Humboldt–Universität zu Berlin
Galois Theorie Algebraischer Gleichungen
WS 2012/2013

A course given by
Dr. Fares Maalouf

Contents

1 Historical problems

1.1 Compass and straightedge constructions

The plane is identified with the field $\mathbb{C}$ of complex numbers. We fix a set P of points of the plane. We suppose that P contains 0 and 1 (usually $P = \{0, 1\}$). For each $n > 0$, we define *the set P_n of points of the plane constructible in n steps form P using compass and straightedge*. We set $P_0 := P$. The set P_n is defined by adding to P_{n-1} all the points which are:

1. intersections of two straight lines, each containing at least two distinct points of P_{n-1}
2. intersections of two circles centered at points of P_{n-1}, and having their radii equal to distances between points of P_{n-1}
3. intersections of a straight line containing at least two distinct points of P_{n-1} with a circle centered at a point of P_{n-1} and with radius equal to the distance between two points of P_{n-1}.

The union $K(P) := \bigcup_{n\in\mathbb{N}} P_n$ is called *the set of points constructible from P using straightedge and compass*. The set $K(\{0, 1\})$ is called ***the set of constructible points***.

Exercise 1.1. All the elements of $\mathbb{Q} + i.\mathbb{Q}$ are constructible.

Lemma 1.2. *Let P be a subset of $\mathbb{C}$. Then the sum and product of two elements of $K(P)$ are in $K(P)$. The conjugate, opposite, inverse and square roots of an element of $K(P)$ are in $K(P)$.*

We say that a subfield L of $\mathbb{C}$ is stable under taking square roots if and only if for any $x \in \mathbb{C}$, if $x^2 \in L$ then $x \in L$.

Remark 1.3. Let $P \subset \mathbb{C}$. The set of subfields of $\mathbb{C}$ containing P and closed under taking square roots and complex conjugates is not empty, since it contains $\mathbb{C}$. The intersection of all the fields of this set is the smallest field containing P and closed under taking square roots and complex conjugates. Denote this field by $K_2(P)$.

Lemma 1.4. *Let $L \subset \mathbb{C}$ be a field stable under taking complex conjugates and square roots. Then for any element $z = x + i.y \in \mathbb{C}$, $z \in L$ if and only if $x, y \in L$.*

Proposition 1.5. *Let $P \subset \mathbb{C}$. Then the set $K(P)$ of constructible points from P is the smallest field containing P and closed under taking complex conjugates and square roots. So $K(P) = K_2(P)$.*

Proof. By Lemma 1.2, the set $K(P)$ is a field closed under taking square roots and complex conjugates. So $K_2(P) \subset K(P)$. The other inclusion is done by induction, showing that for any n, $P_n \subset K_2(P)$. This is clear for $n = 0$. Suppose that $P_n \subset K_2(P)$. Then by Lemma 1.4, all the coordinates of all the elements of P_n are elements of $K_2(P)$. It is easy to check that the coordinates of all elements of P_{n+1} are in $K_2(P)$, hence again by Lemma 1.4, $P_{n+1} \subset K_2(P)$. $\square$

Deciding whether a point a is constructible comes then to the same as deciding whether a is an element of $K_2(\{0,1\})$. It is easy to show that a is in $K_2(\{0,1\})$ if and only if there exists a tower of subfields of $\mathbb{C}$:

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n$$

such that $a \in K_n$, and for any $0 < i \leq n$, K_i is generated by $\sqrt{a_i}$ over K_{i-1}, for some $a_i \in K_{i-1}$. For this, one can check easily by induction that the set of such a is a field, closed under taking square roots and complex conjugates, and that this field is contained in $K_2(P)$.

We will come back later to the straightedge and compass constructions. We will show that $\sqrt[3]{2}$ is not constructible, and this shows that the cube doubling problem (also known as the Delian problem) is unsolvable. This problem involves drawing a cube with twice the volume of a given cube, using only a straightedge and a compass. The number $cos(\frac{\pi}{9})$ will also be shown not to be constructible. This shows the impossibility of angle trisection in the general case, using only a straightedge and a compass (note that there are constructible points A, B, C, with $[\vec{AB}, \vec{AC}] = \frac{\pi}{3}$). We will also give a characterization of constructible regular n-gons.

1.2 Expressing the roots of polynomial equations.

Another historical problem concerns finding solutions to polynomial equations. It can be shown that any polynomial $P \in \mathbb{C}[X]$ with degree n has n roots in $\mathbb{C}$ - counting with multiplicities. The problem is to calculate these roots.

We start first with an intuitive notion. Let L be a field, $(a_i)_{i\in I}$ be a family of elements of L, and $a \in L$. We say that a has an *algebraic expression in the* a_i, (or over the family $(a_i)_{i\in I}$), if a can be obtained from the a_i using the four arithmetic operations, and taking roots of arbitrary degree.
So the complex numbers

$$\sqrt{2}, \quad \frac{1}{\sqrt{2}+\sqrt{3}}, \quad \frac{1+\sqrt[7]{2-\sqrt{1-\frac{3}{\sqrt[3]{5}}}}}{3+\sqrt{-1}}$$

have algebraic expressions over $\mathbb{Q}$. In our notations, each of the above expressions has many possible values.

Let $P \in \mathbb{C}[X]$ be a polynomial of degree two. Then the roots of P can be expressed algebraically in its coefficients. The same will be shown to hold for polynomials of degree 3 and 4. However, we will show that the roots of the polynomial $X^5 - 4X + 2$ do not have algebraic expressions over $\mathbb{Q}$.

Definition 1.6. Let $K \subset L$ be two fields.

1. Let $a \in L$ and $n \in \mathbb{N}^*$. Then a is said to be a n^{th}***-root*** over K if $a^n \in K$.

2. The field K is said to be closed in L under taking roots if whenever $a \in L$ is a n^{th}-root over K, then $a \in K$.

Given two fields $K \subset L$, we denote by K_L^r, or by K^r if there is no possible confusion, the set of elements of L having an algebraic expression over K. It can be easily shown by induction on the number of operations needed to express algebraically an element $a \in K_L^r$ over K, that K_L^r is the set of elements $a \in L$ such that there exists a tower of subfields of L:

$$K_0 = K \subset K_1 \subset \cdots \subset K_n$$

with $a \in K_n$, and for any $0 < i \leq n$, K_i is generated by some $\sqrt[n_i]{a_i}$ over K_{i-1}, for some $a_i \in K_{i-1}$ and $n_i \in \mathbb{N}^*$. As above, one shows by induction that K_L^r is the smallest subfield of L containing K and closed under taking roots.

Denote by $\mathbb{Q}^{alg}$ the set those elements of $\mathbb{C}$ which are roots of some polynomial $P \in \mathbb{Q}[X]$. We will show later that $\mathbb{Q}^{alg}$ is a field, it is called *the field of algebraic numbers.* It is clear that $\mathbb{Q}^{alg}$ is closed under taking roots. So we have

$$\mathbb{Q} \subset \mathbb{Q}^r \subset \mathbb{Q}^{alg} \subset \mathbb{C}.$$

The first inclusion is strict, since $\sqrt{2}$ is in $\mathbb{Q}^r$ and not in $\mathbb{Q}$, and the last is strict for cardinality reasons (exercise), or by Exercise 5.3. One of the aims of this lecture is to show that the second inclusion is strict as well. Equivalently to what has been claimed above, the roots of the polynomial $X^5 - 4X + 2$ are obviously in $\mathbb{Q}^{alg}$, but will be shown not to be in $\mathbb{Q}^r$.

2 Introduction

2.1 Fields and field extensions

Definition 2.1. Let $(K, +, ., 0, 1)$ be a field. The ***characteristic*** $char(K)$ of K is the smallest natural number n such that $n.1 = 0$ when such a number exists, and 0 in the other case.

Lemma 2.2. *If $char(K) = n > 0$, then n is a prime number.*

Proof. Suppose for a contradiction that the characteristic of K is a non prime number n, and let $1 < a, b < n$ be such that $n = a.b$. By the definition of $char(K)$, we have that $a.1 \neq 0$. Let $\alpha \in K$ be the multiplicative inverse of $a.1$, so $\alpha.(a.1) = 1$. Now we have that

$$0 = \alpha.0 = \alpha.(n.1) = \alpha.((a.b).1) = \alpha.((a.1).(b.1)) = (\alpha.(a.1)).(b.1) = 1.(b.1) = b.1$$

So $b.1 = 0$ and $b < n$. This contradicts the definition of n. □

The following can be easily checked.

Remark 2.3. Let K be any field. The application Φ which to each $n \in \mathbb{Z}$ associates the elements $n.1 \in K$ defines a ring homomorphism between $\mathbb{Z}$ and a subring of K. If $char(K) = 0$, then Φ is injective, and the ring $\mathbb{Z}$ of integers can be regarded as a subring of K. In this case, Φ can be extended to a field isomorphism between $\mathbb{Q}$ and a subfield of K, so $\mathbb{Q}$ can be regarded as a subfield of K. Now if the characteristic $char(K)$ of K is a prime number p, then the kernel of Φ is the ideal $p.\mathbb{Z}$, and Φ factors into an isomorphism between F_p and a subfield of K. So in this case, F_p can be regarded as a subfield of K.

Definition 2.4.

1. Let K, L be two fields. We say that L is an *extension* of K or that L/K is a ***field extension*** if K is a subfield of L.
2. Given an extension M of a field L which is in turn an extension of a field K, then L is said to be an ***intermediate field*** (or *intermediate extension*) of the field extension (M/K).

