for a prime number p, is a field of characteristic p, and so is $\mathbb{F}_p(X)$ (the fraction field of $\mathbb{F}_p[X]$).

1.3. Let K/F be a field extension, then $1_K = 1_F$ and the characteristics of F and K coincide. Moreover, K is a vector space over F in a natural way. Its dimension $\dim_F K$ is called the *degree* of the extension and it is denoted by $[K : F]$. If it is finite, then K/F is said to be a *finite extension*.

The most important example. Let F be a field and $f(X) \in F[X]$ be an irreducible polynomial. Then $\big(f(X)\big)$ is a maximal ideal, so that $K = F[X]/\big(f(X)\big)$ is a field. We may view F as a subfield of K by means of the map $F \hookrightarrow K$, $a \mapsto a + \big(f(X)\big)$. Take the element $\theta = X + \big(f(X)\big) \in K$ and assume that $f(X) = a_0 + a_1X + \cdots + a_nX^n$ with $a_n \neq 0$. Then θ is trivially a root of $f(X)$ in K, because

$$\begin{aligned} f(\theta) &= a_0 + a_1\theta + \cdots + a_n\theta^n \\ &= a_0 + a_1(X + \big(f(X)\big)) + \cdots + a_n(X + \big(f(X)\big))^n \\ &= a_0 + a_1X + \cdots + a_nX^n + \big(f(X)\big) \\ &= f(X) + \big(f(X)\big) = 0. \end{aligned}$$

Moreover, $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of K as a vector space over F. In particular, $[K : F] = \deg f(X)$.

Proof. Let us show first that $\{1, \theta, \ldots, \theta^{n-1}\}$ is free. Assume that there are scalars $b_0, \ldots, b_{n-1} \in F$ such that $b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$. As before,

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = (b_0 + b_1X + \cdots + b_{n-1}X^{n-1}) + \big(f(X)\big),$$

so that we conclude that $b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \in \big(f(X)\big)$. That is, $f(X)$ divides $b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$ and this is only possible if $b_0 = \cdots = b_{n-1} = 0$.

To show that $\{1, \theta, \ldots, \theta^{n-1}\}$ is a spanning set, take an arbitrary element $g(X) + \big(f(X)\big) \in K$. Since $F[X]$ is an euclidean domain, there are polynomials $c(X), r(X) \in F[X]$ with $\deg r(X) \leq n-1$ such that $g(X) = c(X)f(X) + r(X)$. If $r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1}$, then

$$g(X) + \big(f(X)\big) = r(X) + \big(f(X)\big) = r_01 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}$$

is a linear span with coefficients in F of the elements in $\{1, \theta, \ldots, \theta^{n-1}\}$, as required. □

Therefore,

$$\begin{aligned} K = F[X]/(f(X)) &= F1 + \cdots + F\theta^{n-1} \\ &= \{r(\theta) : r(X) \in F[X] \text{ and } \deg r(X) < n\}, \end{aligned}$$

and the operations in K are given by:

$$\begin{cases} r_1(\theta) + r_2(\theta) = (r_1 + r_2)(\theta), \\ r_1(\theta) r_2(\theta) = r(\theta), \end{cases}$$

for $r_1(X), r_2(X) \in F[X]$ of degree at most $n-1$, and where $r(X)$ is the remainder of the division of $r_1(X)r_2(X)$ by $f(X)$.

Let us consider a couple of examples:

- $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$.
- The polynomial $X^3 - 2 \in \mathbb{Q}[X]$ is irreducible (Eisenstein's criterion). Let $K = \mathbb{Q}[X]/(X^3-2)$ and $\theta = X + (X^3 - 2)$. Then $K = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q}\}$, $\theta^3 = 2$, $\theta^4 = 2\theta$. Therefore, the multiplication in K is given by:

$$\begin{aligned} &(a + b\theta + c\theta^2)(a' + b'\theta + c'\theta^2) \\ &\qquad = (aa' + 2bc' + 2cb') + (ab' + ba' + 2cc')\theta + (ac' + ca' + bb')\theta^2. \end{aligned}$$

  If we want to compute $(1+\theta)^{-1}$, we proceed as follows: since $X^3 - 2$ is irreducible, $\gcd(X^3 - 2, X + 1) = 1$ and we compute the coefficients of Bezout's identity to get:

$$1 = -\frac{1}{3}(X^3 - 2) + \frac{1}{3}(X^2 - X + 1)(X + 1),$$

  so that $1 = (\theta + 1)\dfrac{\theta^2 - \theta + 1}{3}$. Therefore, $(1 + \theta)^{-1} = \dfrac{\theta^2 - \theta + 1}{3}$.

1.4. Let K/F be a field extension and let $\alpha \in K$. The evaluation map:

$$\begin{aligned} \psi : F[X] &\longrightarrow K \\ f(X) &\mapsto f(\alpha) \end{aligned}$$

is a ring homomorphism and there are two possibilities:

1. $\ker \psi = 0$. In this case there is no nonzero polynomial in $F[X]$ for which α is a root, and ψ extends to a ring monomorphism $F(X) \hookrightarrow K$, whose image is $F(\alpha)$. In particular, $[F(\alpha) : F] = [F(X) : F] \geq \dim_F F[X] = \infty$. Then α is said to be *transcendental* over F. (Here, and in what follows, given a subset S of K, $F(S)$ denotes the smallest subfield of K containing both F and S.)

2. $\ker\psi \neq 0$. Since $F[X]$ is a principal ideal domain and $\operatorname{im}\psi$ is an integral domain (it is a subring of the field K), $\ker\psi = (m(X))$ for a unique monic irreducible polynomial $m(X) \in F[X]$. Hence any polynomial $f(X) \in F[X]$ with $f(\alpha) = 0$ is a multiple of $m(X)$. Hence $m(X)$ is the monic polynomial of lowest degree that annihilates α. The polynomial $m(X)$ is called the *minimal polynomial* of α over F and it is denoted by $m_{\alpha,F}(X)$. In this case, α is said to be *algebraic* over F. Note that $F(\alpha)$ is isomorphic to $F[X]/(m_{\alpha,F}(X))$ and hence $[F(\alpha) : F] = \deg m_{\alpha,F}(X)$.
The extension field K/F is said to be *algebraic* if for any $\alpha \in K$, α is algebraic over F.

Examples.

- $\mathbb{C}/\mathbb{R}$ is algebraic, because for any $\alpha = a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$, α is a root of $(X - \alpha)(X - \bar{\alpha}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$.
- $\mathbb{Q}(X)/\mathbb{Q}$ is not algebraic.

1.5 Example. (Quadratic extensions)
Let K/F be a field extension with $[K : F] = 2$ and assume that the characteristic of F is $\neq 2$. Then any $\alpha \in K \setminus F$ is a root of a polynomial $X^2 + bX + c \in F[X]$. But

$$X^2 + bX + c = \left(X - \frac{b}{2}\right)^2 - \frac{b^2 - 4c}{4},$$

so that $\beta = 2\alpha - b\,(\in K \setminus F)$ satisfies $\beta^2 = b^2 - 4c \in F$. With $D = b^2 - 4c$ this shows that the minimal polynomial of β is $X^2 - D$. Since $[F(\beta) : F] = 2$, necessarily $K = F(\beta) = F(\sqrt{D})$.

1.6 Corollary. *Let K/F be a field extension and $\alpha \in K$. Then α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.*

1.7 Corollary. *Any field extension K/F with $[K : F] < \infty$ is algebraic.*

1.8 Proposition. *Let K/F and L/K be two field extensions. Then*

$$[L : F] = [L : K][K : F].$$

Proof. Let $\{\beta_i : i \in I\}$ be a basis of L over K and let $\{\alpha_j : j \in J\}$ be a basis of K over F. Then, any $\gamma \in L$ can be written uniquely as

$$\gamma = b_1\beta_{i_1} + \cdots + b_r\beta_{i_r},$$

with $b_1, \ldots, b_r \in K$, and each b_h can be written uniquely as

$$b_h = a_{h,1}\alpha_{j_1} + \cdots + a_{h,s}\alpha_{j_s},$$

with $a_{h,1}, \ldots, a_{h,s} \in F$. Therefore, γ can be written uniquely as $\gamma = \sum a_{h,k}\alpha_{j_k}\beta_{i_h}$. Hence $\{\alpha_j\beta_i : I \in I, j \in J\}$ is a basis of L over F. Thus,

$$[L : F] = |I||J| = [L : K][K : F].$$ □

1.9 Example. Consider the field extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. Then

$$\mathbb{Q} \underset{(\sqrt{2}\notin\mathbb{Q})}{\subsetneq} \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \,(\subseteq \mathbb{R}).$$

Now, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since $m_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$ (irreducible by Eisenstein's criterion). Also, $\sqrt{3}$ is a root of $X^2 - 3 \in \mathbb{Q}[X] \subseteq \mathbb{Q}(\sqrt{2})[X]$, so $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(X) \mid X^2 - 3$, and either $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, or $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})$, that is, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. But in the latter case, there would exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$, so $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. Since $\sqrt{2} \notin \mathbb{Q}$, this last equation forces either $a = 0$ or $b = 0$. But $b = 0$ would imply $\sqrt{3} \in \mathbb{Q}$, which is not true, while $a = 0$ implies $\sqrt{6} = 2b \in \mathbb{Q}$, again a contradiction. Therefore, $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4.$$

Moreover, $\{1, \sqrt{2}\}$ is a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $\{1, \sqrt{3}\}$ is a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ (because $\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(X) = 2$). By the argument in the previous proof, it follows that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$.

1.10 Theorem. *Let K/F be a field extension. Then $[K : F] < \infty$ if and only if there are $r \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_r \in K$, all of them algebraic over F, such that $K = F(\alpha_1, \ldots, \alpha_r)$.*

In this case, if $\deg m_{\alpha_i,F}(X) = n_i$ for any $i = 1, \ldots, r$, then $[K : F] \leq n_1 \cdot \cdots \cdot n_r$.

Proof. If $[K : F] < \infty$ and $\{\alpha_1, \ldots, \alpha_r\}$ is a basis of K over F, then for any $i = 1, \ldots, r$, $[F(\alpha_i) : F] \leq [K : F] < \infty$, so that α_i is algebraic over F and, evidently, $K = F(\alpha_1, \ldots, \alpha_r)$.

Now, assume that we have $K = F(\alpha_1, \ldots, \alpha_r)$ with α_i algebraic over F for any i, and let $\deg m_{\alpha_i,F}(X) = n_i$. Thus, $m_{\alpha_r,F}(X)$ is a polynomial in $F(\alpha_1, \ldots, \alpha_{r-1})[X]$ which 'kills' α_r, and therefore $m_{\alpha_r,F(\alpha_1,\ldots,\alpha_{r-1})}(X)$ divides $m_{\alpha,F}(X)$ in $F(\alpha_1, \ldots, \alpha_{r-1})[X]$. Hence we get $[K : F(\alpha_1, \ldots, \alpha_{r-1})] \leq n_r$. By an easy induction argument on r we conclude that

$$\begin{aligned}[K : F] &= [K : F(\alpha_1, \ldots, \alpha_{r-1})][F(\alpha_1, \ldots, \alpha_{r-1}) : F] \\ &\leq n_r \cdot (n_1 \cdot \cdots \cdot n_{r-1}) = n_1 \cdot \cdots \cdot n_r < \infty.\end{aligned}$$

□

1.11 Corollary. *Let K/F be a field extension and let $\alpha, \beta \in K$ be two algebraic elements over F. Then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$ (if $\beta \neq 0$) are algebraic over F too.*

In particular, the set $\{\gamma \in K : \gamma$ is algebraic over $F\}$ is a subfield of K which contains F.

Proof. From the Theorem above we conclude that $[F(\alpha, \beta) : F] < \infty$, and therefore the field extension $F(\alpha, \beta)/F$ is algebraic. Now everything follows since the elements $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$ (if $\beta \neq 0$) are all in $F(\alpha, \beta)$. □

1.12 Corollary. *If K/F and L/K are algebraic field extensions, so is L/F.*

Proof. Let $\alpha \in L$ and assume $m_{\alpha,K}(X) = b_0 + b_1X + \cdots + b_{n-1}X^{n-1} + X^n$, with $b_0, \ldots, b_{n-1} \in K$. Thus α is algebraic over the subfield $F(b_0, \ldots, b_{n-1})$ of K, and hence $[F(b_0, \ldots, b_{n-1}, \alpha) : F(b_0, \ldots, b_{n-1})] < \infty$. But $b_0, \ldots, b_{n-1}$ are all algebraic over F, since they all belong to K and K/F is algebraic. Thus, by the Theorem above $[F(b_0, \ldots, b_{n-1}) : F] < \infty$. Hence,

$$[F(b_0, \ldots, b_{n-1}, \alpha) : F] = [F(b_0, \ldots, b_{n-1}, \alpha) : F(b_0, \ldots, b_{n-1})][F(b_0, \ldots, b_{n-1}) : F] < \infty,$$

so that $F(b_0, \ldots, b_{n-1}, \alpha)/F$ is an algebraic field extension and, in particular, α is algebraic over F. □

§ 2. Splitting fields. Algebraic closure

The definition and first properties of splitting fields were considered too in *Algebraic Structures*.

2.1 Definition. Let F be a field and $0 \neq f(X) \in F[X]$. A field extension K of F is said to be a *splitting field* of $f(X)$ over F if, as a polynomial in $K[X]$, it *splits*, that is:

$$f(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$$

where $a \in F$ (since it is the leading coefficient of $f(X)$), $\alpha_1, \ldots, \alpha_n \in K$, and $K = F(\alpha_1, \ldots, \alpha_n)$.

2.2 Examples.

- $\mathbb{C}$ is a splitting field of $X^2 + 1 \in \mathbb{R}[X]$.
- $\mathbb{Q}(\sqrt{2})$ is a splitting field of $X^2 - 2$ over $\mathbb{Q}$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $(X^2 - 2)(X^2 - 3)$ over $\mathbb{Q}$.
- The splitting field of $X^3 - 2$ over $\mathbb{Q}$ is not $\mathbb{Q}(\sqrt[3]{2})$, because the roots (in $\mathbb{C}$) of $X^3 - 2$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where $\omega = \frac{-1+i\sqrt{3}}{2}$ is a cubic root of 1. Note that if $\sqrt[3]{2}$ and ω are in a field K containing $\mathbb{Q}$, then so is $i\sqrt{3} = \sqrt{-3}$. Then $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is a splitting field of $X^3 - 2$ over $\mathbb{Q}$. Since $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$, because $\sqrt{-3}$ is a root of $X^2 + 3$ and $K \neq \mathbb{Q}(\sqrt[3]{2})\,(\subseteq \mathbb{R})$, we get $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6$.

2.3 Proposition. *Let K be a splitting field of a polynomial $f(X)$ of degree n over a field F. Then $[K : F] \leq n!$.*

Proof. In case $\deg f(X) = 1$, then $K = F$ and $[K : F] = 1 = 1!$.

Now, if $\deg f(X) = n > 1$ and $\alpha \in K$ is a root of $f(X)$, then $f(X) = (X - \alpha)g(X)$ for some $g(X) \in F(\alpha)[X]$ of degree $n - 1$. Then K is a splitting field too of $g(X)$ over $F(\alpha)$, so by an inductive argument we get

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] \leq (n-1)! \times n = n!$$ □

Our next goal is to recall that there always exist splitting fields of polynomials and that, up to isomorphism, they are unique.

2.4 Lemma. *Let $\varphi : F \to \hat{F}$ be a field isomorphism, $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ an irreducible polynomial, $\hat{f}(X) = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n \in \hat{F}[X]$ (which is irreducible too), α a root of $f(X)$ in some field extension of F and β a root of $\hat{f}(X)$ in some field extension of $\hat{F}$. Then there exists a field isomorphism $\sigma : F(\alpha) \to \hat{F}(\beta)$ such that $\sigma|_F = \varphi$ and $\sigma(\alpha) = \beta$.*

Proof. It is enough to concatenate the following isomorphisms:

$$\begin{array}{ccccccc} F(\alpha) & \cong & F[X]/(f(X)) & \cong & \hat{F}[X]/(\hat{f}(X)) & \cong & \hat{F}(\beta) \\ a \in F & \hookleftarrow & a + (f(X)) & \mapsto & \varphi(a) + (\hat{f}(X)) & \rightarrowtail & \varphi(a) \\ \alpha & \hookleftarrow & X + (f(X)) & \mapsto & X + (\hat{f}(X)) & \rightarrowtail & \beta \end{array} \qquad \square$$

2.5 Theorem. *Let F be a field and let $0 \neq f(X) \in F[X]$. Then:*

(i) *There exist splitting fields of $f(X)$ over F.*

(ii) *All of them are isomorphic. More precisely, if $\varphi : F \to \hat{F}$ is a field isomorphism, $\hat{f}(X)$ is the polynomial which results of applying φ to the coefficients of $f(X)$, E is a splitting field of $f(X)$ over F, and $\hat{E}$ a splitting field of $\hat{f}(X)$ over $\hat{F}$, then there is a field isomorphism $\sigma : E \to \hat{E}$ such that $\sigma|_F = \varphi$.*

Proof. For (i), we use induction of $\deg f(X)$. If $\deg f(X) \leq 1$, then F itself is a splitting field.

Now, if $\deg f(X) = n > 1$, we know that there exists a field extension of F which contains a root α_1 of some irreducible factor of $f(X)$. Let $K_1 = F(\alpha_1)$. Then, in $K_1[X]$, $f(X) = (X-\alpha_1)g(X)$, and $\deg g(X) = n-1$. By induction hypothesis, there exists a splitting field E of $g(X)$ over K_1. Hence, in $E[X]$, $g(X) = a(X-\alpha_2)\cdots(X-\alpha_n)$ for some $\alpha_2, \ldots, \alpha_n \in E$ and $E = K_1(\alpha_2, \ldots, \alpha_n)$. But then, in $E[X]$, $f(X) = (X-\alpha_1)g(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ and $E = K_1(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$; so that E is a splitting field of $f(X)$ over F.

Induction on $n = \deg f(X)$ will be used too for (ii). Again, if $n = 1$, then $E = F$ and $\hat{E} = \hat{F}$ because the roots (if any) of $f(X)$ (respectively $\hat{f}(X)$) are in F (respectively in $\hat{F}$). Hence $\sigma = \varphi$. Now, if $n > 1$, let $f_1(X)$ be an irreducible factor of $f(X)$ and let $\hat{f}_1(X)$ be the corresponding irreducible factor of $\hat{f}(X)$. Let $\alpha \in E$ be a root of $f_1(X)$ and $\beta \in \hat{E}$ a root of $\hat{f}_1(X)$. Thus $F \leq F(\alpha) \leq E$ and $\hat{F} \leq \hat{F}(\beta) \leq \hat{E}$ and, by the previous Lemma, there exists $\sigma_1 : F(\alpha) \to \hat{F}(\beta)$, a field isomorphism, extending φ and such that $\sigma_1(\alpha) = \beta$.

In $F(\alpha)[X]$, $f(X) = (X-\alpha)g(X)$, and in $\hat{F}(\beta)[X]$, $\hat{f}(X) = (X-\beta)\hat{g}(X)$, where $\hat{g}(X)$ is the quotient of $\hat{f}(X)$, which is the polynomial obtained from $f(X)$ by applying σ_1 to all its coefficients, by $(X-\beta)$, which is the polynomial obtained from $(X-\alpha)$ by applying σ_1 to all its coefficients. Therefore $\hat{g}(X)$ is the polynomial obtained from $g(X)$ by applying σ_1 to all its coefficients. Moreover, E is a splitting field of $g(X)$ over $F(\alpha)$ and $\hat{E}$ is a splitting field of $\hat{g}(X)$ over $\hat{F}(\beta)$ so, by the induction hypothesis, there exists a field isomorphism $\sigma : E \to \hat{E}$, such that $\sigma|_{F(\alpha)} = \sigma_1$, which implies that $\sigma|_F = \varphi$, as required. $\square$

2.6 Definition. A finite field extension K/F is said to be *normal* if there is a polynomial $f(X) \in F[X]$ such that K is the splitting field of $f(X)$ over F.

2.7 Theorem. *Let K/F be a finite field extension, then the following are equivalent:*

- *K/F is normal,*
- *For any $\alpha \in K$, $m_{\alpha,F}(X)$ splits in $K[X]$. (In other words, K contains all the roots of $m_{\alpha,F}(X)$.)*

Proof. Assume first that $m_{\alpha,F}(X)$ splits for any $\alpha \in K$, and write $K = F(\alpha_1, \ldots, \alpha_r)$. Then K is the splitting field of the polynomial $\prod_{i=1}^{r} m_{\alpha_i,F}(X)$ over F, and hence K/F is normal.

Conversely, if K is the splitting field of a polynomial $f(X) \in F[X]$, for an arbitrary $\alpha \in K$ take a splitting field L of $m_{\alpha,F}(X)$ over K. Hence L is a splitting field of the polynomial $m_{\alpha,F}(X)f(X)$ over F and $F \subseteq K \subseteq L$. Let $\beta \in L$ be a root of $m_{\alpha,F}(X)$. Then the isomorphism $\tau : F(\alpha) \to F(\beta)$, such that $\tau|_F = 1$ and $\tau(\alpha) = \beta$, extends to an automorphism σ of L. But σ permutes the roots of $f(X) \in F[X]$, and hence $\sigma(K) = K$. It follows that $\beta = \sigma(\alpha)$ is in K, and hence K contains all the roots of $m_{\alpha,F}(X)$. □

2.8 Definition. Let K/F be a field extension. Then K is said to be an *algebraic closure* of F if K/F is an algebraic field extension and any polynomial $f(X) \in F[X]$ with $\deg f(X) \geq 1$ splits in $K[X]$.

2.9 Definition. A field F is said to be *algebraically closed* if any polynomial of degree ≥ 1 over F has a root in F. (That is to say, the irreducible polynomials in $F[X]$ are the degree 1 polynomials.)

2.10 Example. $\mathbb{C}$ is algebraically closed by the Fundamental Theorem of Algebra (proved in *Algebraic Structures*) and hence it is an algebraic closure of $\mathbb{R}$.

2.11 Theorem. *Let F be a field.*

(i) *If $\bar{F}$ is an algebraic closure of F, then $\bar{F}$ is algebraically closed.*

(ii) *There exists an algebraically closed field extension K of F.*

(iii) *If K is an algebraically closed field extension of F, then $\bar{F} = \{\alpha \in K : \alpha$ is algebraic over $F\}$ is an algebraic closure of F.*

(iv) *Up to isomorphisms of field extensions, there is a unique algebraic closure of F.*

Proof. For the first part let $f(X) \in \bar{F}[X]$ be a monic polynomial, $\deg f(X) \geq 1$, and let α be a root of $f(X)$ in some field extension L of $\bar{F}$. Then α is algebraic over $\bar{F}$ and $\bar{F}/F$ is algebraic, so that α is algebraic over F. But $m_{\alpha,F}(X) \in F[X]$ factors over $\bar{F}$ as a product of degree 1 polynomials: $m_{\alpha,F}(X) = (X - \alpha_1) \cdots (X - \alpha_r)$, with $\alpha_1, \ldots, \alpha_r \in \bar{F}$. Since $0 = m_{\alpha,F}(\alpha) = \prod_{i=1}^{r}(\alpha - \alpha_i)$ in L, it follows that there is an i such that $\alpha = \alpha_i$, and thus $\alpha \in \bar{F}$, as required.

For the second part we will follow the proof by Artin. For each monic polynomial $f(X) \in F[X]$ of degree ≥ 1, let X_f be a variable, and consider the ring R of polynomials in the variables X_f with coefficients in F. Let I be the ideal generated by the set

$$\{f(X_f) : f(X) \in F[X], \text{ monic of degree} \geq 1\}.$$

In case $I = R$, then $1 \in I$, so that there are monic degree ≥ 1 polynomials $f_1(X), \ldots, f_r(X)$ and polynomials $g_1, \ldots, g_r$ in in the variables X_f's such that $1 = g_1 f_1(X_{f_1}) + \cdots + g_r f_r(X_{f_r})$. Rename the variables $X_{f_1} = X_1, \ldots, X_{f_r} = X_r$, and denote by $X_{r+1}, \ldots, X_n$ the remaining variables appearing in the g_i's. Then we have:

$$1 = g_1(X_1, \ldots, X_n)f_1(X_1) + \cdots + g_r(X_1, \ldots, X_n)f_r(X_r). \tag{2.12}$$

Let F' be a splitting field of $f_1(X)\cdots f_n(X)$ over F. In F' there are elements α_i such that $f_i(\alpha_i)=0$ for $i=1,\ldots,r$. Then evaluate equation (2.12) with $X_i\mapsto\alpha_i$, for $i=1,\ldots,r$, and $X_i\mapsto 0$, for $i=r+1,\ldots,n$, to get $1=0$, a contradiction.

Therefore the ideal I is not the whole R. Let M be a maximal ideal of R containing I, and consider the field $K_1=R/M$. K_1 is a field extension of F through the embedding $\iota:F\to R/M$, $a\mapsto a+M$, and if $x_f=X_f+M$ for any monic polynomial of degree ≥ 1, x_f is a root of $f(X)$ over K_1. Thus K_1 contains a root for each monic polynomial in $F[X]$ of degree ≥ 1. We repeat the process with K_1 to get a field extension K_2 of K_1 such that any degree ≥ 1 monic polynomial in $K_1[X]$ has a root in K_2, and then we repeat the process with K_2, ... Eventually we get a chain

$$F=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_n\subseteq K_{n+1}\subseteq\cdots$$

where any degree ≥ 1 monic polynomial in $K_n[X]$ has a root in K_{n+1} for any $n\geq 0$. Consider $K=\cup_{n=0}^{\infty}K_n$, which is a field extension of F. Also, given any degree ≥ 1 monic polynomial $h(X)\in K[X]$, there is an $n\in\mathbb{N}$ such that $h(X)\in K_n[X]$, and hence $h(X)$ has a root in $K_{n+1}\subseteq K$. Therefore, K is algebraically closed.

Now the third part of the Theorem is easy. $\bar{F}$ is a subfield of K containing F, $\bar{F}/F$ is an algebraic field extension and if $f(X)\in F[X]$ is a polynomial of degree ≥ 1, then $f(X)=a(X-\alpha_1)\cdots(X-\alpha_r)$ with $a\in F$ and $\alpha_1,\ldots,\alpha_n\in K$. But then $\alpha_1,\ldots,\alpha_r\in\bar{F}$, as they are roots of $f(X)$, and hence algebraic over F.

Finally, because of items (ii) and (iii) there are algebraic closures of F. If K_1 and K_2 are two such algebraic closures, consider the set $\mathcal{S}$ consisting of all the triples (L_1,L_2,φ), where L_1 is a field extension of F contained in K_1, L_2 is a field extension of F contained in K_2 and $\varphi:L_1\to L_2$ is an F-isomorphism (that is, an isomorphism which restricts to the identity map of F). The set $\mathcal{S}$ is partially ordered with $(L_1,L_2,\varphi)\leq(L_1',L_2',\varphi')$ if $L_1\subseteq L_1'$, $L_2\subseteq L_2'$ and $\varphi=\varphi'|_{L_1}$. Besides, any chain has an upper bound (obtained as the union of the first and second components, and the natural isomorphism among these unions). By Zorn's Lemma, there exists a maximal element (L_1,L_2,φ) in $\mathcal{S}$. If $L_1\neq K_1$, take an element $\alpha\in K_1\setminus L_1$. Since α is algebraic over L_1, φ can be extended (as in the proof of Theorem 2.5) to an isomorphism from $L_1(\alpha)$ onto a subfield of K_2 containing L_2, a contradiction. Hence $L_1=K_1$, and similarly we prove that $L_2=K_2$. Therefore, K_1 and K_2 are isomorphic. □

§ 3. Separable extensions

3.1 Definition. Let $f(X)$ be a degree ≥ 1 polynomial over a field F. Then $f(X)$ is said to be *separable* if it does not have multiple roots (in a splitting field).

As proved in *Algebraic Structures*, under these circumstances:

$$f(X)\text{ is separable}\iff\gcd(f(X),f'(X))=1\iff\mathrm{D}(f(X))\neq 0,$$

where $\mathrm{D}(f(X))$ is the discriminant of $f(X)$.

Recall from *Algebraic Structures* that if $f(X) = a_0 + a_1X + \cdots + a_nX^n$ and $g(X) = b_0 + b_1X + \cdots + b_mX^m$ are polynomials over a field F with $n, m \geq 1$ (although we admit that a_n or b_m may be 0), then the *resultant* of $f(X)$ and $g(X)$ is the determinant of the *Sylvester matrix*:

$$\mathrm{Res}_{n,m}(f,g) = \underbrace{\left|\begin{array}{ccccccccccc} a_n & a_{n-1} & a_{n-2} & \dots & \dots & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & \dots & \dots & a_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_n & \dots & \dots & \dots & a_1 & a_0 & 0 \\ 0 & \dots & \dots & 0 & a_n & \dots & \dots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & \dots & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & \dots & \dots & b_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b_m & \dots & \dots & \dots & b_1 & b_0 & 0 \\ 0 & \dots & \dots & 0 & b_m & \dots & \dots & b_2 & b_1 & b_0 \end{array}\right|}_{n+m \text{ columns}} \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right\} n \text{ rows} \end{array}$$

If $\deg f(X) = n$ and $\deg g(X) = m$ (that is, if $a_n \neq 0 \neq b_m$), then we write simply $\mathrm{Res}(f,g)$.