It is easy to check that if K is a field and L is a ring containing K, then L can be canonically endowed with a K-vector space structure. So if (L/K) is a field extension, then L is a K-vector space, and moreover L and K have the same characteristic.

Definition 2.5. Let (L/K) be a field extension. The ***dimension*** of the extension (L/K), denoted by $[L : K]$, is the dimension of L as a K-vector space. If this dimension is finite (respectively infinite) we say that L is a finite (respectively infinite) extension of K, or that the extension (L/K) is finite (respectively infinite).

Proposition 2.6. *Let (M/K) be a field extension, and L be an intermediate field. Then $[M : K] = [M : L].[L : K]$*

Proof. □

Remark 2.7. The above formula shows that $[M : L]$ and $[L : K]$ divide $[M : K]$.

Corollary 2.8. *Let $K_1 \subset K_2 \subset \cdots K_n$ be a tower of fields. Then*

$$[K_n : K_1] = [K_n : K_{n-1}].[K_{n-1} : K_{n-2}]. \cdots .[K_2 : K_1].$$

Proof. Obvious by induction. □

Corollary 2.9. *Let M, L and K be as above. If $[M : K]$ is finite, then both $[M : L]$ and $[L : K]$ are finite.*

Proof. If $m_1, \cdots m_n$ are n different $L-$linearly independent elements of M, and $l_1, \cdots l_p$ are p different $K-$linearly independent elements of L, then the above arguments shows that the $m_i l_j$ are K-linearly independent elements of M. So $n.p \leq [M : K]$, and both $[M : L]$ and $[L : K]$ are $\leq [M : K]$. □

Notation: For a field K and a free variable X, $K[X]$ denotes the ring of polynomials in X with coefficients in K, and $K(X)$ denotes the field of rational functions in X with coefficients in K.

Proposition 2.10.
1. *Let K, L be two rings with $K \subset L$, and let A be a subset of L. Then there is a unique ring R with $K \subset R \subset L$ containing A and minimal for the inclusion among the rings I containing A with $K \subset I \subset L$. This ring is denoted by $K[A]$.*
2. *The ring $K[A]$ is the set $\mathcal{E}$ of elements of L of the form $T(a_1, \cdots, a_n)$ where T is a polynomial of $K[X_1, \cdots, X_n]$ and the a_i are elements of A.*

Proof.
1. Let $\mathcal{P}$ be the set of rings I containing A, with $K \subset I \subset L$. The set $\mathcal{P}$ is not empty, since $L \in \mathcal{P}$. Let $K[A]$ be the intersection of all the rings from $\mathcal{P}$. It is obvious that $K[A]$ is the unique minimal ring R containing A and satisfying $K \subset R \subset L$.
2. It is clear that an element of $\mathcal{E}$ is contained in any ring I containing A and satisfying $K \subset I \subset L$. On the other hand, it is clear that $\mathcal{E}$ is a ring. So $\mathcal{E} = K[A]$.

□

The ring $K[A]$ is called the *ring generated by A over K*. If $A = \{a_1, \cdots, a_n\}$, then $K[A]$ will be denoted by $K[a_1, \cdots, a_n]$. It can be easily checked that $K[A \cup B] = K[A][B]$.

Proposition 2.11.
1. *Let L/K be a field extension, and A be a subset of L. Then there is a unique intermediate field of the extension L/K, denoted by $K(A)$, containing A, and minimal for the inclusion among the intermediate fields containing A.*
2. *$K(A)$ is the set $\mathcal{E}$ of elements of L of the form*

$$\frac{T(a_1, \cdots, a_n)}{U(a_1, \cdots, a_n)}$$

where T and U are polynomials of $K[X_1, \cdots, X_n]$ and the a_i are elements of A with $U(a_1, \cdots, a_n) \neq 0$.

Proof.
1. Let $\mathcal{P}$ be the set of intermediate fields containing A. The set $\mathcal{P}$ is not empty, since $L \in \mathcal{P}$. Let $K(A)$ be the intersection of all the fields from $\mathcal{P}$. It is obvious that $K(A)$ is the unique minimal intermediate field containing A.
2. It is clear that an element of $\mathcal{E}$ is contained in any intermediate field containing A. On the other hand, it is clear that $\mathcal{E}$ is a field. So $\mathcal{E} = K(A)$.

□

The extension $K(A)$ is called the ***extension generated by A over K.*** If $A = \{a_1, \cdots, a_n\}$, then $K(A)$ is often denoted by $K(a_1, \cdots, a_n)$. It can be easily checked that $K(A \cup B) = K(A)(B)$.

Definition 2.12. Let K be a field, and P be a polynomial with coefficients in K. A ***splitting field*** of P over K is any extension L of K, in which P splits into linear factors, and which is minimal for inclusion with this property.

2.2 Polynomials

2.2.1 Basic definitions and properties

For a field K and a variable X, we denote by $K[X]$ the ring of polynomials in X with coefficients in K. A basic fact about $K[X]$ is that it is a Euclidean domain. Euclidean domains are domains endowed with a Euclidean function, or norm function, for which a division algorithm holds. In $K[X]$, the norm of a polynomial is defined as being its degree (the norm of the zero polynomial is $-\infty$). For two polynomials $A, B \in K[X]$, there exist unique polynomials $Q, R \in K[X]$ with $deg(R) < deg(B)$, and such that

$$A = Q.B + R.$$

The polynomials Q and R are called respectively the *quotient* and the *remainder* of the division.

By uniqueness, it is easy to see that the quotient and remainder are independent of the field K in the following sense: if L is an extension of K, then the quotient and remainder of P divided by P' are unchanged, independently of whether P, P' are considered as polynomials in $K[X]$ or $L[X]$.

So in the Euclidean domain $K[X]$, the Euclidean algorithm holds. This algorithm yields for two polynomials A and B their greatest common divisor (gcd). This is the unique monic polynomial with the highest possible degree, dividing both A and B. Furthermore, if $gcd(A, B) = G$, then the Euclidean Algorithm gives an expression of G of the form:

$$G = U.A + V.B,$$

for some polynomials $U, V \in K[X]$. The polynomials P and Q are said to be relatively prime if $gcd(P, Q) = 1$.

Proposition 2.13. *Let $P, Q \in K[X] \setminus \{0\}$ and L be an extension of K. Then $gcd(P, Q)$ is unchanged, independently of whether P and Q are considered as polynomials in $K[X]$ or $L[X]$. In particular, P divides Q in $K[X]$ if and only if P divides Q in $L[X]$, and $gcd(P, Q) = 1$ in $K[X]$ if and only if $gcd(P, Q) = 1$ in $L[X]$.*

Proof. Let D and D' be the gcd of P and Q in K and L respectively. Every polynomial in $K[X]$ is also a polynomial in $L[X]$. So in $L[X]$, the polynomial D divides P and Q, so it divides D'.
Let $U, V \in K[X]$ be such that $D = UP + VQ$. In $L[X]$, the polynomial D' divides P and Q, so it divides D (in $L[X]$).
Consequently, the monic polynomials D and D' divide each other in $L[X]$, and so they are equal. $\square$

Every Euclidean domain is a principal ideal domain (PID). So every ideal I of $K[X]$ can be generated by some polynomial P, in which case we write $I =< P >$. This is a direct consequence of the Euclidean algorithm: take for P any non-zero element of I with minimal degree. For any element $A \in I$, let $Q, R \in K[X]$ be such that $A = Q.P + R$, with $deg(R) < deg(P)$. The polynomials A and P are in the ideal I, so the same holds for $R = A - Q.P$. But $deg(R) < deg(P)$, and by definition, the degree of P is the smallest possible degree of a non-zero element of I, so $R = 0$. This shows that every element of I is a multiple of P, thus $I =< P >$.

In an integral domain, we have the notions of irreducible and prime elements. Let a be a non-unit element. Then a is said to be ***irreducible***, if it is not the product of two non-units. a is said to be ***prime*** if whenever a divides a product $\alpha.\beta$, then a divides α or a divides β. In an integral domain, every prime is irreducible, and in principal ideal domains, the two notions coincide. A consequence of this fact is the following

Proposition 2.14. *Let K be a field, X be a free variable, and $P \in K[X]$ be an irreducible polynomial of degree n. Then $K[X]/ < P >$ is an integral domain and a n dimensional vector space over K.*

$K[X]/ < P >$ is in fact a field.