The *discriminant* of the polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ of degree $n \geq 2$ ($a_n \neq 0$) is the scalar (in F)

$$\mathrm{D}(f) = (-1)^{\binom{n}{2}} a_n^{-1} \mathrm{Res}_{n,n-1}(f, f').$$

In case $f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$ in some field extension of F, then $\mathrm{D}(f) = \left(\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)\right)^2$. Note that $\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)$ may not belong to F, but its square is the discriminant, which does belong to F.

3.2 Examples.

- $X^{p^n} - X \in \mathbb{F}_p[X]$ is separable, because its derivative is -1.
- Over a field of characteristic 0 any irreducible polynomial is separable, as $\gcd\big(f(X), f'(X)\big) = 1$, since $f(X)$ is irreducible, and $0 \neq f'(X)$ is not a multiple of $f(X)$.
- Assume that F is a field of characteristic $p > 0$. The polynomial $f(X) = X^n - 1$ satisfies

$$f'(X) = nX^{n-1} = \begin{cases} 0 & \text{if } p \,|\, n, \\ \neq 0 & \text{if } p \nmid n, \end{cases}$$

  and hence, $f(X)$ is separable if and only if $p \nmid n$.
- Over a finite field (and hence of prime characteristic) any irreducible polynomial is separable. Actually, let F be a finite field of characteristic p, and let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be an irreducible polynomial over F ($a_n \neq 0$). If $f'(X) \neq 0$, we conclude as before that $f(X)$

is separable. Otherwise $f'(X) = 0$ and hence the powers of X which appear on $f(X)$ with a nonzero coefficient are of the form X^{ps} for some s. But $\varphi : F \to F$, $a \mapsto a^p$ is one-to-one and, since F is finite, it is a bijection. Hence, for any $a \in F$ there is a unique $b \in F$ with $b^p = a$. Hence

$$\begin{aligned} f(X) = a_0 + a_p X^p + \cdots + a_{rp} X^{rp} &= b_0^p + b_1^p X^p + \cdots + b_r^p X^{rp} \\ &= (b_0 + b_1 X + \cdots + b_r X^r)^p, \end{aligned}$$

for some $b_0, b_1, \ldots, b_r \in F$. But this is a contradiction with the irreducibility of $f(X)$.

3.3 Definition.

- Given a field extension K/F, an element $\alpha \in K$ is said to be *separable* over F if it is algebraic and $m_{\alpha,F}(X)$ is separable.
- A finite field extension K/F is said to be *separable* if any element of K is separable over F.
- A field F is said to be *perfect* if all its finite field extensions are separable.

3.4 Properties.

(i) *A field F is perfect if and only if any irreducible polynomial in $F[X]$ is separable.*

(ii) *The fields of characteristic 0 and the finite fields are perfect.*

(iii) *Let F be a field of characteristic p and let $F^p = \{\alpha^p : \alpha \in F\}$. (This is a subfield of F!) Then F is perfect if and only if $F = F^p$.*
Actually, if $F^p = F$, the same arguments as in the last example above show that F is perfect. Conversely, if F is perfect and $\alpha \in F$, take K a splitting field of $X^p - \alpha$ over F, and take a root β in K, so that $\beta^p = \alpha$ and $X^p - \alpha = X^p - \beta^p = (X - \beta)^p$ in $K[X]$. Since F is perfect, $m_{\beta,F}(X)$ is separable, but $m_{\beta,F}(X) \,|\, X^p - \alpha$. We conclude that $m_{\beta,F}(X) = X - \beta$ and $\beta \in F$. Hence $F = F^p$.

3.5 Example. $\mathbb{F}_p(X)$ is not a perfect field, because $X \notin (\mathbb{F}_p(X))^p$.

§ 4. Galois group

Let K be a field and let $\sigma : K \to K$ be an automorphism. The element $a \in K$ is *fixed* by σ if $\sigma(a) = a$. Note that we have $\sigma(1) = 1$, and hence $\sigma(m1) = m1$ for any $m \in \mathbb{Z}$. Hence any automorphism fixes the prime subfield of K.

4.1 Definition.

(i) Let K/F be a field extension. The *Galois group* of K/F is the group

$$\mathrm{Gal}(K/F) = \{\sigma \in \mathrm{Aut}\, K : \sigma(a) = a \ \forall a \in F\} \ (\leq \mathrm{Aut}\, K).$$

(ii) Let F be a field and let $0 \neq f(X) \in F[X]$ be a nonzero polynomial. Let E be the splitting field of $f(X)$ over F. Then $\mathrm{Gal}(E/F)$ is said to be the *Galois group of the polynomial* $f(X)$ *over* F.

4.2 Proposition. *Let K/F be a field extension, let $\alpha \in K$ be algebraic over F, and let σ be an element in* $\mathrm{Gal}(K/F)$. *Then $\sigma(\alpha)$ is a root of $m_{\alpha,F}(X)$. (That is, σ induces a permutation of the roots of $m_{\alpha,F}(X)$ which lie in K.)*

Proof. Assume $m_{\alpha,F}(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$, $a_i \in F$ for all $i = 0, \ldots, n-1$. Then $0 = m_{\alpha,F}(X) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n$, and hence, since $\sigma(a_i) = a_i$ for any i we get $0 = a_0 + a_1\sigma(\alpha) + \cdots a_{n-1}\sigma(\alpha)^{n-1} + \sigma(\alpha)^n$, so that $\sigma(\alpha)$ is a root too of $m_{\alpha,F}(X)$. □

4.3 Examples.

(i) Take $K = \mathbb{Q}(\sqrt{2})$. Then any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ satisfies $\tau(\sqrt{2}) = \pm\sqrt{2}$, since $\tau(\sqrt{2})$ is a root of $X^2 - 2$. Therefore $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$, where 1 denotes the identity automorphism and σ is given by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Therefore $\mathrm{Gal}(K/\mathbb{Q})$ is the cyclic group of two elements.

(ii) Now let $K = \mathbb{Q}(\sqrt[3]{2})$. Since $m_{\sqrt[3]{2},\mathbb{Q}}(X) = X^3 - 2$ and the other two roots of this polynomial are not in K, we conclude that $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, and hence $\mathrm{Gal}(K/\mathbb{Q}) = 1$.

The proofs of the following two propositions are straightforward.

4.4 Proposition. *Let K be a field and let H be a subgroup of* $\mathrm{Aut}\, K$. *Then $K^H = \{a \in K : \sigma(a) = a \ \forall \sigma \in H\}$ is a subfield of K, which is called the* fixed field *by H.*

4.5 Proposition. *Let K be a field.*

(i) *If F_1 and F_2 are two subfields of K with $F_1 \subseteq F_2$, then* $\mathrm{Gal}(K/F_2)$ *is a subgroup of* $\mathrm{Gal}(K/F_1)$. *(Thus* $\mathrm{Gal}(K/F_2) \leq \mathrm{Gal}(K/F_1) \leq \mathrm{Aut}\, K$.*)*

(ii) *Let H_1 and H_2 be two subgroups of* $\mathrm{Aut}\, K$ *with $H_1 \leq H_2$. Then K^{H_2} is a subfield of K^{H_1}.*

Therefore the two maps:

$$\begin{array}{ccc} \{\textit{subfields of } K\} & \to & \{\textit{subgroups of } \mathrm{Aut}\, K\} \\ F & \mapsto & \mathrm{Gal}(K/F), \end{array}$$

and

$$\begin{array}{ccc} \{\textit{subgroups of } \mathrm{Aut}\, K\} & \to & \{\textit{subfields of } K\} \\ H & \mapsto & K^H, \end{array}$$

reverse containments.

4.6 Dedekind's Lemma. Let G be a group, K a field, and $\sigma_1, \dots, \sigma_n : G \to K^\times$ different group homomorphisms. Then $\sigma_1, \dots, \sigma_n$ are "linearly independent". That is, if $a_1, \dots, a_n \in K$ satisfy $\sum_{i=1}^n a_i\sigma_i(g) = 0$ for any $g \in G$, then $a_1 = \cdots = a_n = 0$.

Proof. The proof is done by induction on n, the result being clear if $n = 1$. Hence assume the result to be true for $n-1$ homomorphisms and that there are different group homomorphisms $\sigma_1, \dots, \sigma_n : G \to K^\times$ and scalars $a_1, \dots, a_n \in K$, not all of them different from 0, such that

$$a_1\sigma_1(g) + \cdots + a_n\sigma_n(g) = 0,$$

for any $g \in G$. If one of these scalars is 0, then we get a contradiction with the $n-1$ case. Hence $a_i \neq 0$ for any i. Now, as $\sigma_1 \neq \sigma_n$, there is an element $h \in G$ such that $\sigma_1(h) \neq \sigma_n(h)$. Then we have:

$$\sum_{i=1}^n a_i\sigma_i(hg) = a_1\sigma_1(h)\sigma_1(g) + \cdots + a_n\sigma_n(h)\sigma_n(g) = 0$$
$$\sigma_n(h)\Big(\sum_{i=1}^n a_i\sigma_i(g)\Big) = a_1\sigma_n(h)\sigma_1(g) + \cdots + a_n\sigma_n(h)\sigma_n(g) = 0.$$

If we subtract the two equations we get:

$$a_1\big(\sigma_1(h) - \sigma_n(h)\big)\sigma_1(g) + \cdots + a_{n-1}\big(\sigma_{n-1}(h) - \sigma_n(h)\big)\sigma_{n-1}(g) = 0.$$

But since $a_1\big(\sigma_1(h) - \sigma_n(h)\big)$ is not 0, we get a contradiction with the induction hypothesis. □

The next theorem is usually attributed to Artin, but it is already present in the work of Dedekind:

4.7 Theorem. *Let K be a field and let G be a subgroup of* Aut K *of order $n \in \mathbb{N}$, then $[K : K^G] = n$.*

Proof. Let $F = K^G$ and $G = \{\sigma_1 = 1, \dots, \sigma_n\}$. Assume first $[K : F] < n$ and let $\{\omega_1, \dots, \omega_m\}$ be a basis of K over F ($m < n$). Consider the following homogeneous system of m linear equations with n unknowns over K:

$$\begin{cases} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n = 0, \\ \qquad\qquad \vdots \\ \sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n = 0. \end{cases}$$

As $m < n$, there is a nontrivial solution $\alpha_1, \dots, \alpha_n$. Now, for any $0 \neq \alpha \in K$, there are scalars $\lambda_1, \dots, \lambda_m \in F$ such that $\alpha = \lambda_1\omega_1 + \cdots + \lambda_m\omega_m$. Note that $\sigma_i(\lambda_j) = \lambda_j$ for any i, j, because $F = K^G$, so if we multiply in the system above, with the x_i's substituted by the α_i's, the first row by λ_1, the second row by λ_2, ..., and we add the resulting equations we get

$$\sigma_1(\alpha)\alpha_1 + \cdots + \sigma_n(\alpha)\alpha_n = 0$$

for any $0 \neq \alpha \in K$, and this contradicts Dedekind's Lemma. (Here we have to consider $\sigma_1, \dots, \sigma_n$ as group homomorphisms $K^\times \to K^\times$.)

Note that we have not used here that G is a group, only that $\sigma_1, \ldots, \sigma_n$ are different automorphisms of K.

Assume now $[K : F] > n$, and let $\omega_1, \ldots, \omega_{n+1} \in K$ be a family of linearly independent elements (over F). Again there is a nontrivial solution $\alpha_1, \ldots, \alpha_{n+1}$ of the homogeneous linear system of equations:

$$\begin{cases} \sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} = 0, \\ \qquad\qquad\qquad \vdots \\ \sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n-1})x_{n+1} = 0. \end{cases}$$

As $\sigma_1 = 1$ and the ω_i's are linearly independent over F, not all the α_i's are in F (look at the first row of the system). Among all the possible nontrivial solutions we take one $(\alpha_1, \ldots, \alpha_{n+1})$ with the lowest possible number r of nonzero elements. After reordering the ω_i's, we may assume that this solution is of the form $(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$ with $\beta_r = 1$ and $\beta_1 \notin F$. Therefore, for any $j = 1, \ldots, n$ we have

$$\sigma_j(\omega_1)\beta_1 + \cdots + \sigma_j(\omega_{r-1})\beta_{r-1} + \sigma_j(\omega_r) = 0.$$

Now, since $\beta_1 \notin F$, there is an index k such that $\sigma_k(\beta_1) \neq \beta_1$. Apply σ_k to the last equation to get for any j:

$$\sigma_k\sigma_j(\omega_1)\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_j(\omega_{r-1})\sigma_k(\beta_{r-1}) + \sigma_k\sigma_j(\omega_r) = 0.$$

But since G is a group, we get $G = \{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n\}$, and the tuple $(\sigma_k(\beta_1), \ldots, \sigma_k(\beta_r), 0, \ldots, 0)$ is another solution of the homogeneous linear system. Therefore we get the new solution $(\beta_1 - \sigma_k(\beta_1), \ldots, \beta_{r-1} - \sigma_k(\beta_{r-1}), 1 - 1, 0, \ldots, 0)$ with at most $r - 1$ nonzero components, and with the first component different from 0. This contradicts our assumption on the minimality of r. □

4.8 Corollary. *Let K/F be a finite field extension. Then $|\mathrm{Gal}(K/F)| \leq [K : F]$, and the equality holds if and only if F is the fixed field by $\mathrm{Gal}(K/F)$.*

Proof. Write $G = \mathrm{Gal}(K/F)$. The first part of the proof above shows that $|G|$ is at most $[K : K^G]$, but $[K : F] = [K : K^G][K^G : F]$, so that $|G| \leq [K : K^G] \leq [K : F]$. In particular G is finite.

Now, the previous theorem shows that $|G| = [K : K^G]$, and hence $|G| = [K : F]$ if and only if $[K^G : F] = 1$, if and only if $F = K^G$. □

4.9 Corollary. *Let K be a field and let G and H be two finite subgroups of $\mathrm{Aut}\, K$. Then $K^G = K^H$ if and only if $G = H$.*

Proof. If $K^G = K^H$ and $\sigma \in H \setminus G$, then the fixed subfield by $G \cup \{\sigma\}$ is K^G, but the first part of the proof of Theorem 4.7 shows that $|G| + 1 \leq [K : K^G]$ and also $|G| = [K : K^G]$, thus getting a contradiction. The converse is trivial. □

4.10 Corollary. *Let K be a field and let G be a finite subgroup of $\mathrm{Aut}\, K$. Then $\mathrm{Gal}(K/K^G) = G$.*

Proof. The containment $G \leq \mathrm{Gal}(K/K^G)$ is clear, and both subgroups have the same fixed subfield, so the previous corollary applies. □

4.11 Theorem. *Let K/F be a finite field extension, and let $G = \mathrm{Gal}(K/F)$ be its Galois group. The following conditions are equivalent:*

(i) $F = K^G$,

(ii) $|\mathrm{Gal}(K/F)| = [K : F]$,

(iii) *Any irreducible polynomial $h(X) \in F[X]$ which has a root in K is separable and splits over K.*

(iv) *K is the splitting field of a separable polynomial $f(X) \in F[X]$.*

Proof. The previous corollaries prove the equivalence of conditions (i) and (ii).

(i) ⇒ (iii): Let $f(X) \in F[X]$ be an irreducible polynomial and let $\alpha \in K$ be a root of $f(X)$. Consider the different elements $\alpha_1, \ldots, \alpha_r$ in the set $\{\sigma(\alpha) : \sigma \in G\}$ (which is contained in the set of roots of $f(X)$) and take the polynomial $g(X) = (X - \alpha_1) \cdots (X - \alpha_r) \in K[X]$. Each $\sigma \in G$ permutes the α_i's, and hence the coefficients of $g(X)$ are fixed by σ. By (i) we get $g(X) \in F[X]$. But $g(X) \,|\, f(X)$ and $f(X)$ is irreducible, so we get $f(X) = ag(X)$ for some $0 \neq a \in F$, which is separable with all its roots in K.

(iii) ⇒ (iv): Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of K over F. Item (iii) implies that $m_{\omega_i,F}(X)$ is separable for any i and all its roots are in K. Hence K is the splitting field of the least common multiple of these polynomials $m_{\omega_i,F}(X)$, which is separable.

(iv) ⇒ (ii): We know that if $\varphi : F \to F^\sharp$ is a field isomorphism, K is a splitting field of a polynomial $f(X) \in F[X]$ over F, and $K^\sharp$ is a splitting field of the polynomial $f^\sharp(X) = \varphi(f(X))$ over $F^\sharp$ (this is the polynomial obtained from $f(X)$ by applying φ to all its coefficients), then there is a field isomorphism $\psi : K \to K^\sharp$ which extends φ. We will prove by induction on $[K : F]$ that the number of ψ's extending φ is at most $[K : F]$, and that it is exactly $[K : F]$ if $f(X)$ is separable. The particular case of $F = F^\sharp$, $K = K^\sharp$ and $\varphi = 1$ proves (iv) ⇒ (ii).

If $[K : F] = 1$, then $K = F$, $K^\sharp = F^\sharp$ and $\psi = \varphi$ is the only possibility.

Assume then that $[K : F] > 1$ and that the result is valid for lower degree extensions. Let $h(X)$ be an irreducible factor of $f(X)$ with a root $\alpha \in K \setminus F$, and let $h^\sharp(X)$ be its "image" under φ. If ψ extends φ then $\alpha^\sharp = \psi(\alpha)$ is a root of $h^\sharp(X)$ and $\tau = \psi|_{F(\alpha)} : F(\alpha) \to F^\sharp(\alpha^\sharp)$ is an isomorphism extending φ. We get the diagram:

$$\begin{array}{rcl} \psi : K & \xrightarrow{\sim} & K^\sharp \\ \bigcup\uparrow & & \bigcup\uparrow \\ \tau : F(\alpha) & \xrightarrow{\sim} & F^\sharp(\alpha^\sharp) \\ \bigcup\uparrow & & \bigcup\uparrow \\ \varphi : F & \xrightarrow{\sim} & F^\sharp \end{array}$$

Conversely, if $\alpha^\sharp$ is a root of $h^\sharp(X)$, there is an isomorphism $\tau : F(\alpha) \to F^\sharp(\alpha^\sharp)$ extending φ and such that $\tau(\alpha) = \alpha^\sharp$, and since K (respectively $K^\sharp$) is a splitting field of $f(X)$ (respectively $f^\sharp(X)$) over F (respectively $F^\sharp$), there is an isomorphism $\psi : K \to K^\sharp$ extending τ. Therefore the number of extensions $\psi : K \to K^\sharp$ of φ equals the product of the number of extensions $\tau : F(\alpha) \to F^\sharp(\alpha^\sharp)$ of φ by the number of extensions of each such τ to an isomorphism $\psi : K \to K^\sharp$. This last number is, by the induction hypothesis, at most $[K : F(\alpha)]$, with equality if $f(X)$ is separable, while the first

number (of extensions τ) is the number of roots of $h(X)$, which is at most $\deg h(X) = [F(\alpha) : F]$, again with equality if $f(X)$ (and hence $h(X)$) is separable. Therefore the number of extensions ψ of φ is at most $[K : F(\alpha)][F(\alpha) : F] = [K : F]$, with equality if $f(X)$ is separable. □

4.12 Definition. A finite field extension K/F satisfying the equivalent conditions in the previous theorem is said to be a *Galois extension.*

4.13 Corollary. *Let K/F be a finite field extension. Then K/F is a Galois extension if and only if it is separable and normal.*

Proof. If K/F is a Galois extension, then for any $\alpha \in K$, $m_{\alpha,F}(X)$ is separable by item (iii) in the previous theorem, and hence K/F is separable. By item (iv) K/F is normal too.

Conversely, if K/F is a finite normal field extension, then K is the splitting field of a monic polynomial $f(X) \in F[X]$. Consider its factorization into irreducible factors: $f(X) = f_1(X)^{m_1} \cdots f_s(X)^{m_s}$ (the $f_i(X)'s$ are irreducible and coprime). Then K is also the splitting field over F of the polynomial $f_1(X) \cdots f_s(X)$. Now, if K/F is separable, each $f_i(X)$ is separable, and hence so is its product. Hence item (iv) of the previous theorem is fulfilled. □

4.14 Consequences.

(i) *Let K/F be a finite field extension, and assume that $K = F(\alpha_1, \ldots, \alpha_r)$ with α_i separable over F for any $i = 1, \ldots, r$. Then K/F is separable.*

(ii) *Let K/F be a finite field extension. Consider the set $S = \{\alpha \in K : \alpha$ is separable over $F\}$. Then S is a subfield of K containing F. Moreover, if the characteristic of F is 0, then $S = K$, while if the characteristic of F is $p > 0$, then for any $\alpha \in K$ there is an $n \in \mathbb{N} \cup \{0\}$ such that $\alpha^{p^n} \in S$.*

(iii) *If L/K and K/F are two finite field extensions, then L/F is separable if and only if so are L/K and K/F.*

Proof. For (i) note that if L is a splitting field over F, and containing K, of the least common multiple of the $m_{\alpha_i,F}(X)$'s, then L/F is a Galois extension. Hence L/F is separable and so is K/F.

For (ii) note that F is trivially contained in S and that, because of (i), for any two elements $\alpha, \beta \in S$, the subfield $F(\alpha, \beta)$ is contained in S, in particular, $\alpha + \beta, \alpha\beta, \alpha^{-1}$ (if $\alpha \neq 0$) are in S and S is a subfield. If the characteristic is 0 any field extension is separable, so the last assertion follows. Assume now that the characteristic is p, and take $\alpha \in K$ and $f(X) = m_{\alpha,F}(X)$. Then there is an $n \in \mathbb{N} \cup \{0\}$ and a polynomial $g(X) \in F[X]$ such that $f(X) = g(X^{p^n})$ and $g'(X) \neq 0$. Since $f(X)$ is irreducible, so is $g(X)$, and hence $g(X)$ is separable. It follows that $\alpha^{p^n} \in S$.

For (iii) note that if L/F is separable, then so is K/F. Also for any $\alpha \in L$, $m_{\alpha,K}(X)$ divides $m_{\alpha,F}(X)$, which is separable, and hence $m_{\alpha,K}(X)$ is separable too. This shows that L/K is separable. Conversely, if L/K and K/F are separable, then if the characteristic is 0 obviously L/F is separable, while if the characteristic is p, by (ii) the subfield $S = \{\alpha \in L : \alpha \text{ is separable}\}$ contains K, and for any $\alpha \in L$, there is an n such that $\alpha^{p^n} \in S$. Then $m_{\alpha,S}(X) \,|\, X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$. But L/K is separable, and hence so is L/S. Therefore $m_{\alpha,S}(X) = X - \alpha$ and $\alpha \in S$. Thus $L = S$ is separable over F. □

§ 5. The Fundamental Theorem of Galois Theory

5.1 Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$. Then K is a splitting field of $(X^2 - 2)(X^2 - 3)$ over F, and hence K/F is a Galois extension.

For any $\xi \in \mathrm{Gal}(K/F)$, ξ is determined by the valued $\xi(\sqrt{2})$ (which is a root of $X^2 - 2$) and $\xi(\sqrt{3})$ (a root of $X^2 - 3$). Hence there are four possibilities:

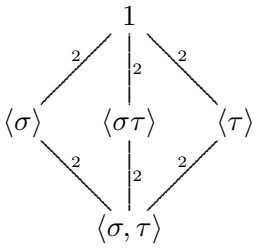
$$\underset{1}{\begin{cases}\sqrt{2} \mapsto \sqrt{2},\\ \sqrt{3} \mapsto \sqrt{3},\end{cases}} \qquad \underset{\sigma}{\begin{cases}\sqrt{2} \mapsto -\sqrt{2},\\ \sqrt{3} \mapsto \sqrt{3},\end{cases}} \qquad \underset{\tau}{\begin{cases}\sqrt{2} \mapsto \sqrt{2},\\ \sqrt{3} \mapsto -\sqrt{3},\end{cases}} \qquad \underset{\sigma\tau = \tau\sigma}{\begin{cases}\sqrt{2} \mapsto -\sqrt{2},\\ \sqrt{3} \mapsto -\sqrt{3},\end{cases}}$$

Since $\mathrm{Gal}(K/F)$ has order 4, it follows that $\mathrm{Gal}(K/F) = \{1, \sigma, \tau, \sigma\tau\} = \langle\sigma\rangle \times \langle\tau\rangle \simeq C_2 \times C_2$.

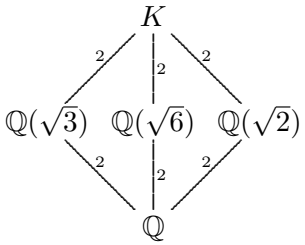
Let us have a look at the subgroups of $\mathrm{Gal}(K/F)$ and the corresponding fixed subfields:

Subgroups of $\mathrm{Gal}(K/F)$	**Fixed subfields**
1	$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\langle\sigma\rangle$	$\mathbb{Q}(\sqrt{3})$
$\langle\tau\rangle$	$\mathbb{Q}(\sqrt{2})$
$\langle\sigma\tau\rangle$	$\mathbb{Q}(\sqrt{6})$
$\langle\sigma, \tau\rangle = \mathrm{Gal}(K/F)$	$\mathbb{Q}$

Here is the diagram of subgroups:



and here the diagram of fixed subfields:



The Fundamental Theorem of Galois Theory establishes a bijection between the set of intermediate subfields in a Galois extension K/F and the set of subgroups of the group $\mathrm{Gal}(K/F)$. The first set seems, in principle, quite difficult to deal with (its elements are usually quite complicated infinite objects), while the second set is a finite discrete set, more suitable for direct computations (with or without a computer).

5.2 Fundamental Theorem of Galois Theory. Let K/F be a Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. Then the maps

$$\begin{array}{ccc} \{\text{Subfields of } K \text{ containing } F\} & \xrightarrow{\varphi} & \{\text{Subgroups of } G\} \\ E & \mapsto & \mathrm{Gal}(K/E), \end{array}$$

and

$$\begin{array}{ccc} \{\text{Subgroups of } G\} & \xrightarrow{\psi} & \{\text{Subfields of } K \text{ containing } F\} \\ H & \mapsto & K^H, \end{array}$$

(both of which reverse containments) are bijective and mutually inverse.

Moreover, for $H \leq G$ and $E = K^H$, we have $[E : F] = [G : H]$ and $[K : E] = |H|$. Besides K/E is a Galois extension, while the extension E/F is a Galois extension if and only if H is a normal subgroup of G. In this case, $\mathrm{Gal}(E/F)$ is isomorphic to G/H.

Proof. We already know that if H_1 and H_2 are subgroups of G and $K^{H_1} = K^{H_2}$, then $H_1 = H_2$. Hence ψ is one-to-one.

If E is a subfield with $F \subseteq E \subseteq K$, then since K/F is a Galois extension, K is a splitting field over F of a separable polynomial $f(X) \in F[X]$, and hence K is a splitting field too of $f(X)$ over E. Therefore, K/E is a Galois extension. On the other hand, the extension K/E is a Galois extension if and only if E is the fixed field by $\mathrm{Gal}(K/E)$, that is: $E = K^{\mathrm{Gal}(K/E)} = \psi(\varphi(E))$. This shows that $\psi\varphi = 1$, and hence ψ is onto too. We conclude that ψ is a bijection and $\varphi = \psi^{-1}$.

Moreover, since K/E is a Galois extension, we get $[K : E] = |H|$, with $H = \mathrm{Gal}(K/E)$. But

$$|G| = \begin{cases} [G : H]|H|, \\ [K : F] = [K : E][E : F], \end{cases}$$

and we obtain $[E : F] = [G : H]$.

Finally, let H be a subgroup of G and let $E = K^H$. Let us prove the equivalence of the following condtions: **(i)** E/F is a Galois extension, **(ii)** $\sigma(E) = E$ for any $\sigma \in G$, **(iii)** H is a normal subgroup of G.

(i)⇒(ii): If E/F is a Galois extension, then E is the splitting field over F of a separable polynomial $f(X) \in F[X]$: $f(X) = (X - \alpha_1) \cdots (X - \alpha_r)$, where $\alpha_1, \ldots, \alpha_r$ are all different and $E = F(\alpha_1, \ldots, \alpha_r)$. Now for any $\sigma \in G$ and any i, $1 \leq i \leq r$, $\sigma(\alpha_i)$ is a root of $f(X)$. Thus σ permutes the α_i's, and hence $\sigma(E) = E$.

(iii)⇒(ii): If H is normal, for any $\sigma \in G$, $\tau \in H$, and $\gamma \in E$, $\tau(\sigma(\gamma)) = \sigma(\sigma^{-1}\tau\sigma)(\gamma) = \sigma(\gamma)$, because $\sigma^{-1}\tau\sigma$ is in H. Hence $\sigma(\gamma) \in K^H = E$ and $\sigma(E) = E$.

(ii) ⇒ (i) and (iii): If $\sigma(E) = E$ for any $\sigma \in G$, we have the group homomorphism:

$$\begin{array}{ccc} G = \mathrm{Gal}(K/F) & \xrightarrow{\pi} & \mathrm{Gal}(E/F) \\ \sigma & \mapsto & \sigma|_E, \end{array}$$

with kernel $\mathrm{Gal}(K/E) = H$, so that H is normal. Besides π is onto, since any automorphism $\tau : E \to E$ can be extended to K because K is a splitting field over F. By the First Isomorphism

Theorem G/H is isomorphic to $\mathrm{Gal}(E/F)$ and $|\mathrm{Gal}(E/F)| = [G : H] = [E : F]$. We conclude that E/F is a Galois extension. (Alternatively, for any $\alpha \in E^{\mathrm{Gal}(E/F)}$ and $\sigma \in G$, $\sigma(\alpha) = \sigma|_E(\alpha) = \alpha$, so $\alpha \in K^G = F$. Hence $F = E^{\mathrm{Gal}(E/F)}$, and E/F is a Galois extension.) □

5.3 Corollary. *Let K/F be a Galois extension. Then there is a finite number of intermediate subfields between F and K.*

§ 6. Finite fields

6.1 Lemma. *Let F be a field and let G be a finite subgroup of the multiplicative group $F^\times$. Then G is cyclic.*

Proof. G is a finite abelian group, and hence G is isomorphic to a direct product of cyclic groups $G \simeq C_{m_1} \times \cdots \times C_{m_r}$, with $m_1 \mid m_2 \mid \cdots \mid m_r$. Therefore any $x \in G$ is a root of the polynomial $X^{m_r} - 1$. But F contains at most m_r roots of this polynomial. We conclude that $r = 1$, G is cyclic, and G is the set of roots of the separable polynomial $X^{m_r} - 1$ in F. □

If F is a finite field, then its characteristic is a prime number p. If n denotes the dimension of F over its prime subfield $\mathbb{F}_p$: $n = \dim_{\mathbb{F}_p} F$, then $|F| = p^n$.