Proposition 2.15. *Let K be a field, and L be an integral domain containing K which is a finite dimensional K-vector space. Then L is a field.*

Proof. Let $a \neq 0$ be any element of L. Since the dimension of L is finite over K, the elements $1, a, a^2, \cdots, a^i, \cdots$ are K-linearly dependent. Let

$$k_m.a^m + k_{m+1}.a^{m+1} + k_{m+2}.a^{m+2} + \cdots + k_n a^n = 0$$

be a non trivial K-linear combination of the $a^i, m \leq i \leq n$, for some $m < n \in \mathbb{N}$, with $k_m \neq 0$. So

$$k_m.a^m = -k_{m+1}.a^{m+1} - k_{m+2}.a^{m+2} - \cdots - k_n a^n.$$

Now k_m is invertible in K, and L is an integral domain. This yield

$$1 = a.(-\frac{k_{m+1}}{k_m} - \frac{-k_{m+2}}{k_m}.a - \cdots - \frac{k_n}{k_m}a^{n-m-1}).$$

So a is invertible in L, and this holds for any $a \in L$ with $a \neq 0$. So L is a field. □

Proposition 2.16. *Let K be a field and $P \in K[X]$ be a non-constant irreducible polynomial of degree n. Then $L := K[X]/ < P >$ is a field, and it is an extension of K in which P has a root.*

Proof. Note first that the result is obvious if the degree of P is 1: in this case P has a root in K. Denote by $\bar{X}$ the class of the polynomial X modulo $< P >$. By Proposition 2.14, L is an integral domain. Furthermore, L is spanned by $\bar{X}$ over K, and in L, we have that $P(\bar{X}) = P(X)/ < P >= 0$. So $\bar{X}$ is algebraic over K, and the integral domain L is a finite dimensional K-vector space, spanned by $1, \bar{X}, \bar{X}^2, \cdots, \bar{X}^{n-1}$. By Proposition 2.15, the integral domain L is a field. So L/K is a field extension which contains a root of P. □

Proposition 2.17. *Let K be a field and $P \in K[X]$. Then there is an extension L of K which is a splitting field of P.*

Proof. Fix $P \in K[X]$ of degree n. It is enough to show that there is an extension M of K in which P splits into linear factors $(X - x_1).(X - x_2). \cdots .(X - x_n)$. Then the subfield L of M defined by $L := K(x_1, \cdots, x_n)$ is a splitting field of P.
The existence of such a field M will be proved by induction on the degree n of P, and for all fields at the same time. If P splits into linear factor in K, then take $M = K$. If not, let $P_1 \in K[X]$ be any irreducible factor of P, and let M_1 be an extension of K containing a root α_1 of P_1. Let Q_1 be a polynomial of $M_1[X]$ such that $P = (X - \alpha_1).Q_1$. So Q_1 has degree $n-1$, and by the induction hypothesis, there is an extension M of M_1 in which Q_1 splits into linear factors. It is clear that P splits in M into linear factors.
□

Another basic fact about a polynomial rings, and any other PID, is that it is a unique factorization domain. This means that every element can be represented as a product of irreducible elements, and this representation is unique up to units and permutations of the terms.

Proposition 2.18. *Let $P \in K[X]$ be a non-zero polynomial and let a be an element of K. Then a is a root of P if and only if $X - a$ divides P.*

Proof. Clear by the division algorithm. □

Proposition 2.19. *Let $P \in K[X]$ be a non-zero polynomial. Then the number of roots of P in any extension of K is less than or equal to the degree of P.*

Proof. Let L be an extension of K, and consider P as an element of $L[X]$. The proof is done by induction on the degree of P. If this degree is 1, or P has no roots in L, then the statement is clear. Suppose the statement is proved for polynomials of degree n, and let $P \in L[X]$ with $deg(P) = n + 1$. Let $a \in L$ be a root of P. By the preceding lemma, there is a polynomial $Q \in L[X]$ such that

$$P(X) = (X - a).Q(X).$$

Now since L is an integral domain, any root of $P(X)$ is a root of $X - a$ or $Q(X)$. The polynomial $X - a$ has one root, namely a, and Q has at most n roots by the induction hypothesis and the fact that $deg(Q) = n$, so P has at most $n + 1$ roots. □

2.2.2 Derivatives and multiple roots

The derivative of polynomials is defined in the usual way. For

$$P = \sum_{i=0}^{n} a_i X^i \in K[X],$$

the derivative ∂P of P is the polynomial

$$\partial P = \sum_{i=0}^{n-1} i.a_i X^{i-1} \in K[X].$$

A simple fact about derivatives is the following identity for any two polynomials P and Q:

$$\partial(PQ) = P.\partial Q + Q.\partial P$$

Now let $P \in K[X]$. Suppose that in some extension L of K the polynomial P has a multiple root a. Then in there is a polynomial $Q \in L[X]$ such that $P = (X-a)^2.Q$, and we have the following identity in $L[X]$:

$$\partial P = (X-a)^2.\partial Q + 2(X-a).Q = (X-a).((X-a).\partial Q + 2.Q)$$

So $\partial P(a) = 0$, and in L, P and ∂P are not relatively prime, as both are divisible $X - a$. By Proposition 2.13, P and ∂P are not relatively prime in $K[X]$. Conversely, if a is not a multiple root of P, so we can write P as a product $(X-a).Q$ where $Q(a) \neq 0$. Then $\partial(P)(a) = Q(a) \neq 0$, and $P, \partial P$ have no common roots in any extension of K, they are then relatively prime. We have then the following:

Proposition 2.20. *Let K be a field and $P \in K[X]$. Then P has a multiple root in some (or any) extension of K if and only if $gcd(P, \partial P) \neq 1$. Furthermore, the multiple roots of a polynomial P are exactly the common roots to P and ∂P.*

Example. In characteristic 5, the polynomial $P = X^5 - 2^5 = (X-2)^5$ has all its roots equal to 2. The derivative ∂P of P is obviously 0, so $gcd(P, \partial P) = P$.

Proposition 2.21. *Let K be any field and P be an irreducible polynomial over K. Then P has a multiple root in some (or any) extension of K if and only $\partial P = 0$. In particular, if $char(K) = 0$ then all the roots of P are simple.*

Proof. If $\partial P = 0$, then $gcd(P, \partial P) = P \neq 1$, so by Proposition 2.20, all the roots of P are multiple roots. Now if $\partial P \neq 0$, the $gcd(P, \partial P)$ is not P for degree reasons. So by the irreducibility of P, $gcd(P, \partial P) = 1$. Hence all the roots of P are simple by Proposition 2.20. As for the rest, note that in characteristic 0, the derivative of a nonconstant polynomial is never 0. □

2.2.3 Irreducibility criteria

Definition 2.22. Let $P \in \mathbb{Z}[X]$. We define the ***content*** $c(P)$ of P as the greatest common divisor of the coefficients of P.

If $P \in \mathbb{Z}[X] \setminus \{0\}$ and $a \in \mathbb{Z}$, then $c(a.P) = a.c(P)$. For any $P \in \mathbb{Q}[X] \setminus \{0\}$, then there is $n \in \mathbb{N}$ such that $n.P \in \mathbb{Z}[X]$. If $n_1 = c(n.P)$, then $n.P = n_1.P_1$ and $c(P_1) = 1$.

Proposition 2.23. *(Gauss) Let P, Q be two non-zero polynomials of $\mathbb{Z}[X]$. Then*

$$c(P.Q) = c(P).c(Q).$$

Proof. Dividing P and Q by $c(P)$ and $c(Q)$ respectively, it is then sufficient to show that if P, Q are such that $c(P) = c(Q) = 1$, then $c(P.Q) = 1$. Suppose for a contradiction that $c(P) = c(Q) = 1$, and $c(P.Q) \neq 1$. Let $p \in \mathbb{N}$ be a prime number dividing all the coefficients of $P.Q$. Then in $\mathbb{Z}/p[X]$, the polynomial $P.Q = 0$. But $\mathbb{Z}/p[X]$ is an integral domain, so in $\mathbb{Z}/p[X]$, $P = 0$ or $Q = 0$. So $c(P)$ or $c(Q)$ is divisible by p. Contradiction. □

Proposition 2.24. *(Gauss) Let $P \in \mathbb{Z}[X]$ be a polynomial, and suppose that $c(P) = 1$. Then P is irreducible in $\mathbb{Q}[X]$ if and only if P is irreducible in $\mathbb{Z}[X]$.*

Proof. One direction is clear. Suppose now that P is irreducible in $\mathbb{Z}[X]$. For a contradiction, suppose that we can find polynomials $S, T \in \mathbb{Q}[X]$ such that $P = S.T$. Let $s, s_1, t, t_1 \in \mathbb{N}$ be such that $s.S = s_1.S_1$ and $t.T = t_1.T_1$, where $S_1, T_1 \in \mathbb{Z}[X]$ and $c(S_1) = c(T_1) = 1$. So $stP = s_1t_1S_1T_1$, and by the above proposition and the fact that $c(P) = c(S_1) = c(T_1) = 1$, it follows that $P = S_1.T_1$. This contradicts the fact that P is irreducible in $\mathbb{Z}[X]$. □

Proposition 2.25. *(Eisenstein's criterion) Let $P = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$. If there is a prime number p such that p divides all the a_i except a_n, and p^2 does not divide a_0, then P is irreducible in $\mathbb{Q}[X]$.*

Proof. It is enough to show the irreducibility in $\mathbb{Z}[X]$ in the case where $c(P) = 1$. Suppose that P satisfies all the above conditions, and for a contradiction, let $S, T \in \mathbb{Z}[X]$ be such that $P = S.T$. Write $S = aX^n + S_1$ and $T = bX^m + T_1$, where aX^n and bX^m are the leading terms of S and T respectively. Reduce $P = S.T$ modulo p. Since a_n is not divisible by p and all the other coefficients are, and by the fact that $\mathbb{Z}/p.\mathbb{Z}$ is an integral domain, it follows that S_1 and T_1 are 0 modulo p. So the constant terms of both S_1 and T_1 are divisible by p. But the constant term of P is not divisible by p^2, and we have a contradiction. □

3 Symmetric functions

Notation: For a nonzero natural number n, we denote by S_n the symmetric group on the set $\{1, 2, \cdots, n\}$, that is the group of permutations of $\{1, 2, \cdots, n\}$.

Definition 3.1. Let K be a field, $x_1, \cdots, x_n$ be n distinct indeterminates. Let $K[x_1, \cdots, x_n]$ be the ring of polynomials over K in $x_1, \cdots, x_n$, and $K(x_1, \cdots, x_n)$ be the field of rational functions over K in $x_1, \cdots, x_n$.