The following result is due to Galois:

6.2 Theorem. *For each prime number p and each natural number n there exists a unique (up to isomorphism) field F with p^n elements. Moreover, the extension $F/\mathbb{F}_p$ is a Galois extension and $\mathrm{Gal}(F/\mathbb{F}_p)$ is the cyclic group of order n. (Notation: $F = GF(p^n)$.)*

Proof. If F is a field with p^n elements, then $F^\times$ is a cyclic group of order $p^n - 1$ whose elements are the roots of the separable polynomial $X^{p^n-1} - 1$. Therefore F is the splitting field of the separable polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$. This proves the uniqueness.

On the other hand, let E be a splitting field of the separable polynomial $f(X) = X^{p^n} - X$ over $\mathbb{F}_p$ (note that the derivative of this polynomial is -1, and hence $\gcd(f(X), f'(X)) = 1$ and it contains no multiple roots). Let $F = \{x \in E : f(x) = 0\}$. Then since $f(X)$ has no multiple roots, $|F| = p^n$. But F is a field, because $(a + b)^{p^n} = a^{p^n} + b^{p^n}$, $(ab)^{p^n} = a^{p^n} b^{p^n}$ and, if $b \neq 0$, $(b^{p^n})^{-1} = (b^{-1})^{p^n}$ for any $a, b \in E$. Hence $F = E$ and $|E| = p^n$. This shows the existence.

Finally, for $F = E$ as above, the map $\sigma : F \to F$, $x \mapsto x^p$ is an automorphism (called the *Frobenius automorphism*). Since $F^\times$ is cyclic, $F^\times = \langle\alpha\rangle$ for some $0 \neq \alpha \in F$, with $\alpha^{p^n-1} = 1$ and $\alpha^i \neq 1$ for any $i < p^n - 1$. Then $\sigma^n(\alpha) = \alpha^{p^n} = \alpha$, while $\sigma^i(\alpha) \neq \alpha$ for $i < p^n - 1$. Hence the order of σ is $n = |\mathrm{Gal}(F/\mathbb{F}_p)|$, and hence $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$ is cyclic. □

6.3 Remark.

(i) By the Fundamental Theorem of Galois Theory, the subfields of $GF(p^n)$ are in one-to-one correspondence with the subgroups of $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$, and hence with the set of divisors of n. For any divisor d of n, $\langle\sigma^d\rangle$ is a subgroup of $\langle\sigma\rangle = \mathrm{Gal}(F/\mathbb{F}_p)$ and the fixed subfield by σ^d is $\{\beta \in F : \beta^{p^d} = \beta\} = GF(p^d)$. Thus the set of subfields of $GF(p^n)$ is $\{GF(p^d) : d \mid n\}$.

(ii) If α is a generator of the cyclic group $GF(p^n)^\times$, then $GF(p^n) = \mathbb{F}_p(\alpha)$ and $\deg m_{\alpha,\mathbb{F}_p}(X) = n$. In particular, for any $n \in \mathbb{N}$ there is an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n.

§ 7. Primitive elements

7.1 Definition. A field extension K/F is said to be *simple* if there is an element $\alpha \in K$ such that $K = F(\alpha)$. In this case, the element α is said to be a *primitive element* of the extension.

The following theorem is due to Steinitz:

7.2 Theorem. *Let K/F be a finite field extension. Then K/F is simple if and only if the number of intermediate subfields between F and K is finite.*

Proof. Assume first that $K = F(\alpha)$ is a simple extension, and let $f(X) = m_{\alpha,F}(X)$. Let E be an intermediate subfield: $F \subseteq E \subseteq K$. Then the polynomial $m_{\alpha,E}(X) = a_0 + a_1X + \cdots + a_rX^r + X^{r+1}$ divides $f(X)$ (in $E[X]$, and hence in $K[X]$). Consider the subfield $E' = F(a_0, a_1, \ldots, a_r)$. Then $F \subseteq E' \subseteq E \subseteq K$ and $m_{\alpha,E}(X) \mid m_{\alpha,E'}(X)$ in $E[X]$, but $m_{\alpha,E}(X) \in E'[X]$, and it is irreducible over E, and hence over E', so equality follows: $m_{\alpha,E}(X) = m_{\alpha,E'}(X)$. But then we have $[K : E] = [E(\alpha) : E] = \deg m_{\alpha,E}(X) = [K : E']$ and $E = E'$.

Therefore the intermediate subfields are generated over F by the coefficients of monic factors of $f(X)$, and there are only a finite number of such factors.

For the converse, if F is finite, then K is finite too and hence $K = \mathbb{F}_p(\alpha) = F(\alpha)$ for some α. If F is infinite, it is enough to show that for any $\alpha, \beta \in K$, there is an element $c \in F$ such that $F(\alpha, \beta) = F(\alpha + c\beta)$. Since F is infinite and there is only a finite number of intermediate subfields, there are elements $c_1 \neq c_2$ in F such that $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$, but then $\alpha + c_1\beta, \alpha + c_2\beta \in F(\alpha + c_2\beta)$, and it follows that $F(\alpha + c_2\beta)$ contains both α and β, so $F(\alpha + c_2\beta) = F(\alpha, \beta)$. □

7.3 Primitive Element Theorem. Let K/F be a finite separable field extension. Then K/F is simple.

Proof. Let $K = F(\alpha_1, \ldots, \alpha_r)$ and $f(X) = \operatorname{lcm}(m_{\alpha_1,F}(X), \ldots, m_{\alpha_r,F}(X))$. Then $f(X)$ is a least common multiple of separable polynomials, and hence it is separable. Let E be a splitting field of $f(X)$ over F with $F \subseteq K \subseteq E$. Then E/F is a Galois extension so the number of intermediate fields between F and E is finite. Hence so is the number of intermediate fields between F and K and Steinitz's Theorem applies. □

§ 8. Ruler and compass constructions

Recall from *Algebraic Structures* that an element $x \in \mathbb{R}_{\geq 0}$ is said to be *constructible* if, starting with the unit segment, it is possible to construct, with ruler and compass only, a segment of length x. An element $x \in \mathbb{R}_{<0}$ is *constructible* if so is $-x$.

It was shown that the set $C = \{x \in \mathbb{R} : x \text{ is constructible}\}$ is a subfield of $\mathbb{R}$ containing $\mathbb{Q}$.

The main result on C proved in that course is the following:

8.1 Theorem. *Let $a \in \mathbb{R}$, then $a \in C$ if and only if there are $n \in \mathbb{N} \cup \{0\}$ and subfields $F_0, F_1, \ldots, F_n$ of $\mathbb{R}$ such that $F_0 = \mathbb{Q} \leq F_1 \leq \cdots \leq F_n$, $[F_i : F_{i-1}] = 2$ for any $i = 1, \ldots, n$, and $a \in F_n$.*

In particular, if $a \in C$, then $[\mathbb{Q}(a) : \mathbb{Q}]$ is a power of 2.

Now we can improve a little bit on this.

8.2 Lemma. *Let K/F be a Galois extension of characteristic $\neq 2$ with $[K : F] = 2^r$ for some $r \geq 0$, and let E/K be a degree 2 field extension. Then there is a field extension L/E such that L/F is a Galois extension whose degree is again a power of 2.*

Proof. Because of the restriction on the characteristic, $E = K(\alpha)$ for some $\alpha \in E$ with $m_{\alpha,K}(X) = X^2 - \mu$ for some $\mu \in K$. Write $G = \mathrm{Gal}(K/F)$. The Primitive Element Theorem shows that there is an element $\beta \in K$ such that $K = F(\beta)$. Write $m_{\beta,F}(X) = f(X)$. Let $\mu_1, \ldots, \mu_m$ be the different elements in the set $\{\sigma(\mu) : \sigma \in G\}$, and consider the polynomial $g(X) = \prod_{j=1}^{m}(X^2 - \mu_j)$. This is a polynomial in $F[X]$, because its coefficients are fixed by the elements in G (which permute the μ_j's). Let L be a splitting field over F of the separable polynomial $\mathrm{lcm}(f(X), g(X))$ containing E. Hence L/F is a Galois extension. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ be the roots of $g(X)$ in L and note that none of them is in K (as $\gamma \in K$ and $\gamma^2 = \sigma(\mu)$ implies $\left(\sigma^{-1}(\gamma)\right)^2 = \mu$, and hence $X^2 - \mu$ would have a root in K). Then $L = K(\alpha_1, \ldots, \alpha_r)$ and the degree of each extension $K(\alpha_1, \ldots, \alpha_i)/K(\alpha_1, \ldots, \alpha_{i-1})$ is ≤ 2. Hence $[L : K]$ is a power of 2, and so is $[L : F] = [L : K][K : F]$. □

8.3 Theorem. *Let α be a real number algebraic over $\mathbb{Q}$, and let K be a splitting field of $m_{\alpha,\mathbb{Q}}(X)$ over $\mathbb{Q}$. Then α is constructible if and only if $[K : \mathbb{Q}]$ is a power of 2.*

Proof. If α is constructible, then there is a tower of field extensions $F_0 = \mathbb{Q} \leq F_1 \leq \cdots \leq F_n$, such that F_i is a subfield of $\mathbb{R}$ and $[F_i : F_{i-1}] = 2$ for any $i = 1, \ldots, n$, and $\alpha \in F_n$. An inductive argument using the previous lemma shows that there is a Galois extension $L/\mathbb{Q}$ with $F_n \subseteq L \subseteq \mathbb{C}$ and $[L : \mathbb{Q}]$ a power of 2. Since $\alpha \in L$ and $L/\mathbb{Q}$ is a Galois extension, there is a splitting field of $m_{\alpha,\mathbb{Q}}(X)$ contained in L. The uniqueness of splitting fields give the result.

Conversely, assume that α belongs to K, which may be assumed to be contained in $\mathbb{C}$, and $K/\mathbb{Q}$ is a Galois extension of degree a power of 2. Then $G = \mathrm{Gal}(K/\mathbb{Q})$ is a 2-group and a chain of subgroups can be obtained: $1 = G_0 \leq G_1 \leq \cdots \leq G_r = G$, such that $[G_i : G_{i-1}] = 2$ for any $i = 1, \ldots, r$. Considering the corresponding fixed fields, we get a tower of subfields of $\mathbb{C}$:

$$\mathbb{Q} = K_0 = K^{G_r} \leq K_1 = K^{G_{r-1}} \leq \cdots \leq K_r = K = K^{G_0},$$

such that $[K_j : K_{j-1}] = 2$ for any $j = 1, \ldots, r$. The problem is that for any j, K_j is contained in $\mathbb{C}$, and not necessarily in $\mathbb{R}$. Write $K_j = K_{j-1}(a_j + b_j i)$, with $(a_j + b_j i)^2 \in K_{j-1}$. For each j consider the field F_j generated over $\mathbb{Q}$ by the real and imaginary parts of the elements of K_j. It is easy to check that $F_0 = \mathbb{Q}$ and $F_j = F_{j-1}(a_j, b_j)$ for any $j \geq 1$. Note that $\alpha \in \mathbb{R} \cap K$, so that $\alpha \in F_r$.

But $(a_j + b_j i)^2 \in K_{j-1}$, which implies $a_j^2 - b_j^2, a_j b_j \in F_{j-1}$, and hence we have two extensions

$$F_{j-1} \leq F_{j-1}(a_j^2 + b_j^2) \leq F_{j-1}(a_j, b_j),$$

whose degrees are either 1 or 2, because $(a_j^2 + b_j^2)^2 = (a_j^2 - b_j^2)^2 + (2a_j b_j)^2$ is in F_{j-1}, and if, for instance, $a_j \neq 0$, then $b_j \in F_{j-1}(a_j)$ (as $a_j b_j \in F_{j-1}$), and $a_j^2 = \frac{1}{2}(a_j^2 + b_j^2) + \frac{1}{2}(a_j^2 - b_j^2) \in F_{j-1}(a_j^2 +$

b_j^2). (The same argument applies if $b_j \neq 0$.) Therefore the tower of subfields $\mathbb{Q} = F_0 \leq \cdots \leq F_r$ can be refined to a tower of subfields with degree 2 consecutive field extensions. □

§ 9. Galois groups of polynomials

Recall that if F is a field and $f(X) \in F[X]$ is a degree ≥ 1 polynomial over F, then the *Galois group* of $f(X)$ over F is the Galois group $\mathrm{Gal}(E/F)$, where E is a splitting field of $f(X)$ over F. If $f(X)$ is separable, then E/F is a Galois extension.

9.1 Proposition. *Let F be a field and let $f(X) \in F[X]$ be a polynomial of degree ≥ 1. Let E be a splitting field of $f(X)$ over F. Consider the complete factorization $f(X) = a f_1(X)^{n_1} \cdots f_r(X)^{n_r}$, where $0 \neq a$ is the leading coefficient and $f_1(X), \ldots, f_r(X)$ are the different monic irreducible factors of $f(X)$. Denote by Ω_i the set of roots of $f_i(X)$ in E, for any $i = 1, \ldots, r$, and by $\Omega = \Omega_1 \cup \cdots \cup \Omega_r$ (disjoint union) the set of roots of $f(X)$ in E. Then:*

(i) *Any $\sigma \in \mathrm{Gal}(E/F)$ permutes the elements of Ω_i for any $i = 1, \ldots, r$. Hence there is an associated one-to-one group homomorphism:*

$$\mathrm{Gal}(E/F) \to S(\Omega_1) \times \cdots \times S(\Omega_r) \ \Big(\subseteq S(\Omega)\Big).$$

(ii) *For any $\alpha \in \Omega_i$ ($i = 1, \ldots, r$), the orbit of α by the action of $\mathrm{Gal}(E/F)$ is the whole Ω_i. (That is, $\mathrm{Gal}(E/F)$ acts transitively on each Ω_i.)*

Proof. If α is in Ω_i, it is a root of $f_i(X) \in F[X]$, and so is $\sigma(\alpha)$ for any $\sigma \in \mathrm{Gal}(E/F)$. Hence $\sigma(\alpha) \in \Omega_i$ too. On the other hand, if an element $\sigma \in \mathrm{Gal}(E/F)$ satisfies $\sigma(\alpha) = \alpha$ for any $\alpha \in \Omega$ then, as $E = F(\Omega)$, $\sigma = 1$, so the above group homomorphism is one-to-one.