1. A polynomial $P \in K[x_1 \cdots, x_n]$ is said to be ***symmetric*** if it remains unchanged when its variables are permuted, i.e.

$$\forall \sigma \in S_n : P(x_{\sigma(1)} \cdots, x_{\sigma(n)}) = P(x_1 \cdots, x_n)$$

2. A rational function $f \in K(x_1 \cdots, x_n)$ is said to be *symmetric* if it remains unchanged when its variables are permuted, i.e.

$$\forall \sigma \in S_n : f(x_{\sigma(1)} \cdots, x_{\sigma(n)}) = f(x_1 \cdots, x_n).$$

The following polynomials of $K[x_1 \cdots, x_n]$ are symmetric:

$$\begin{aligned}
s_1 &= \sum_{i \leq n} x_i = x_1 + x_2 + \cdots + x_n \\
s_2 &= \sum_{i<j \leq n} x_i.x_j \\
s_3 &= \sum_{i<j<k \leq n} x_i.x_j.x_k \\
&\dots \\
s_n &= x_1.x_2. \cdots .x_n
\end{aligned}$$

These polynomials are called ***the elementary symmetric polynomials***.

Remark 3.2. Let X be a new indeterminate. Then the following polynomial identity holds:

$$(X - x_1).(X - x_2). \cdots .(X - x_n) = X^n - s_1.X^{n-1} + s_2.X^{n-2} - s_3.X^{n-3} + \cdots + (-1)^n.s_n.$$

Example. Let $P(X) := X^5 - 3X^3 + X^2 - 2X + 1$, and let $a_1, \cdots, a_5$ be the roots of P. Then the sum of the a_i is 0, the product of the a_i is -1, and the sum of the $a_i.a_j$ for $i < j$ is -3.

It is clear that any polynomial or rational function in the elementary symmetric polynomials is symmetric. The fundamental theorems of symmetric polynomials and functions claim that the converse to these facts also holds.

Theorem 3.3. *Let $p \in K[x_1, \cdots, x_n]$ be a symmetric polynomial in the indeterminates $x_1, \cdots, x_n$. Then p can be expressed as a polynomial in $s_1, \cdots, s_n$.*

Proof. We define an ordering on monic monomials in the x_i by setting

$$x_1^{i_1}.x_2^{i_2}.\cdots.x_n^{i_n} > x_1^{j_1}.x_2^{j_2}.\cdots.x_n^{j_n}$$

if either

$$i_1 + \cdots + i_n > j_1 + \cdots + j_n$$

or the equality holds and for some $m \leq n$,

$$i_1 = j_1,\ i_2 = j_2,\ \cdots,\ i_{m-1} = j_{m-1} \text{ but } \ i_m > j_m.$$

We define a ***norm function*** ν from $K[x_1, \cdots, x_n]$ to the set of monic polynomials of $K[x_1, \cdots, x_n]$, by defining the image of a polynomial f as being the highest monomial occurring in f (we ignore its coefficient).

Set $\nu(p) = x_1^{k_1}.x_2^{k_2}.\cdots.x_n^{k_n}$, and let $c(p) \in K^*$ be the coefficient of $\nu(p)$ in p. Since p is symmetric, then the monomials obtained from $\nu(p)$ by permuting the x_i occur in p as well. Thus $k_1 \geq k_2 \geq \cdots \geq k_n$.

The norm of the symmetric polynomial s_m is $x_1 x_2 \cdots x_m$. So the norm of the symmetric polynomial

$$s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}$$

is

$$x_1^{a_1+\cdots+a_n} x_2^{a_2+\cdots+a_n} \cdots x_n^{a_n}.$$

Let

$$p_1 := p - c(p) s_1^{k_1-k_2} s_2^{k_2-k_3} s_3^{k_3-k_4} \cdots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n}.$$

We see easily that $\nu(p_1) < \nu(p)$. We repeat this process with p_1, and by Exercise 3.4, after a finite number of steps we have an expression of p as a polynomial in $s_1, \cdots, s_n$. □

Exercise 3.4. An ordered set $(X, \leq)$ is said to be well-ordered if every strictly decreasing sequence of elements of X is finite. Equivalently, the set $(X, \leq)$ is well-ordered if every non-empty subset of X has a least element. Show that ordering defined in the above proof on the monic monomials is a well-ordering.

Theorem 3.5. *Let $f \in K(x_1, \cdots, x_n)$ be a symmetric rational function in the indeterminates $x_1, \cdots, x_n$. Then f can be expressed as a rational function in $s_1, \cdots, s_n$.*

Proof. Let $f \in K(x_1, \cdots, x_n)$ be symmetric, and let $p, q \in K[x_1, \cdots, x_n]$ be such that $f = p/q$. Let $r := \prod_{\sigma \in S_n} \sigma q$. The polynomial r is symmetric, and f is a symmetric rational function, hence the polynomial $f.r$ is symmetric. So both $f.r$ and r lie in $K[s_1, \cdots, s_n]$. Hence their quotient $f = f.r/r$ lies in $K(s_1, \cdots, s_n)$. □

Theorem 3.6. *Let $f \in K(x_1, \cdots, x_n)$ be a rational function in the indeterminates $x_1, \cdots,$ x_n. Suppose that f has exactly m different images when its variables are permuted. Then f is a root of a polynomial $P \in K(s_1, \cdots, s_n)[X]$ of degree m.*

Proof. Let $f_1 = f, f_2, \cdots, f_m$ be the different images of f when the variables are permuted. Let $P(X) := \prod_{1 \leq i \leq m}(X - f_i)$. The polynomial P has degree m, and it remains unchanged when the x_i are permuted. So the coefficients of P are symmetric functions in the x_i, and by Theorem 3.5, they lie in $K(s_1, \cdots, s_n)$. So $P \in K(s_1, \cdots, s_n)[X]$. □

Let f be as above, and denote by $Fix(f)$ the subgroup of permutations of S_n fixing f. It is clear that $Fix(f)$ is a normal subgroup of S_n, and that f has the same image under any two permutations of the same coset of $Fix(f)$. Furthermore, the number of these cosets is the cardinality of the quotient $S_n/Fix(f)$. This together with Theorem 3.6 yields the following

Theorem 3.7. *Let $f \in K(x_1, \cdots, x_n)$ be a rational function in the indeterminates $x_1, \cdots,$ x_n, and let $Fix(f)$ be the subgroup of permutations of S_n fixing f. Then f is a root of a polynomial $P \in K(s_1, \cdots, s_n)[X]$ of degree $|S_n/Fix(f)|$.*

Example. Discriminant

4 Polynomial equations of degree 3 and 4

Remark 4.1. Let K be a field, $n \neq char(K)$ and

$$P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X].$$

If we substitute the variable X by

$$Y - \frac{a_{n-1}}{na_n},$$

we get a polynomial $Q(Y)$ with the same degree as P, and in which the coefficient of Y^{n-1} is 0. Furthermore, if we know the roots of Q, it is easy to find those of P. So for the purpose of finding a general formula for expressing the roots of polynomials of a certain degree, we will restrict ourselves to polynomials of the form $P = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ where $a_{n-1} = 0$ (and $a_n = 1$).

For this section, we fix a field K with $char(K) \neq 2, 3$.

4.1 Equations of degree 3

The problem of solving polynomial equations of degree three will be reduced to solve equations of degree two. To this end, we will use the ideas of the previous section - see Theorem 3.6- and introduce an adequate rational function of the roots of the polynomial we want to solve, to find a solution“by steps”. We shall follow a method introduced by Lagrange in his book “Refléxions sur la résolution algébrique des équations” (1770).

Let K be a field with $char(K) \neq 2, 3$, and let $P(X) = X^3 + pX + q \in K[X]$. Suppose that $p, q \neq 0$. Let L be an extension of K containing the primitive third roots of unity (i.e. roots of the polynomial $X^2 + X + 1$), and the roots a, b, c of P. We will show in the subsequent that such a field L always exists. Note that the roots of $X^2 + X + 1$ are the inverses of each other, so they are also the squares of each other. We denote them by $j := -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ and $j^2 := -\frac{1}{2} - \frac{\sqrt{-3}}{2}$, where $\sqrt{-3}$ denotes one of the square roots of -3. Denote by K_1 the field generated over K by j and j^2. So

$$K_1 = K(\sqrt{-3}).$$

Let $x_1 = a + jb + j^2c$ and $x_2 := a + j^2b + jc$. Note that

$$x_1.x_2 = a^2 + b^2 + c^2 - (ab + ac + bc) = -3(ab + ac + bc) = -3p.$$

The function $x_1 = a + jb + j^2c$ considered as a polynomial function in the free variables a, b, c, takes six different values when a, b, c are permuted. Those values are x_1, jx_1, j^2x_1, x_2, jx_2, j^2x_2. Now if instead of x_1 we consider the function $y_1 := x_1^3$, the number of values drops to two when a, b, c are permuted: $x_1^3 = y_1$ and $x_2^3 =: y_2$. By Theorem 3.6, y_1 and y_2 are roots of a polynomial of degree 2 with coefficients in $K_1[X]$. The discriminant of this polynomial is

$$d := (y_1 + y_2)^2 - 4y_1y_2.$$

So $y_1, y_2 \in K_1(\sqrt{d})$, where $\sqrt{d}$ denotes one of the square roots of d. Let

$$K_2 := K_1(\sqrt{d}).$$

So $y_1, y_2 \in K_2$. Denote by $\sqrt[3]{y_1}$ one of the cubic roots of y_1, and note that K_2 contains all the cubic roots of unity. Then x_1 is in the field K_3 defined by

$$K_3 := K_2(\sqrt[3]{y_1}) = K(\sqrt{-3}, \sqrt{d}, \sqrt[3]{y_1}).$$

We saw that $x_1.x_2 = -3p$, so x_2 is in K_3 as well. The field K_3 contains the roots a, b, c of $P(X)$, since those are, in K_3, the solutions of the linear system

$$\begin{aligned} a + b + c &= 0 \\ a + bj + cj^2 &= x_1 \\ a + bj^2 + cj &= x_2. \end{aligned}$$

We showed that there is a tower of subfields of L:

$$K \subset K(\sqrt{-3}) \subset K(\sqrt{-3}, \sqrt{d}) \subset K(\sqrt{-3}, \sqrt{d}, \sqrt[3]{y_1})$$

such that every subfield is generated over the previous one by some n^{root}. This means that every cubic equation is solvable.

Remark 4.2. This does not work in characteristic 2, as in this case the formula giving the roots of quadratic equations does not work. Neither does this work in characteristic 3. In this case $j = j^2 = 1$, so the above linear system is dependent

Now we calculate explicitly the roots of $P(X) = X^3 + pX + q$. We calculate first x_1^3 and x_2^3. We have already showed $x_1^3 + x_2^3$ and $x_1^3.x_1^3$ are elements of K. Let us calculate their values explicitly. We showed above that $x_1.x_2 = -3p$. Using that $1 + j + j^2 = a + b + c = 0$, and the fact that a is a root of $X^3 + pX + q$, we have the following:

$$\begin{aligned} x_1^3.x_2^3 &= (-3p)^3 = -27p^3 \\ x_1^3 + x_2^3 &= (x_1 + x_2)^3 - 3.(x_1.x_2)(x_1 + x_2) \\ &= (2a - b - c)^3 + 9p(2a - b - c) \\ &= (3a)^3 + 27pa \\ &= 27(a^3 + pa) \\ &= -27q \end{aligned}$$

Therefore, x_1^3 and x_2^3 are the roots of the polynomial

$$X^2 + 27qX - 27p^3.$$

Let

$$d = 27(4p^3 + 27q^2)$$

be the ***discriminant*** of this polynomial, and denote by $\sqrt{4p^3 + 27q^2}$ one of the square roots of $4p^3 + 27q^2$. Now we have

$$x_1^3 = \frac{-27q + \sqrt{27}\sqrt{4p^3 + 27q^2}}{2}$$

and

$$x_2^3 = \frac{-27q - \sqrt{27}\sqrt{4p^3 + 27q^2}}{2}$$

Denote by $\sqrt[3]{\frac{-27q+\sqrt{27}\sqrt{4p^3+27q^2}}{2}}$ any cubic root of the first expression. Call α this cubic root. Denote by $\sqrt[3]{\frac{-27q-\sqrt{27}\sqrt{4p^3+27q^2}}{2}}$ the cubic root of the second expression which is equal to $-\frac{3p}{\alpha}$. If we choose for x_1 the value α, so $x_2 = -\frac{3p}{\alpha}$. Now we have the system

$$
\begin{aligned}
a+b+c &= 0 \\
a+bj+cj^2 &= \alpha \\
a+bj^2+cj &= -\frac{3p}{\alpha}.
\end{aligned}
$$

The roots a, b, c of P are thus

$$\frac{1}{3}(\alpha - \frac{3p}{\alpha}) = \frac{1}{3}\left(\sqrt[3]{\frac{-27q+\sqrt{27}\sqrt{4p^3+27q^2}}{2}} + \sqrt[3]{\frac{-27q-\sqrt{27}\sqrt{4p^3+27q^2}}{2}}\right)$$

$$\frac{1}{3}(j^2\alpha - j\frac{3p}{\alpha}) = \frac{1}{3}\left(j^2\sqrt[3]{\frac{-27q+\sqrt{27}\sqrt{4p^3+27q^2}}{2}} + j\sqrt[3]{\frac{-27q-\sqrt{27}\sqrt{4p^3+27q^2}}{2}}\right)$$

$$\frac{1}{3}(j\alpha - j^2\frac{3p}{\alpha}) = \frac{1}{3}\left(j\sqrt[3]{\frac{-27q+\sqrt{27}\sqrt{4p^3+27q^2}}{2}} + j^2\sqrt[3]{\frac{-27q-\sqrt{27}\sqrt{4p^3+27q^2}}{2}}\right).$$

These are known as the “Cardano formulas”, named after Gerolamo Cardano(1501-1576).

4.1.1 Some remarks on the cubic equations with real coefficients

Let K be a subfield of $\mathbb{R}$ and $P = X^3 + pX + q$ be a cubic polynomial of $K[X]$. The polynomial P has either one or three real roots. If P has exactly one real root, then the two non-real roots are conjugates. Using the fact that a is a root of P, $a+b+c=0$ and $a.b.c = -q$, we have:

$$(b-c)^2 = (b+c)^2 - 4bc = -p + \frac{3q}{a}.$$

The polynomial P has a multiple root in $\mathbb{C}$ if and only if, without loss of generality, $(b-c) = 0$, so $\frac{3q}{p}$ is a root of P, thus $4p^3 + 27q^2 = 0$.

Suppose first that $4p^3 + 27q^2 > 0$, so α can be chosen to be real, and looking at the Cardano formulas one sees easily that P has two non real roots and one real root.

Now if $4p^3 + 27q^2 < 0$, then x_1^3 and x_2^3 are complex conjugates, as those are the roots of a polynomial of degree two with real coefficients, and it is easy to check that α and $-\frac{3p}{\alpha}$ are complex conjugates as well. From this fact it follows easily that all the roots of P are real.

This may sound a bit paradoxical: the roots of P are all real if and only if the square root $\sqrt{4p^3+27q^2}$ appearing in the expression of the roots is imaginary. We will show in fact that if P is irreducible and has three real roots, then one can not avoid imaginary roots in the expression with radicals of the roots of P. More precisely, we show in this case that there is no tower of subfields of $\mathbb{R}$

$$K_0 = K \subset K_1 \subset \cdots \subset K_n \subset \mathbb{R}$$

such that, for any $0 < i \leq n$, K_i is generated by some $\sqrt[n]{a_i}$ over K_{i-1}, for some $a_i \in K_{i-1}$ and $n \in \mathbb{N}^*$, and K_n contains all the (real) roots of P.

4.1.2 Historical notes

At the times of the Cardano discovery, there were neither complex numbers, nor negative numbers. So the radicals appearing in the cardano formulas were to be interpreted as positive real numbers: the edge length of a cube with a given volume, or the edge length of a square with a given surface. There was thus one Cardano formula, and not three of them. And this Cardano formula baffled the mathematicians of the 16^{th} century, starting by Cardano himself. Trying to solve an equation like $X^3 = 15X + 4$, which admits obviously 4 as a solution, the Cardano formula yields a strange expression:

$$\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

The validity of the Cardano formula in this case remained contentious for a long time. But soon, Cardano came to realize that, even in this case, his formula holds some truth if one doesn't try systematically to give a geometric interpretation for the emerging square and cubic roots. So in his calculation, he started treating the square and cubic roots in formal way. Thus $\sqrt{a}$ is a number (possibly an *impossible number* according to the new terminology of Cardano, when $a < 0$) whose square is a. A simple calculation shows then that

$$(2 + \sqrt{-1})^3 = 2 + \sqrt{-121} \quad \text{and} \quad (2 - \sqrt{-1})^3 = 2 - \sqrt{-121}.$$

So the solution given by the Cardano formula to the equation $X^3 = 15X + 4$ is just

$$(2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4,$$

as expected. And this is exactly how the complex numbers appeared in mathematics: it was an attempt from Cardano and his students to understand the scope of validity of the Cardano Formula.

Another new fact arising from the Cardano formula, was the discovery that some cubic equations can have two, or even three solutions. One should yet note the following. Given three numbers a, b, c one can easily construct a polynomial $P(X)$ of degree 3 having a, b, c as roots: take $P = (X - a).(X - b).(X - c)$. Furthermore, it follows easily by the Euclid algorithm (for polynomials !) that a, b and c are the unique roots of $P(X)$. Well, this argument was not that clear for Cardano. The equations were interpreted geometrically, and written literally, with words. So X^3 was the volume of some cube, and X^2 was the surface of the side of the same cube, the coefficient of X^2 was some length, and the coefficient of X was a surface, etc.. Moreover, there were no negative numbers. So the terms with negative coefficients were to be taken to the other side of the equation. All this to say, that at that time, a very important mathematical object was missing: the polynomial. So Cardano had no polynomials, and of course, he couldn't multiply polynomials, (since he didn't have any...). So our simple argument for finding P as the product of $X-a$, $X-b$ and $X-c$ was not as obvious as that at that time, and the discovery that some cubic equations have three roots was rather surprising. This led Cardano to the conjecture that every cubic equation has three roots, if one counts the *impossible solutions*. In the subsequent years, this conjecture was generalized to equations of degree n, and was even used as fact for a long time, until Gauss provided a proof for it as he proved the fundamental theorem of algebra.

4.2 Equations of degree 4

The solution of quartic equations was found soon after that of the cubic by a student of Cardano named Ludovico Ferrari (1522-1565). Nevertheless, this discovery arose much less interest than that of Cardano. And one of the reasons for this, is that quartic equations do not have an obvious geometric interpretation.