For any $i = 1, \ldots, r$ and $\alpha, \beta \in \Omega_i$ there is a field isomorphism $\tau : F(\alpha) \to F(\beta)$ which acts as the identity on F and takes α to β. But E is a splitting field of $f(X)$ over F, and hence this τ extends to an automorphism σ of E. Hence there is an element $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma(\alpha) = \beta$. □

9.2 Example. For the polynomial $f(X) = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$, the splitting field is $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and the orbits in the proposition above are $\Omega_1 = \{\sqrt{2}, -\sqrt{2}\}$ and $\Omega_2 = \{\sqrt{3}, -\sqrt{3}\}$. In this case $\mathrm{Gal}(E/F) \simeq S(\Omega_1) \times S(\Omega_2) \simeq C_2 \times C_2$.

Let us check now that the symmetric groups S_n appear as Galois groups of certain polynomials.

9.3 Definition. Let F be a field and for $n \in \mathbb{N}$ let $x_1, \ldots, x_n$ be n different unknowns. The

elements $s_1, \dots, s_n \in F(x_1, \dots, x_n)$ defined by:

$$\begin{cases} s_1 = x_1 + \cdots + x_n, \\ s_2 = \displaystyle\sum_{1 \le i < j \le n} x_i x_j, \\ s_3 = \displaystyle\sum_{1 \le i < j < k \le n} x_i x_j x_k, \\ \quad \vdots \\ s_n = x_1 x_2 \cdots x_n, \end{cases}$$

are called the *elementary symmetric polynomials.*

The polynomial $p_n(X) = (X - x_1)(X - x_2) \cdots (X - x_n) \in F(x_1, \dots, x_n)[X]$ is said to be the *general polynomial of degree n.*

9.4 Remark. Note that

$$\begin{aligned} p_n(X) &= (X - x_1)(X - x_2) \cdots (X - x_n) \\ &= X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n \in F(s_1, s_2, \dots, s_n)[X], \end{aligned}$$

and that $F(x_1, \dots, x_n)$ is a splitting field of the separable polynomial $p_n(X)$ over $F(s_1, \dots, s_n)$. Hence $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ is a Galois extension.

9.5 Theorem. *The Galois group* $\mathrm{Gal}\big(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)\big)$ *is isomorphic to the symmetric group* S_n.

Proof. By the previous proposition the map

$$\begin{aligned} \mathrm{Gal}\big(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)\big) &\longrightarrow S_n \\ \sigma \quad &\mapsto \{1, \dots, n\} \to \{1, \dots, n\} \\ i \ &\mapsto \ j \qquad \text{if } \sigma(x_i) = x_j, \end{aligned}$$

is a one-to-one group homomorphism. But for any $\tau \in S_n$ we may define the automorphism:

$$\begin{aligned} \tilde{\tau} : F(x_1, \dots, x_n) &\to F(x_1, \dots, x_n) \\ f(x_1, \dots, x_n) &\mapsto f(x_{\tau(1)}, \dots, x_{\tau(n)}). \end{aligned}$$

Then $\tilde{\tau}(s_i) = s_i$ for any i, so we have $\tilde{\tau} \in \mathrm{Gal}\big(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)\big)$ and the monomorphism above is an isomorphism. □

9.6 Corollary. *The general polynomial of degree n:* $p_n(X)$, *is irreducible over* $F(s_1, \dots, s_n)$.

Proof. Just notice that S_n acts transitively on $\{1, \dots, n\}$. □

9.7 Definition. A rational function $f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ is said to be symmetric if for any $\tau \in S_n$, $f(x_1, \dots, x_n) = f(x_{\tau(1)}, \dots, x_{\tau(n)})$.

9.8 Example. $\big((x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\big)^2$ is symmetric in $F(x_1, x_2, x_3)$.

9.9 Proposition. *A rational function $f(x_1,\dots,x_n) \in F(x_1,\dots,x_n)$ is symmetric if and only if it belongs to $F(s_1,\dots,s_n)$.*

Proof. Note that $f(x_1,\dots,x_n)$ is symmetric if and only if it belongs to the fixed field by the Galois group $\mathrm{Gal}(F(x_1,\dots,x_n)/F(s_1,\dots,s_n)) \simeq S_n$, and this is $F(s_1,\dots,s_n)$. □

For the rest of this section, the characteristic of the fields involved will be assumed to be $\neq 2$.

Note that the discriminant of the general polynomial is

$$\mathrm{D} = \Big(\prod_{1\le i<j\le n}(x_i - x_j)\Big)^2.$$

We will identify any $\sigma \in S_n$ with the corresponding element in $\mathrm{Gal}(F(x_1,\dots,x_n)/F(s_1,\dots,s_n))$. Write $\Delta = \prod_{1\le i<j\le n}(x_i - x_j)$. Then for any $\sigma \in S_n$, $\sigma(\Delta) = \pm\Delta$, and we have.

$$\sigma(\Delta) = \Delta \quad\Longleftrightarrow\quad \sigma \in A_n.$$

9.10 Proposition. *Let $f(X) \in F[X]$ be a monic separable polynomial of degree ≥ 1, let E be a splitting field of $f(X)$ over F, let $\alpha_1,\dots,\alpha_n$ be the different roots of $f(X)$ in E (so that $f(X) = (X-\alpha_1)\cdots(X-\alpha_n)$, $\Delta = \prod_{1\le i<j\le n}(\alpha_i - \alpha_j)$, and $\Delta^2 = \mathrm{D}(f(X))$). Let $G = \mathrm{Gal}(E/F)$ be the associated Galois group, which will be identified with a subgroup of S_n through its action on the roots of $f(X)$, and let H be the intersection of G with the alternating group A_n: $H = G \cap A_n$.*

Then we have $E^H = F(\Delta)$, so Δ is in F if and only if G is contained in A_n.

Proof. For any $\sigma \in G$, $\sigma(\Delta) = \Delta$ if and only if $\sigma \in H$. Thus we get $\mathrm{Gal}(E/F(\Delta)) = H$, and $E^H = F(\Delta)$, because E/F is a Galois extension. □

Galois groups of degree 2 polynomials.

If $f(X) = X^2+bX+c$ is a monic degree 2 polynomial over a field F, then $D = \mathrm{D}(f(X)) = b^2-4c$, and $\Delta = \sqrt{b^2-4c}$. Let E be a splitting field of $f(X)$ over F, and $G = \mathrm{Gal}(E/F)$ the associated Galois group. Then $G \lesssim S_2 \simeq C_2$, so either $G = 1$ and $\Delta \in F$, or G is the cyclic group of order 2, $\Delta \notin F$ and $E = F(\Delta)$.

Galois groups of degree 3 polynomials. (Characteristic $\neq 2, 3$)

Let $f(X) = X^3 + aX^2 + bX + c$ be a monic degree 3 polynomial over a field F of characteristic $\neq 2, 3$. Let E be a splitting field of $f(X)$ over F and let G be the associated Galois group.

If $f(X)$ is reducible, then either it is a product of polynomials of degree 1 over F, and hence $E = F$ and $G = 1$, or $f(X)$ is a product of a polynomial of degree 1 and an irreducible polynomial of degree 2. The considerations above show that in this case G is the cyclic group of order 2.

Hence we will assume from now on that $f(X)$ is irreducible. The characteristic being $\neq 3$ assures that $f(X)$ is separable, so there are three different roots $\alpha_1, \alpha_2, \alpha_3 \in E$ with $f(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$. The Galois group G is, up to isomorphism, a subgroup of S_3 which acts transitively on these roots. Therefore either $G = A_3$ or $G = S_3$ and by the previous proposition $G = A_3$ if and only if $\Delta = \sqrt{\mathrm{D}(f(X))} = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$ is in F.

Note that the discriminant is computed as follows:

$$\begin{aligned}
\mathrm{D}(f(X)) &= -\begin{vmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 3 & 2a & b & 0 & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{vmatrix} = -\begin{vmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 0 & -a & -2b & -3c & 0 \\ 0 & 0 & -a & -2b & -3c \\ 0 & 0 & 3 & 2a & b \end{vmatrix} \\
&= \begin{vmatrix} 1 & a & b & c \\ 0 & a^2-2b & ab-3c & ac \\ 0 & a & 2b & 3c \\ 0 & 3 & 2a & b \end{vmatrix} = \begin{vmatrix} a^2-2b & ab-3c & ac \\ a & 2b & 3c \\ 3 & 2a & b \end{vmatrix} \\
&= a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc.
\end{aligned}$$

Recall from *Algebraic Structures* that in order to get the roots, we may proceed as follows. By means of the change of variables given by $Y = X + \frac{1}{3}a$, we are left with a degree 3 equation of the form

$$Y^3 + pY + q = 0,$$

with $p = \frac{1}{3}(3b - a^2)$ and $q = \frac{1}{27}(2a^3 - 9ab + 27c)$. Write $Y = u + v$ to get

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0,$$

which, with $uv = -\frac{p}{3}$, gives

$$\begin{cases} u^3 + v^3 = -q, \\ uv = -\dfrac{p}{3}. \end{cases}$$

And this allows us to compute u^3 and v^3, and hence u and v, by solving a degree 2 equation. Let ω be a primitive cubic root of 1 in an extension field of E. Hence $1 + \omega + \omega^2 = 0$ and if u, v is a solution of the previous equations, then the possible solutions are: u and v, ωu and $\omega^2 v$, and $\omega^2 u$ and ωv. We thus get the roots of our original equation: $u + v$, $\omega u + \omega^2 v$, $\omega^2 u + \omega v$.

Galois groups of degree 4 polynomials. (Characteristic $\neq 2, 3$)

Let $f(X) = X^4 + aX^3 + bX^2 + cX + d$ be a monic degree 4 polynomial over a field F of characteristic $\neq 2, 3$. Let E be a splitting field of $f(X)$ over F and let G be the associated Galois group.

To simplify later computations, we can always perform the change of variables $Y = X + \frac{1}{4}a$, and hence assume that our polynomial is $f(X) = X^4 + pX^2 + qX + r$.

If $f(X)$ is reducible, the computation of G reduces to the computation for lower degree polynomials. Hence we will assume that $f(X)$ is irreducible. Since the characteristic is $\neq 2$, it is separable and hence $f(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)$ for different elements $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in E$. We know that G acts transitively on these roots and, as usual, G will be identified, through its action on the roots, with a subgroup of S_4. Consider Klein's four group

$$V = \{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},$$

which is a normal subgroup of S_4 such that S_4/V is isomorphic to S_3. Let $H = G \cap V$.

Consider now the following elements of E^H:

$$\begin{cases} \theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \\ \theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \\ \theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3). \end{cases}$$

The elements of G permute the θ_i's, and hence the elementary symmetric polynomials on the θ_i's are in $E^G = F$. Our hypotheses imply that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ and a few easy computations yield:

$$\theta_1 + \theta_2 + \theta_3 = 2\sum_{i<j} \alpha_i\alpha_j = 2p,$$

$$\begin{aligned}
\theta_1\theta_2+&\theta_1\theta_3 + \theta_2\theta_3 \\
&= \Big((\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)\Big)^2 \\
&\quad + \Big((\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4)\Big)^2 + \Big((\alpha_1 + \alpha_4)(\alpha_1 + \alpha_2)\Big)^2 \\
&= (\alpha_1^2 + \alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3)^2 \\
&\quad + (\alpha_1^2 + \alpha_1(\alpha_3 + \alpha_4) + \alpha_3\alpha_4)^2 + (\alpha_1^2 + \alpha_1(\alpha_2 + \alpha_4) + \alpha_2\alpha_4)^2 \\
&= (\alpha_2\alpha_3 - \alpha_1\alpha_4)^2 + (\alpha_3\alpha_4 - \alpha_1\alpha_2)^2 + (\alpha_2\alpha_4 - \alpha_1\alpha_3)^2 \\
&= \sum_{1\le i<j\le 4} (\alpha_i\alpha_j)^2 - 6\alpha_1\alpha_2\alpha_3\alpha_4 = \sum_{1\le i<j\le 4} (\alpha_i\alpha_j)^2 - 6r \\
&= \Big(\sum_{1\le i<j\le 4} \alpha_i\alpha_j\Big)^2 - 2\sum_{i=1}^{4} \alpha_i^2 \Big(\sum_{\substack{1\le j\le k<4 \\ j,k\ne i}} \alpha_j\alpha_k\Big) - 12r \\
&= p^2 - 2\sum_{i=1}^{4} \Big(\alpha_i \sum_{\substack{1\le j\le k<4 \\ j,k\ne i}} \alpha_i\alpha_j\alpha_k\Big) - 12r \\
&= p^2 - 2\sum_{i=1}^{4} (\alpha_i q - r) - 12r \\
&= p^2 - 2\Big(\sum_{i=1}^{4} \alpha_i\Big)q - 4r = p^2 - 4r,
\end{aligned}$$

$$\begin{aligned}
\theta_1\theta_2\theta_3 &= -\Big((\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4)\Big)^2 \\
&= -\Big(\alpha_1^3 + \alpha_1^2(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_1(\alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) + \alpha_2\alpha_3\alpha_4\Big)^2 \\
&= -q^2.
\end{aligned}$$

Hence $\theta_1, \theta_2, \theta_3$ are the roots of the polynomial

$$h(X) = (X - \theta_1)(X - \theta_2)(X - \theta_3) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2,$$

which is called the *cubic resolvent* of $f(X)$.

Moreover, we have $\theta_1 - \theta_2 = -(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$ and similarly for $\theta_1 - \theta_3$ and $\theta_2 - \theta_3$, so we get:

$$\mathrm{D}(f(X)) = \Big(\prod_{1\le i<j\le 4}(\alpha_i - \alpha_j)\Big)^2 = \Big(\prod_{1\le i<j\le 3}(\theta_i - \theta_j)\Big)^2 = \mathrm{D}(h(X)),$$

and $\Delta = \prod_{1\le i<j\le 4}(\alpha_i - \alpha_j) = -\prod_{1\le i<j\le 3}(\theta_i - \theta_j)$.

We conclude that $\theta_1, \theta_2, \theta_3$ are different elements and now it is easy to check that for any $\sigma \in G$, $\sigma(\theta_i) = \theta_i$ for any $i = 1, 2, 3$ if and only if $\sigma \in H = G \cap V$. (Note that $\sigma(\theta_i) = \theta_i$ for any i implies $\sigma(\Delta) = \Delta$, so that $\sigma \in A_4 = V \cup (1\,2\,3)V \cup (1\,3\,2)V$, but $(1\,2\,3)\theta_1 = \theta_3$, ...)