There was a good reason for which the algebraic questions which interested mathematicians were only those having a geometrical interpretation. Pythagoras taught that the world can be explained with numbers, and here we mean natural numbers. He said that in geometry for example, for an adequate choice of the unit, every measure will be a natural number. Some decades after the death of Pythagoras, one of his followers Hippasus of Metapontum, showed that if the edge length of a square is a number, then it is not the case for the diagonal. Which comes to the same as saying that $\sqrt{2}$ is not a rational number. Hippasus paid his discovery with his life, drowned allegedly at see for producing a counterexample to the Pythagoras' doctrine that "all things are numbers".

After the death of Hippasus, $\sqrt{2}$ kept being irrational, and a generalization of the notion of number beyond rationals was needed in order to deal in a coherent way with numbers arising from geometry. The obvious generalization is by defining numbers as distances between two points. So if x is a distance between two points, x^2 is a surface, and x^3 is a volume. As for x^4, it has no place in Greek algebra.

Now we come back to our quartic equations. By the usual translation, solving a polynomial equation of degree 4 comes to the same as solving an equation of the form

$$X^4 + aX^2 + bX + c$$

where a, b, c are elements of some field K with $char(K) \neq 2, 3$. Denote by x_1, x_2, x_3, x_4 the roots of the above equation. As for the cubic equations, the idea is to find a rational function $f(x_1, x_2, x_3, x_4)$ taking "few" distinct values when the x_i are permuted. "Few" does not mean 1. In this case f is symmetric and considering such an f will not be helpful.

Let's have a look at the structure of S_4, the group of permutations of the set $\{1, 2, 3, 4\}$. This group has 24 elements, four of which keep $\{1, 2\}$ and $\{3, 4\}$ invariant, and another four sending $\{1, 2\}$ to $\{3, 4\}$. These eight permutations form a subgroup H of S_4. Let

$$f(x_1, x_2, x_3, x_4) := x_1x_2 + x_3x_4.$$

It is clear that the subgroup of S_4 fixing f (as a rational function in the free variables x_1, x_2, x_3, x_4) is H. So H is a normal subgroup of S_4 (this fact is not really needed for the argument). Now H has 8 elements, S_4 has 24, and $24/8 = 3$. So by Theorem 3.7, $x_1x_2 + x_3x_4$ is a root of a polynomial of degree 3 over K, namely the polynomial

$$(X - (x_1x_2 + x_3x_4))(X - (x_1x_3 + x_2x_4))(X - (x_1x_4 + x_2x_3))$$

Fix the following notation:

$$\alpha := x_1x_2 + x_3x_4, \quad \beta := x_1x_3 + x_2x_4, \quad \gamma := x_1x_4 + x_2x_3.$$

Computing the elementary symmetric functions of α, β and γ, we have:

$$\alpha + \beta + \gamma = a$$

$$\alpha\beta + \beta\gamma + \alpha\gamma = (\sum x_i)(\sum_{i<j<k} x_ix_jx_k) - 4x_1x_2x_3x_4 = -4c$$

$$\alpha\beta\gamma = x_1x_2x_3x_4(\sum x_i)^2 + (\sum_{i<j<k} x_ix_jx_k)^2 - 4x_1x_2x_3x_4 \sum_{i<j} x_ix_j = b^2 - 4ac.$$

So α, β and γ are the three roots of the polynomial

$$X^3 - aX^2 - 4cX + 4ac - b^2.$$

By the results of the last section, α, β and γ have algebraic expressions in the coefficients, so in a, b and c, and they are contained in some extension by radicals of the field K.

We show now that the roots x_1, x_2, x_3 and x_4 have algebraic expressions in α, β and γ. $x_1 + x_3$ takes exactly two distinct values under the permutations fixing α and β, so it should be the root of a polynomial of degree two on $K(\alpha, \beta)$, the other root being $x_2 + x_4$. And indeed, we have:

$$(x_1 + x_3).(x_2 + x_4) = \alpha + \beta,$$

$$(x_1 + x_3) + (x_2 + x_4) = 0$$

Denote by $\sqrt{-\alpha - \beta}$ a square root of $-\alpha - \beta$. Now we have

$$x_1 + x_3 = \sqrt{-\alpha - \beta},$$

$$x_2 + x_4 = -\sqrt{-\alpha - \beta}$$

Note that $-\alpha - \beta = \gamma - a$. With the same calculation, we have

$$x_1 + x_3 = \sqrt{\gamma - a},$$

$$x_2 + x_4 = -\sqrt{\gamma - a},$$

$$x_1 + x_4 = \sqrt{\beta - a},$$

$$x_2 + x_3 = -\sqrt{\beta - a},$$

$$x_1 + x_2 = \sqrt{\alpha - a},$$

$$x_3 + x_4 = -\sqrt{\alpha - a}.$$

(The square roots are not fixed independently of each other.) The expressions of the x_i follow directly:

$$2x_1 = \sqrt{\gamma - a} + \sqrt{\beta - a} + \sqrt{\alpha - a},$$
$$2x_2 = -\sqrt{\gamma - a} - \sqrt{\beta - a} + \sqrt{\alpha - a},$$
$$2x_3 = \sqrt{\gamma - a} - \sqrt{\beta - a} - \sqrt{\alpha - a},$$
$$2x_4 = -\sqrt{\gamma - a} + \sqrt{\beta - a} - \sqrt{\alpha - a}.$$

This shows that every equation of degree 4 is solvable by radicals.

4.3 And for 5?

We reduced the equations of degree three to equations of degree two, and those of degree four to ones of degree three. In each case, we were able to find a function f of the roots taking the "good number" of distinct values when the roots x_i of the polynomial are permuted. Equivalently, the the group $Fix(f)$ had the "good order".

For the polynomials of degree 3 on a field K, we defined f as $(x_1+jx_2+j^2x_3)^3$. $Fix(f) \subset S_3$ has order 3, and f takes two distinct values when the x_i are permuted. So f is the root of a polynomial of degree 2 of K.

For the polynomials of degree 4 on a field K, we defined f as $x_1x_2 + x_3x_4$. $Fix(f) \subset S_4$ has order 8, and f takes three distinct values when the x_i are permuted. So f is the root of a polynomial of degree 3 of K.

From $n = 5$, Cauchy proved that this "does not work anymore". He showed that if n is prime, then any function f of the roots takes either more than n values (and this doesn't help, since f is then a root of a polynomial with degree greater than n), or one or two values (and this is not very helpful neither). So in the language of groups, he showed that if n is a prime number, and H a subgroup of S_n with index $\leq n-1$, then H has index 1 or 2.

To see this, we show first that all the cycles of length n are in H. So let σ be such a cycle. The cosets $H, H\sigma, H\sigma^2, \cdots, H\sigma^{n-1}$ cannot be all disjoint from each other since the index of H is at most $n-1$. So for some $i < j < n$, σ^{j-i} is an element of H. But σ^{j-i} generates a non trivial subgroup of the subgroup generated by σ, which has prime order n. So σ^{j-i} and σ generate the same subgroup of S_n, and $\sigma \in H$.

Now we show that A_n is a subgroup of H by checking that every 3-cycle is in H. And indeed:

$$(1, 2, 3, 4, \cdots, n-1, n)(n, n-1, \cdots, 4, 2, 3, 1) = (2, 4, 3).$$

So A_n is a subgroup of H and thus H has index 1 or 2.

Now we have a look at the field extensions of the form $K(f)/K$ where f takes one or two values. One of those functions taking exactly two distinct values when the x_i are permuted, is the function

$$d := \prod_{i<j\leq n} (x_i - x_j).$$

The function d is in fact a square root of the discriminant of the polynomial. Now let f be any function of the roots. If f takes one value then f is symmetric, so $f \in K$ and $K(f) = K$. And if f takes exactly two values, say $f_1 = f$ and f_2 then $Fix(f) = Fix(d) = A_n$. The functions $f_1 + f_2$ and $d(f_1 - f_2)$ are then symmetric, so they are in K. So $f \in K(d)$ and $K(f) = K(d)$.

5 Algebraic extensions

5.1 Algebraic elements

Definition 5.1. Let L/K be a field extension, and let a be an element of L. Then a is said to be ***algebraic*** over K if there is a nonzero polynomial $P(X) \in K[X]$ such that $P(a) = 0$. If a is not algebraic over K, then a is said to be ***transcendental*** over K.

Examples: $\sqrt{2}$, $\sqrt{2}+1$, $e^{\frac{2i\pi}{n}}$ with $n \in \mathbb{N}$, are algebraic over $\mathbb{Q}$. If L/K is a field extension, then every $a \in K$ is algebraic over K. If K is a field and X a free variable, then in the field extension $K(X)/K$, the element X is transcendental over K. In fact, every element of $K(X) \setminus K$ is transcendental over K.

Remark 5.2. In the field extension $\mathbb{R}/\mathbb{Q}$, there are countably many algebraic numbers over $\mathbb{Q}$ since there are countably many polynomials with coefficients in $\mathbb{Q}$. On the other hand $\mathbb{R}$ is uncountable. Therefore there are uncountably many elements of $\mathbb{R}$ which are transcendental over $\mathbb{Q}$.

Exercise 5.3. (Liouville's Theorem-1844) For every sequence $(a_n)_{n\in\mathbb{N}}$ of natural numbers between 1 and 9, the number $\sum\limits_{n\geq 0} a_n.10^{-n!}$ is transcendental over $\mathbb{Q}$ (Hint: show that if a is a root of an irreducible polynomial $P \in \mathbb{Z}[X]$ of degree $n > 1$, then there is constant $c > 0$ such that for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$, we have $|a - \frac{p}{q}| \geq \frac{c}{q^n}$).