Therefore we have $F(\Delta) = E^{G\cap A_4}$ and $F(\theta_1, \theta_2, \theta_3) = E^{G\cap V}$:

$$\begin{array}{ccc} & E & \\ & \bigcup| & [E : E_1] \text{ divides } 4 = |V| \\ E_1 = F(\theta_1, \theta_2, \theta_3) & & \\ & \bigcup| & [E_1 : E_2] \text{ divides } 3 = [A_4 : V] \\ E_2 = F(\Delta) & & \\ & \bigcup| & [E_2 : F] \text{ divides } 2 = [S_4 : A_4] \\ & F & \end{array}$$

We are left with several possibilities:

- If $h(X)$ is irreducible, then $|G| = [E : F]$ is a multiple of both 3 since E contains the subfield $F(\theta_1)$ and $[F(\theta_1) : F] = \deg h(X) = 3$, and 4 since $[F(\alpha_1) : F] = 4$. Hence $|G|$ is a multiple of 12, and G is a subgroup of S_4, whose order is 24. The only subgroup of S_4 of order 12 is A_4, and hence either $G = A_4$ (and $\Delta \in F$), or $G = S_4$ (and $\Delta \notin F$).

- If $h(X)$ is reducible, and $\theta_1, \theta_2, \theta_3 \in F$, then necessarily $|G| = 4$, and $G = V$. (Note that in this case $\Delta \in F$.)

- If $h(X)$ is reducible and, without loss of generality, $\theta_1 \in F$, but $\theta_2, \theta_3 \notin F$, then any $\sigma \in G$ satisfies $\sigma(\theta_1) = \theta_1$, so that

  $$\sigma \in V \cup (1\,2)V = V \cup \{(1\,2), (3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\} = D_4,$$

  the dihedral group of degree 4. Also there is a $\sigma \in G$ with $\sigma(\theta_2) \neq \theta_2$, so that G is not contained in V. Hence G is not contained in A_4 (as $D_4 \cap A_4 = V$), so we get $\Delta \notin F$. Therefore, G is a group whose order is a multiple of 4, contained in D_4, different from V and which acts transitively on $\{1, 2, 3, 4\}$. There are only two possibilities: either $G = D_4$ or $G = \langle(1\,3\,2\,4)\rangle = C_4$. In the first case $G \cap A_4 = G \cap V = V$ and the action of $\mathrm{Gal}\big(E/F(\Delta)\big) = V$ on the roots is transitive, so that $f(X)$ is irreducible over $F(\Delta)$. In the second case the action of $\mathrm{Gal}\big(E/F(\Delta)\big) = C_2$ is not transitive, and hence $f(X)$ is reducible over $F(\Delta)$.

We summarize our findings in the next table:

	$h(X)$ irreducible	$h(X)$ reducible
$\Delta \in F$	A_4	V
$\Delta \notin F$	S_4	D_4 or C_4

To obtain the roots of the equation $X^4+pX^2+qX+r=(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$ we proceed as follows. First we compute the roots of the cubic resolvent $h(X)$, which are θ_1, θ_2 and θ_3. But:

$$\begin{aligned}(\alpha_1+\alpha_2)+(\alpha_3+\alpha_4)&=0,\\ (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)&=\theta_1,\end{aligned}$$

so we get $\alpha_1+\alpha_2=\sqrt{-\theta_1}$ and $\alpha_3+\alpha_4=-\sqrt{-\theta_1}$. In a similar vein, $\alpha_1+\alpha_3=\sqrt{-\theta_2}$ and $\alpha_2+\alpha_4=-\sqrt{-\theta_2}$, and $\alpha_1+\alpha_4=\sqrt{-\theta_3}$ and $\alpha_2+\alpha_3=-\sqrt{-\theta_3}$. Besides, $\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3}=(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_1+\alpha_4)=\alpha_1^3+\alpha_1^2(\alpha_2+\alpha_3+\alpha_4)+\sum_{1\le i<j<k\le 4}\alpha_i\alpha_j\alpha_k=-q$ (recall $\alpha_1+\alpha_2+\alpha_3+\alpha_4=0$), and hence once we have chosen the square roots $\sqrt{-\theta_1}$ and $\sqrt{-\theta_2}$, the value (among the two possible ones) of $\sqrt{-\theta_3}$ is completely determined. Using again that $\alpha_1+\alpha_2+\alpha_3+\alpha_4=0$, we get

$$2\alpha_1=(\alpha_1+\alpha_2)+(\alpha_1+\alpha_3)+(\alpha_1+\alpha_4)=\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3},$$

and, in a similar vein,

$$\begin{cases}2\alpha_1=\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3},\\ 2\alpha_2=\sqrt{-\theta_1}-\sqrt{-\theta_2}-\sqrt{-\theta_3},\\ 2\alpha_3=-\sqrt{-\theta_1}+\sqrt{-\theta_2}-\sqrt{-\theta_3},\\ 2\alpha_4=-\sqrt{-\theta_1}-\sqrt{-\theta_2}+\sqrt{-\theta_3}.\end{cases}$$

9.11 Remark. The group S_5 is not solvable, so we do not have a chain of normal subgroups like the one used for S_4: $S_4\supseteq A_4\supseteq V\supseteq 1$.

§ 10. Solvability by radicals

Under what conditions can the roots of a polynomial in one variable be obtained by just using the operations of addition, subtraction, multiplication, division and extraction of roots?

10.1 Definition.

(i) An extension K/F is said to be *purely radical* if there is an element $\alpha\in K$ and a natural number $n\in\mathbb{N}$ such that $K=F(\alpha)$ and $\alpha^n\in F$. (Hence α is an n^{th} root of an element in F.)

(ii) Let $f(X)\in F[X]$ be a degree ≥ 1 polynomial over a field F. Then $f(X)$ is said to be *solvable by radicals* if there exists a 'tower' of field extensions:

$$F=K_0\subseteq K_1\subseteq K_2\subseteq\cdots\subseteq K_r=K$$

such that each K_i/K_{i-1} is purely radical ($i=1,\dots,r$) and there are $\alpha_1,\dots,\alpha_s\in K$ with $f(X)=a(X-\alpha_1)\cdots(X-\alpha_s)$. The extension K/F is said to be a *radical extension.*

10.2 Remark. A field extension K/F is then radical if $K = F(\gamma_1, \ldots, \gamma_r)$ and for each $i = 1, \ldots, r$ there is a natural number $n_i \in \mathbb{N}$ such that $\gamma_i^{n_i} \in F(\gamma_1, \ldots, \gamma_{i-1})$.

10.3 Lemma. *Let F be a field and let μ_n be the set of n^{th} roots of unity in F: $\mu_n = \{\alpha \in F : \alpha^n = 1\}$. Then μ_n is a cyclic group whose order divides n.*

Proof. It is clear that μ_n is a finite subgroup of $F^\times$, hence it is cyclic (Lemma 6.1). If γ is a generator of μ_n, then $\gamma^n = 1$, so that the order of μ_n, which equals the order of γ, divides n. □

In the event that $|\mu_n| = n$, the generators of μ_n are called the *primitive n^{th} roots of* 1. Note that if $\mu_n = \langle\zeta\rangle$ with $|\zeta| = n$, then ζ^i is a primitive n^{th} root of 1 if and only if $\gcd(i, n) = 1$.

10.4 Lemma. *Let F be a field and n a natural number. The polynomial $X^n - 1 \in F[X]$ has n different roots (in a splitting field over F) if and only if the characteristic of F does not divide n.*

Proof. Take $f(X) = X^n - 1$. Then $f'(X) = nX^{n-1}$ is $\neq 0$ if and only if the characteristic of F does not divide n, and in this case $\gcd(f(X), f'(X)) = 1$, and $f(X)$ has no multiple roots. On the contrary, if $f'(X) = 0$, then $f(X)$ contains multiple roots. □

10.5 Proposition. *Let F be a field, $n \in \mathbb{N}$, and let ζ be a primitive n^{th} root of* 1 *in a field extension of F (so that the characteristic does not divide n). Then $F(\zeta)/F$ is a Galois extension and* $\mathrm{Gal}(F(\zeta)/F)$ *is an abelian group.*

Proof. Since $\zeta \in F(\zeta)$ and the roots of $X^n - 1$ are the powers of ζ, it follows that $F(\zeta)$ is the splitting field of the separable polynomial $X^n - 1$ over F, and hence $F(\zeta)/F$ is a Galois extension.

Any $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ is determined by the value $\sigma(\zeta)$. Hence there is a one-to-one group homomorphism

$$\begin{aligned} \mathrm{Gal}(F(\zeta)/F) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto \bar{\imath} \text{ such that } \sigma(\zeta) = \zeta^i. \end{aligned}$$

But $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group, and hence so is $\mathrm{Gal}(F(\zeta)/F)$. □

10.6 Proposition. *Let F be a field and let $n \in \mathbb{N}$ such that the characteristic of F does not divide n and such that F contains all the n^{th} roots of unity (that is, $|\mu_n| = n$). Let K/F be a finite field extension. Then K/F is a Galois extension with* $\mathrm{Gal}(K/F)$ *a cyclic group whose order is a divisor of n if and only if there is an element $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^n \in F$.*

Proof. If $K = F(\alpha)$ and $\alpha^n = a \in F$, then either $a = 0$ and hence $K = F$ and $\mathrm{Gal}(K/F)$ is trivial, or K/F is a splitting field over F of the separable polynomial $X^n - a$ (whose roots are $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ for a primitive n^{th} root of unity ζ, and they all lie in F). Hence K/F is a Galois extension. Moreover, the map

$$\begin{aligned} \mathrm{Gal}(K/F) &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \bar{\imath} \text{ such that } \sigma(\alpha) = \zeta^i\alpha, \end{aligned}$$

is a one-to-one group homomorphism. Therefore $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of the cyclic group of order n, and it is thus cyclic of order a divisor of n.

Conversely, assume that K/F is a Galois field extension whose Galois group is cyclic of order a divisor of n. Let $m = |\mathrm{Gal}(K/F)|$ and let $\xi = \zeta^{n/m}$, which is a primitive m^{th} root of 1, $\xi \in F$. Let σ be a generator of $\mathrm{Gal}(K/F)$. For any $\alpha \in K$ consider the so called *Lagrange resolvent of* α:

$$(\alpha, \xi) = \alpha + \xi\sigma(\alpha) + \cdots + \xi^{m-1}\sigma^{m-1}(\alpha).$$

Note that for any i:

$$\sigma^i((\alpha, \xi)) = \sigma^i(\alpha) + \xi\sigma^{i+1}(\alpha) + \cdots = \xi^{-i}(\alpha, \xi).$$

As $1, \sigma, \ldots, \sigma^{m-1}$ are linearly independent (by Dedekind's Lemma 4.6), there is an element $\alpha \in K$ such that $(\alpha, \xi) \neq 0$. Write $\beta = (\alpha, \xi)$. Then for any i, $\sigma^i(\beta) = \xi^{-i}\beta$, so that β is not fixed under any nontrivial element in $\mathrm{Gal}(K/F)$. Therefore β does not belong to any proper subfield of K containing F. Hence $K = F(\beta)$. Besides, $\sigma(\beta^m) = \sigma(\beta)^m = (\xi^{-1}\beta)^m = \beta^m$, and hence $\beta^m \in F$. It follows that $\beta^n \in F$ too, as required. □

10.7 Theorem. *Let K/F be a radical extension and let E be an intermediate subfield: $F \subseteq E \subseteq K$. Then the Galois group* $\mathrm{Gal}(E/F)$ *is solvable.*

Proof. Some reductions will be made:

1) The extension E/F can be assumed to be a Galois extension:

Actually, $\mathrm{Gal}(E/F) = \mathrm{Gal}(E/F_0)$ where F_0 is the fixed field by $\mathrm{Gal}(E/F)$, and hence E/F_0 is a Galois extension. Besides, we have $F \subseteq F_0 \subseteq E \subseteq K$ and K/F_0 is radical too.

2) We may assume that K is a splitting field of some polynomial over F (that is, K/F is a normal extension):

To prove this note that $K = F(u_1, \ldots, u_r)$ with $u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$ for each $i = 1, \ldots, r$, for some elements u_i's in K and natural numbers m_i's. Consider the polynomial

$$f(X) = m_{u_1,F}(X)m_{u_2,F}(X)\cdots m_{u_r,F}(X) \in F[X]$$

and let $\tilde{K}$ be a splitting field of $f(X)$ over K (and hence also over F). We get the containments $F \subseteq E \subseteq K \subseteq \tilde{K}$.

If v is a root of $m_{u_j,F}(X)$ in $\tilde{K}$, there is a unique isomorphism $\tau : F(u_j) \to F(v)$ such that $\tau|_F = 1$ and $\tau(u_j) = v$, and this τ extends to an isomorphism $\sigma : \tilde{K} \to \tilde{K}$. Then $F \subseteq \sigma(K) \subseteq \tilde{K}$ and $v \in \sigma(K)$. Moreover, σ being an isomorphism, we have $v^{m_j} = \sigma(u^{m_j}) \in F\big(\sigma(u_1), \ldots, \sigma(u_{j-1})\big)$. Then with $\mathrm{Gal}(\tilde{K}/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_m\}$, the field $\tilde{K}$ is generated over F by the roots of $f(X)$, and hence it equals

$$\tilde{K} = F\big(u_1, \ldots, u_r, \sigma_2(u_1), \ldots, \sigma_2(u_r), \ldots, \sigma_m(u_1), \ldots, \sigma_m(u_r)\big),$$

which is clearly a radical extension of F. Besides, $F \subseteq E \subseteq \tilde{K}$.

3) We may assume that K/F is a Galois extension and that $E = K$.

To prove this, and since E/F is assumed to be a Galois extension (and hence E is the splitting field of some polynomial over F), we have the restriction map

$$\begin{aligned} \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(E/F) \\ \sigma &\mapsto \sigma|_E : E \to E, \end{aligned}$$

which is a group homomorphism. Also, since K is being assumed to be a splitting field, any $\tau \in \mathrm{Gal}(E/F)$ extends to a $\sigma \in \mathrm{Gal}(K/F)$. Hence this map is onto. If $\mathrm{Gal}(K/F)$ is solvable, so is $\mathrm{Gal}(E/F)$, so it is enough to prove that $\mathrm{Gal}(K/F)$ is solvable. Applying again the reduction 1), we may assume that K/F is a radical Galois extension.

4) Assume then that K/F is a radical Galois extension. Without loss of generality we may assume too that there are elements $r \in \mathbb{N}$, $u_1, \dots, u_r \in K$ and prime numbers $m_1, \dots, m_r$ such that $K = F(u_1, \dots, u_r)$ and $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$ for any $i = 1 \dots, r$. (Note that if, for instance, $K = F(u)$ with $u^{12} \in F$, then $(u^6)^2 \in F$, $(u^2)^3 \in F(u^6)$ and $u^2 \in F(u^6, u^2) = F(u^2)$, so that $K = F(u^6, u^2, u)$.)