Proposition 5.4. *Let L/K be a field extension, and $a \in L$ be algebraic over K. Then there is a unique polynomial $P \in K[X]$ with leading coefficient 1 and least degree among all polynomials in $K[X]$ having a as a root.*

Proof. Let $Q \in K[X]$ be a nonzero polynomial least degree such that $Q(a) = 0$, and let $\alpha \neq 0$ be the leading coefficient of Q. Let $P := Q/\alpha$. So P is a polynomial in $K[X]$ with leading coefficient 1, and least degree among all polynomials in $K[X]$ having a as a root. If there is another $R \in K[X]$ with these properties, take $S := P - R$. So S is a nonzero polynomial in $K[X]$ with $S(a) = 0$, and the degree of S is strictly smaller than that of P. This contradicts the definition of P. $\square$

Definition 5.5. Let L/K be a field extension, and $a \in L$ be algebraic over K. The ***minimal polynomial*** of a over K is the unique polynomial $P \in K[X]$ with leading coefficient 1 and least degree among all polynomials in $K[X]$ having a as a root.

Examples In the extension $\mathbb{R}/\mathbb{Q}$, X^2-2 is the minimal polynomial of $\sqrt{2}$, and X^3-2 is the minimal polynomial of $\sqrt[3]{2}$.

Proposition 5.6. *Let L/K be a field extension, $a \in L$ be algebraic over K and P be the minimal polynomial of a over K. Then we have the following:*

1. *P is not a constant polynomial.*

2. *Let $Q \in K[X]$ be such that $Q(a) = 0$. Then Q is divisible by P.*

3. *P is irreducible in $K[X]$.*

4. *Every other root of P admits P as its minimal polynomial.*

5. *If K has characteristic 0, then a is a simple root of P.*

Proof. 1. The polynomial P has a root in K. So if it is constant, it has to be identically zero. This contradicts the definition of the minimal polynomial.

2. Let $R, S \in K[X]$ be such that $Q = R.P + S$, with $deg(S) < deg(P)$. Since $P(a) = Q(a) = 0$, then $S(a) = 0$. So S is identically 0 by minimality of $deg(P)$.

3. Immediate by the fact that a field is an integral domain.

4. The element b is a root of P, so b is algebraic over K and has a minimal polynomial Q, and P is divisible by Q by (1). But P is irreducible, and both P and Q have leading coefficient 1, so $P = Q$ and P is the minimal polynomial of b.

5. This is a direct consequence of Proposition 2.21 and the irreducibility of P.

□

Corollary 5.7. *Let $x \in K$ be algebraic over k, and let $P \in k[X]$ be the minimal polynomial of x over k. Let x' be another root of P. Then for $Q \in k[X]$, x is a root of Q if and only if x' is a root of Q.*

Theorem 5.8. *Let L/K be a field extension, and $a \in L$. The following are equivalent:*

1. *a is algebraic over K.*

2. *$K[a]$ is a field.*

3. *$K[a] = K(a)$.*

4. *The extension $K(a)/K$ is finite.*

Proof. It is clear that *2* and *3* are equivalent.

***1*⇒*3*:** Suppose that a is algebraic over K and let $P = X^n + a_{n-1}.X^{n-1} + \cdots + a_0$ be the minimal polynomial of a over K. The identity $P(a) = 0$ shows that a^n is a linear combination of the monomials $1, a, \cdots, a^{n-1}$. By induction, it is easy to see for any $m \geq n$, that a^m is a linear combination of the monomials $1, a, \cdots, a^{n-1}$. So the ring $k[a]$ is a finite dimensional vector space over K, generated by $1, a, \cdots, a^{n-1}$. By Proposition 2.15, the ring $k[a]$ is a field and $k[a] = k(a)$.

***3*⇒*4*:** Suppose that $K[a] = K(a)$. So a^{-1} is a K-linear combination of $1, a, \cdots, a^{n-1}$ for some n, say

$$a^{-1} = k_1 + k_2.a + \cdots + k_n.a^{n-1}.$$

We can moreover suppose that $k_n \neq 0$. Multiplying by a on both sides we have

$$1 = k_1.a + k_2.a^2 + \cdots + k_n.a^n.$$

So

$$a^n = \frac{1}{k_n} - \frac{k_1}{k_n}.a - \frac{k_2}{k_n}a^2 - \frac{k_{n-1}}{k_n}.a^{n-1}.$$

This shows that a^n is a K-linear combination of $1, a, a^2, \cdots, a^{n-1}$, and by induction it is clear that the same holds for any $m \geq n$. Thus the ring $K[a]$ is a finite dimensional K-vector space. But $K[a] = K(a)$, so $K(a)/K$ is finite.

***4⇒1*:** If the extension $K(a)/K$ is finite, then $1, a, \cdots, a^i, \cdots$ are K-linearly dependent. Any non-trivial K-linear combination of the a^i yields a polynomial $P \in K[X]$ with $P(a) = 0$.

□

Corollary 5.9. *Let L/K be a field extension, and let $a \in L$ be algebraic over K. Then the degree of the extension $K(a)/K$ is equal to the degree of the minimal polynomial of a over K.*

Proof. If n is the degree of the minimal polynomial of a over K, we have seen above that for any $m \in \mathbb{N}$, a^m is a linear combination of elements of the set $S = \{1, a, a^2, \cdots, a^{n-1}\}$. So S spans the K-vector space $K[a]$ over K, and since $K(a) = K[a]$, S spans the K-vector space $K(a)$. On the other hand, the set S is independent over K: there is no non-trivial K-linear combination of $1, a, a^2, \cdots, a^{n-1}$ which is 0, that would yield a polynomial $Q \in K[X]$ with degree $< n$ with $Q(a) = 0$. So S is a basis of $K(a)$ over K, and it has obviously n elements. So the degree of the extension $K(a)/K$ is n. □

Definition 5.10. Let L/K be a field extension. The extension L/K is said to be algebraic if every element of L is algebraic over K.

Proposition 5.11. *Let L/K be a finite field extension. Then L/K is algebraic.*

Proof. Let a be any element of L. So $K(a)$ is a K-vector space which is a subvector space of L. Because the dimension of L over K is finite, the same holds for that of $K(a)$ over K. Theorem 5.8 yields that a is algebraic over K. □

Remark 5.12. The converse of Proposition 5.11 does not hold. The field $\mathbb{Q}^{alg}$ of elements of $\mathbb{C}$ which are algebraic over $\mathbb{Q}$ has infinite dimension over $\mathbb{Q}$. To see this, let $p \in \mathbb{N}$ be any prime number, and $n \in \mathbb{N}^*$. Then by Eisenstein's criterion, the polynomial $X^n - p$ is irreducible in $\mathbb{Q}$. So the degree of $\sqrt[n]{p}$ over $\mathbb{Q}$ is n. This shows that the degree of $\mathbb{Q}^{alg}$ over $\mathbb{Q}$ is not bounded, thus infinite.

Proposition 5.13. *Let L/K be a field extension, and let $a_1, \cdots, a_n \in L$ be algebraic over K. Let $p_1, \cdots, p_n$ be the degrees over K of $a_1, \cdots, a_n$ respectively. Then the extension $K(a_1, \cdots, a_n)/K$ is finite, thus algebraic, with degree $\leq p_1.p_2.\cdots.p_n$.*

Proof. Recall first that $K(a_1, \cdots, a_n) = K(a_1)(a_2)\cdots(a_n)$. We prove it by induction. For $n = 1$ the result is given by Theorem 5.8. Suppose this is shown for $n - 1$, and we show it for n. The element a_n has degree p_n over K, and since dependence over K implies dependence over $K(a_1)(a_2)\cdots(a_{n-1})$, then a_n has degree $\leq p_n$ over $K(a_1)(a_2)\cdots(a_{n-1})$. By the multiplicativity formula for degrees and the induction hypothesis, we have that

$$[K(a_1, \cdots, a_n) : K] = [K(a_1, \cdots, a_n) : K(a_1, \cdots, a_{n-1})].[K(a_1, \cdots, a_{n-1}) : K]$$

$$\leq p_1.p_2.\cdots.p_{n-1}.p_n.$$

□

Corollary 5.14. *Let M/L and L/K be two algebraic field extensions. Then M/K is algebraic.*

Proof. Let a be an element of M of degree n, and let $a_0, \cdots, a_{n-1}$ be the coefficients of the minimal polynomial of a over L. Then by the above proposition, the extension $K(a_1, \cdots, a_{n-1})/K$ is finite.On the other hand, the extension $K(a_1, \cdots, a_{n-1})(a)/K(a_1, \cdots, a_{n-1})$ is finite. So $K(a_1, \cdots, a_{n-1})(a)/K$ is finite and a is algebraic over K. $\square$

Corollary 5.15. *Let L/K be a field extension. Then the set K_L^{alg} of elements of L which are algebraic over K is a subfield of L.*

Proof. It is clear that $0, 1 \in K_L^{alg}$. Let a, b be elements of K_L^{alg}, with $b \neq 0$. Then $a - b$ and $a.b^{-1}$ are in $K(a, b)$, which is algebraic extension of K. So $a - b, a.b^{-1} \in K_L^{alg}$. $\square$

Remark 5.16. We have shown that in a field extension L/K, the sum and product of two algebraic elements a, b are algebraic, and has degree smaller than or equal to the product of the degrees of a and b. So in the field extension $\mathbb{R}/\mathbb{Q}$, the element $\sqrt[3]{2} + \sqrt[5]{3}$ is a root of a polynomial of $\mathbb{Q}[X]$ with degree ≤ 15.