Also note that if some m_i equals the characteristic of F, then $u_i^{m_i} \in K_{i-1} = F(u_1, \dots, u_{i-1})$, so that $m_{u_i, K_{i-1}}(X)$ divides $X^{m_i} - u_i^{m_i} = (X - u_i)^{m_i}$. But u_i is separable over F (since K/F is a Galois field extension) and hence also over K_{i-1}. Thus $m_{u_i, K_{i-1}}(X) = X - u_i$, so $u_i \in K_{i-1}$ and we can get rid of u_i in the expression $K = F(u_1, \dots, u_r)$. Hence we may assume that none of the prime numbers m_i equals the characteristic of F.

Take now $m = m_1 \cdots m_r$ and ζ a primitive m^{th} root of 1 in a field extension of K. Take $\tilde{K} = K(\zeta) = F(\zeta, u_1, \dots, u_r)$. The extension $\tilde{K}/F$ is again radical. Moreover, K is the splitting field of a separable polynomial $f(X) \in F[X]$ over F, and hence $\tilde{K}$ is a splitting field of the separable polynomial $\mathrm{lcm}(X^m - 1, f(X))$ over F, so $\tilde{K}/F$ is a Galois extension too. Since, as in reduction 3), $\mathrm{Gal}(K/F)$ is a quotient of $\mathrm{Gal}(\tilde{K}/F)$, we may change K to $\tilde{K}$ and assume $\zeta \in K$.

Thus, we assume $K = F(\zeta, u_1, \dots, u_r)$, with $u_i^{m_i} \in F(\zeta, u_1, \dots, u_{i-1})$, the m_i's being prime numbers different from the characteristic. Take $K_0 = F(\zeta)$, and $K_i = F(\zeta, u_1, \dots, u_i)$ for any $i = 1, \dots, r$:

$$\begin{array}{ccc} K_r = K & & 1 \\ \bigcup| & & \bigcap| \\ \vdots & & \vdots \\ \bigcup| & \text{Galois} & \bigcap| \\ K_1 = F(\zeta, u_1) & \longrightarrow & G_1 = \mathrm{Gal}(K/K_1) \\ \bigcup| & \text{correspondence} & \bigcap| \\ K_0 = F(\zeta) & & G_0 = \mathrm{Gal}(K/K_0) \\ \bigcup| & & \bigcap| \\ F & & G = \mathrm{Gal}(K/F) \end{array}$$

But K_0/F is a Galois extension, and hence G_0 is a normal subgroup of G with $G/G_0 \simeq \mathrm{Gal}(K_0/F)$, which is abelian by Proposition 10.5. Since $\zeta \in K_{i-1}$ for any $i \geq 1$, the extension K_i/K_{i-1} is a cyclic Galois extension (Proposition 10.6), and hence G_i is a normal subgroup of G_{i-1} and $G_{i-1}/G_i \simeq \mathrm{Gal}(K_i/K_{i-1})$ is a cyclic group.

We then have the descending series of subgroups $G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq 1$, with abelian quotients, and hence G is solvable. □

10.8 Corollary. *Let $f(X) \in F[X]$ be a degree ≥ 1 polynomial over a field F which is solvable by radicals. Then the Galois group of $f(X)$ is solvable.*

10.9 Corollary. *There are polynomials of degree ≥ 5 which are not solvable by radicals.*

Proof. Recall that $\mathrm{Gal}(F(x_1,\ldots,x_n)/F(s_1,\ldots,s_n))$ is isomorphic to the symmetric group S_n, which is not solvable for $n \geq 5$. Therefore the general polynomial of degree $n \geq 5$ is not solvable by radicals.

For a more concrete example, take $f(X) = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Then $f(X)$ is irreducible (Eisenstein's Criterion). Let E be the splitting field of $f(X)$ with $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$, and let $G = \mathrm{Gal}(E/\mathbb{Q})$. Let us check that G is not solvable.

The derivative $f'(X) = 5X^4 - 4$, considered as a function of a real variable, grows for $x \geq 0$ and decreases for $x \leq 0$. It follows then easily that $f(X)$ has at most three real roots. But $f(-1) > 0$ and $f(1) < 0$, while $\lim_{x\to-\infty} f(x) = -\infty$, $\lim_{x\to\infty} = \infty$. It follows that $f(X)$ has exactly three different real roots: $\alpha_1, \alpha_2, \alpha_3$, and two non real complex roots: $\alpha_4, \alpha_5 = \bar{\alpha}_4$.

By irreducibility of $f(X)$, $5 = [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$ divides $|G|$, and hence G contains an element of order 5. Identify G with a subgroup of S_5 through its action on the roots. This means that G contains a cycle of length 5. On the other hand, the restriction σ of the complex conjugation to E gives a transposition in G. But an arbitrary cycle of length 5 and an arbitrary transposition generate S_5 (you have essentially proved this as an exercise in Chapter 1). Hence G is the whole S_5, which is not solvable. □

Finally, a partial converse to the previous theorem will be proved.

10.10 Proposition. *Let E/F be a Galois extension with solvable $\mathrm{Gal}(E/F)$ and such that the characteristic of F does not divide $[E : F]$. Then there is a field K with $F \subseteq E \subseteq K$ such that the extension K/F is radical.*

Proof. Again we will start with a reduction:
1) It can be assumed that F contains the roots of unity of order $[E : F]$.

Actually, let ζ be a primitive root of 1 of order $[E : F]$ (which is not a multiple of the characteristic) in some extension of E. Now E is a splitting field of some separable polynomial $f(X) \in F[X]$ over F, so that $E(\zeta)$ is a splitting field of the separable polynomial $\mathrm{lcm}(f(X), X^{[E:F]} - 1)$ over F, and hence the extension $E(\zeta)/F$ is a Galois extension, and so is the extension $E(\zeta)/F(\zeta)$. Note also that the map

$$\begin{array}{ccc} \mathrm{Gal}(E(\zeta)/F(\zeta)) & \longrightarrow & \mathrm{Gal}(E/F) \\ \sigma & \mapsto & \sigma|_E, \end{array}$$

is a one-to-one group homomorphism, which shows that $\mathrm{Gal}(E(\zeta)/F(\zeta))$ is solvable and $[E(\zeta) : F(\zeta)]$ divides $[E : F]$, so it is not a multiple of the characteristic. Finally, if K is an extension of $E(\zeta)$ such that $K/F(\zeta)$ is radical, then K/F is radical too. (Note that $\zeta^{[E:F]/[E(\zeta):F(\zeta)]}$ is a primitive root of unity of order $[E(\zeta) : F(\zeta)]$.)

2) Assuming that F contains the roots of unity of order $[E : F]$, take $G = \mathrm{Gal}(E/F)$. Since G is solvable, there is a normal subgroup H of G such that $[G : H]$ is a prime number p (just take for H any maximal subgroup containing G'). Using an inductive argument, since E/E^H is a Galois extension, we may assume that there is a radical extension K/E^H with E contained in K: $F \subseteq E^H \subseteq E \subseteq K$. But $|\mathrm{Gal}(E^H/F)| = p$, which implies that $\mathrm{Gal}(E^H/F)$ is cyclic, and hence $E^H = F(\alpha)$ with $\alpha^p \in F$ (Proposition 10.6). In particular, E^H/F is radical, and hence so is K/F. □

10.11 Lemma. *Let $f(X) \in F[X]$ be a polynomial of degree $n \geq 1$ over a field F, and let E be a splitting field of $f(X)$ over F. Then if p is a prime factor of $[E : F]$, then p is lower than or equal to n ($p|n!$).*

Proof. We proceed by induction on n, the case $n = 1$ being trivial.

For $n > 1$, let α be a root of $f(X)$ in E: $f(X) = (X-\alpha)g(X)$ in $F(\alpha)[X]$. Hence $[E : F] = [E : F(\alpha)][F(\alpha) : F]$. If p is a factor of $[F(\alpha) : F]$ the result is clear since $[F(\alpha) : F] \leq \deg f(X) = n$. Otherwise p divides $[E : F(\alpha)]$ and by the inductive hypothesis (E is a splitting field of $g(X)$ over $F(\alpha)$) we conclude $p \leq n - 1 = \deg g(X)$. □

Our last result is due to Galois:

10.12 Theorem. *Let $f(X) \in F[X]$ be a degree $n \geq 1$ polynomial over a field F whose characteristic does not divide $n!$ (that is, either the characteristic is 0 or greater than n). Then $f(X)$ is solvable by radicals if and only if its Galois group is solvable.*

Proof. If $f(X)$ is solvable by radicals, then we already know that its Galois group is solvable (Corollary 10.8).

Conversely, assume that the Galois group of $f(X)$ is solvable, and let E be a splitting field of $f(X)$ over F. Take a complete factorization of $f(X)$: $f(X) = ag_1(X)^{r_1} \cdots g_m(X)^{r_m}$, with $0 \neq a \in F$ and the $g_i(X)$'s different monic irreducible polynomials. Because of our restrictions on the characteristic $g_i'(X) \neq 0$ for any i, so that the $g_i(X)$'s are separable, and E is a splitting field of the separable polynomial $g_1(X) \cdots g_m(X)$ over F. Therefore E/F is a Galois extension. Now the previous proposition gives the result. □

Exercises

1. Prove that any degree 2 field extension is normal.
2. Let F be a field of characteristic $p > 0$ and let $t \in F$. Prove that the polynomial $f(X) = X^p - X - t$ has no multiple roots, and that if α is a root in some field extension, then the set of its roots is $\{\alpha + \gamma : \gamma \in \mathbb{F}_p\}$. Conclude that $F(\alpha)$ is a splitting field of $f(X)$ over F.
3. Consider a chain of subfields $F \leq E \leq K$. Check whether the following assertions are valid:
   (a) If K/F is normal, then K/E is normal.
   (b) If K/F is normal, then E/F is normal.
   (c) If E/F and K/E are normal, then K/F is normal.
4. Check whether the following polynomials are separable over the field F: X^2+2X-1, X^3+1, and $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, where F is either $\mathbb{Q}$ or $\mathbb{F}_p$ with $p = 2, 3, 5$.
5. Let K/F be a finite field extension whose degree is not a multiple of the characteristic. Prove that K/F is separable. Is the converse true?

6. Compute the Galois group $\mathrm{Gal}(F/\mathbb{Q})$, where F is a splitting field of each of these polynomials:
   - $X^2 - 2$,
   - $X^3 - 2$,
   - $X^5 - 2$,
   - $(X^2 - 2)(X^3 - 2)$,
   - $X^6 - 9$,
   - $(X^3 - 2)(X^4 - 2)$.

7. This exercise is designed to provide a proof of the *Fundamental Theorem of Algebra*, different from the one given in *Algebraic Structures*. This proof will use the following facts.
   - Any positive real number has a positive square root.
   - Any real polynomial of odd degree has a real root.

   Prove the following assertions:
   (a) $\mathbb{C}$ does not have extensions of degree 2.
   (b) $\mathbb{R}$ does not have proper extensions of odd degree.

   Now let $f(X) \in \mathbb{R}[X]$ be an irreducible real polynomial, and let K be a splitting field of $f(X)$ over $\mathbb{R}$.
   (c) Prove that $K(i)/\mathbb{R}$ is a Galois extension, where i denotes a root of $X^2 + 1$ in some extension of K.
   (d) Write $[K(i) : \mathbb{R}] = 2^n m$ for $n \geq 0$ and odd m. Prove that $m = 1$ by considering the fixed field of a Sylow 2-subgroup of the Galois group.
   (e) Prove that $n = 1$ by arguing with index 2 subgroups of the Galois group.
   (f) Conclude that $f(X)$ splits over $\mathbb{C}$.

8. Prove that an arbitrary finite field has irreducible polynomials of arbitrary degree.

9. Prove that the polynomial $X^{p^n} - X$ is the product of all the irreducible monic polynomials over $\mathbb{F}_p$ whose degree divides n.

10. Let F be a subfield of $\mathbb{R}$, and let $f(X) \in F[X]$ be a degree 3 irreducible polynomial. Then prove the following assertions:
    (a) $\mathrm{D}(f(X)) > 0$ if and only if the three roots of $f(X)$ are real.
    (b) $\mathrm{D}(f(X)) < 0$ if and only if $f(X)$ has only one real root.

11. Let F be a field of characteristic $\neq 2$, and let $f(X) \in F[X]$ be a degree 3 polynomial whose discriminant is a square in F. Prove that either $f(X)$ is irreducible or $f(X)$ splits in F.

12. Prove that over any field F either the cubic polynomial $X^3 - 3X + 1$ is irreducible or it splits over F.

13. Let F be a field of characteristic $\neq 2$, and let $f(X) = X^4 + bX^2 + c \in F[X]$ be an irreducible polynomial. Let G be its Galois group. Prove the following assertions:

    (a) If c is a square in F then $G \simeq C_2 \times C_2$.

    (b) If c is not a square in F but $c(b^2 - 4c)$ is a square in F, then $G \simeq C_4$.

    (c) If neither c nor $c(b^2 - 4c)$ are squares in F, then G is isomorphic to the dihedral group D_4.

14. Compute the Galois group over $\mathbb{Q}$ of the following polynomials:

    (a) $X^3 - 3X + 1$,

    (b) $X^3 + 3X^2 - X - 1$,

    (c) $X^4 - X + 1$,

    (d) $X^4 - 6X^2 + 8X + 28$,

    (e) $X^4 - 2$,

    (f) $X^4 + 4X^2 + 2$,

    (g) $X^4 + 1$,

    (h) $(X^4 - 2)(X^4 - 3)$.

15. For any $n \in \mathbb{N}$ consider the polynomial $\Phi_n(X) = (X - \zeta_1) \cdots (X - \zeta_r)$ where $\zeta_1, \ldots, \zeta_r$ are the primitive n^{th} roots of unity in $\mathbb{C}$. $\Phi_n(X)$ is called the n^{th} *cyclotomic polynomial*. Prove the following assertions:

    (a) $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

    (b) $\Phi_n(X) \in \mathbb{Z}[X]$.

    (c) $\Phi_n(X)$ is irreducible (as a polynomial in $\mathbb{Q}[X]$).

    (d) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, where ϕ denotes the Euler map, and ζ a primitive n^{th} root of unity, and $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

16. Prove that if $n \geq 3$, the regular polygon of n vertices is constructible with ruler and compass if and only if $n = 2^m p_1 \cdots p_r$, where $m, r \geq 0$ and $p_1, \ldots, p_r$ are Fermat primes (that is, of the form $2^{2^m} + 1$).

[15] To show that $\Phi_n(X)$ is irreducible assume the contrary. Then $\Phi_n(X) = f(X)g(X)$ for two monic degree ≥ 1 polynomials in $\mathbb{Z}[X]$, with $f(X)$ irreducible. Then show that there is a primitive root ζ and a prime number p which does not divide n such that $f(\zeta) = 0 \neq f(\zeta^p)$. Conclude that $f(X)$ divides $g(X^p)$. Now reduce modulo p (and use bars to denote the reductions) and show that $\bar{\Phi}_n(X)$ has multiple roots. Get from here a contradiction.