Exercise 5.17. Let P_1, P_2 be polynomials in $K[X]$ of degree m_1 and m_2 respectively. Denote by $x_1, \cdots, x_{m_1}$ the roots of P, and by $y_1, \cdots, y_{m_2}$ those of Q. Let $f(x_1, y_1)$ be any rational function of x_1 and y_1. Define

$$\Theta(X) := \prod_{i \leq m_1, j \leq m_2} (X - f(x_i, y_j)).$$

Use the fundamental theorem of symmetric functions to show that $\Theta(X) \in K[X]$. Generalize the result to the case of n polynomials. Note that this result gives an explicit polynomial of degree 15 with rational coefficients having $\sqrt[3]{2} + \sqrt[5]{3}$ as a root.

5.2 Extending field isomorphisms

Definition 5.18. Let K_1, K_2 be two fields, and f be an application from K_1 to K_2. Then f is a ***field homomorphism*** if $f(1) = 1$ and for any $x, y \in K_1$, $f(x + y) = f(x) + f(y)$ and $f(x.y) = f(x).f(y)$.

Remark 5.19. A field has no nontrivial ideals. So the kernel of field homomorphism f from K_1 to K_2 is $\{0\}$, and f is injective. Thus $f(K_1)$ is a field, and f defines a field isomorphism between K_1 and $f(K_1)$.

Definition 5.20. Let L/K and L'/K be two field extensions, and f an application from L to L'.

1. The application f is a K-***homomorphism*** if f defines a unitary ring homomorphism between L and L', and $f(x) = x$ for any $x \in K$. A K-homomorphism from L to L' is then a homomorphism of K-algebras between L and L'.

2. The application f is said to be a K-***isomorphism*** if it is a bijective K-homomorphism.

3. The application f is said to be a K-***automorphism*** if it is a K-isomorphism and $L = L'$.

Proposition 5.21. *Let L/K be a field extension, $a \in L$ be algebraic over K and P be its minimal polynomial. Denote by $\bar{X}$ the class of the polynomial X modulo $< P >$. Then there is a unique K-isomorphism f from the field $K[X]/ < P >$ to $K(a)$, with $f(\bar{X}) = a$.*

Proof. Let g be the application from $K[X]$ to $K[a]$, which to a polynomial $P[X]$ associates the element $P(a)$. It is clear that g is a well defined homomorphism of K-algebras between $K[X]$ and $K[a]$. By Proposition 5.6, the kernel of g is $< P >$. So g factors into an isomorphism of K-algebras f between $K[X]/ < P >$ and $K[a]$, and $f(\bar{X}) = g(X) = a$. Uniqueness is obvious. □

Proposition 5.22. *Let K_1 and K_2 be two fields and let σ be a field isomorphism from K_1 to K_2. Let $P \in K_1[X]$ be an irreducible polynomial, and let L_1, L_2 be extensions of K_1 and K_2 respectively, in which P and σP have roots, say α_1 and α_2. Then σ can be extended in a unique way to an isomorphism σ' from $K_1(\alpha_1)$ to $K_2(\alpha_2)$, with $\sigma'(\alpha_1) = \alpha_2$.*

Proof. Uniqueness is obvious. As for the existence, note first that σ extends to field isomorphism between $K_1[X]/ < P >$ and to $K_2[X]/ < \sigma P >$. By Proposition 5.21, $K_1(\alpha_1)$ is K_1-isomorphic to $K_1[X]/ < P >$, and $K_2(\alpha_2)$ is K_2-isomorphic to $K_2[X]/ < \sigma P >$. The wanted result follows immediately. □

Corollary 5.23. *Let K be a field and $P \in K[X]$ be irreducible. Let L_1, L_2 be extensions of K containing two roots of P, say α and β. Then there is a unique K-isomorphism σ from $K(\alpha)$ to $K(\beta)$, with $\sigma(\alpha) = \beta$.*

Proof. Follows directly from Proposition 5.22, with $K_1 = K_2 = K$ and $\sigma = id_K$. □

Proposition 5.24. *Let K_1, K_2 be two fields, and σ be an isomorphism between K_1 and K_2. Let P be a polynomial in $K_1[X]$ of degree n, and let L_1 and L_2 be splitting fields of P and σP over K_1 and K_2 respectively. Then σ extends to an isomorphism σ' from L_1 to L_2.*

Proof. Let k be the number of distinct irreducible factors of P in $K_1[X]$. We prove the proposition by induction on $d_{K_1}(P) := n - k$, and for all the fields at the same time.

If $d_{K_1}(P) = 0$, then P splits into linear factors in K_1, so $L_1 = K_1$, $L_2 = K_2$ and there is nothing to prove.

Suppose that $d_{K_1}(P) \neq 0$, and let $Q \in K_1[X]$ be any irreducible factor of P of degree ≥ 2. Let $\alpha_1 \in L_1$ be any root of Q and $\alpha_2 \in L_2$ be any root of σQ. By Proposition 5.22, σ extends to an isomorphism $\tau : K_1(\alpha_1) \to K_2(\alpha_2)$. Furthermore, it is clear that $d_{K_1(\alpha_1)}(P) < d_{K_1}(P)$, and that L_1, L_2 are the splitting fields of $P, \sigma P$ over $K_1(\alpha_1), K_2(\alpha_2)$ respectively. So by the induction hypothesis, τ can be extended to an isomorphisms σ' from L_1 to L_2, and it is clear that σ' extends σ. □

Corollary 5.25. *Let K be a field, $P \in K[X]$ and L be a splitting field of P over K. Let K_1, K_2 be two intermediate fields, and $\sigma : K_1 \mapsto K_2$ be a K-isomorphism. Then σ extends to a K-automorphism σ' of L.*

Proof. Clear by Proposition 5.24. Take $L_1 = L_2 = L$, and note that L is the splitting field of P over K_i, $i = 1, 2$. □

Theorem 5.26. *Let K be a field, and $P \in K[X]$. Then any two splitting fields over K of the polynomial P are isomorphic.*

Proof. Immediate by Proposition 5.24: take $K_1 = K_2 = K$ and $\sigma = id_K$. □

Corollary 5.27. *Let K be a field, $P \in K[X]$ and L be a splitting field of P over K. Let $\alpha, \beta \in L$ be roots of P having the same minimal polynomial. Then there is a K-automorphism σ of L, with $\sigma(\alpha) = \beta$.*

Proof. The elements α and β have the same minimal polynomial over K, so by corollary 5.23 (where we set $L_1 = L_2 = L$), there is a K-isomorphism $\sigma_0 : K(\alpha) \mapsto K(\beta)$ with $\sigma_0(\alpha) = \beta$. By Corollary 5.25, σ_0 extends to a K-automorphism σ of L. It is clear that $\sigma(\alpha) = \beta$. □

Remark 5.28. The isomorphism σ of Proposition 5.24 does not always extend in a unique way. In fact, we will be mainly interested in the case where the extension is not unique: if $P \in K[X]$, and L is a splitting field of P, then the Galois group of P will be exactly the group of distinct extension of id_K to L.

5.2.1 An application: classifying finite fields

A finite field F has obviously a positive characteristic, say p. Furthermore, F is a vector space of dimension r over its prime field, which has p elements, so the cardinality of F is of the form p^r for some $r \in \mathbb{N} \setminus \{0\}$. We show now that for every prime number p and every $r \in \mathbb{N} \setminus \{0\}$, there is exactly one field of cardinality $q := p^r$. We shall later denote this field by $\mathbb{F}_q$. For $r = 1$ the result is clear with $\mathbb{F}_p = \mathbb{Z}/p$.

So fix p and r, and set $q := p^r$. Let $P := X^q - X \in \mathbb{F}_p[X]$, and let $\mathbb{F}_q$ be a splitting field of P over $\mathbb{F}_p$. The derivative ∂P of P is -1, so by Proposition 2.20 the roots of P are all distinct, they form a subset G of $\mathbb{F}_q$ of cardinality q. Using the fact that in $\mathbb{F}_q$, $(x+y)^p = x^p + y^p$, one checks easily that G is stable under $+, .$ and taking opposites and inverses, and it is obvious that $0, 1 \in G$. The set G is thus a field, so $G = \mathbb{F}_q$ and $\mathbb{F}_q$ has exactly q elements. That was for the existence.

As for the unicity, let F be any field having q elements. Note first that $char(F) = p$. Let F^* be the multiplicative group of F. So F^* has $q - 1$ elements, and for every $a \in F^*$ we have $a^{q-1} = 1$. It follows that for every $a \in F$, $a^q - a = 0$. So F is a splitting field over $\mathbb{F}_p$ of the polynomial $X^q - X$. By Theorem 5.26, F is isomorphic to $\mathbb{F}_q$. We proved the following.

Theorem 5.29. *The cardinality of a finite field is a natural number of the form p^r, where p is a prime number, and $r \in \mathbb{N} \setminus \{0\}$. Furthermore, for every prime p and $r \in \mathbb{N} \setminus \{0\}$, there is up to isomorphism exactly one field $\mathbb{F}_{p^r}$ of cardinality p^r. The field $\mathbb{F}_{p^r}$ is in fact the splitting field of the polynomial $X^{p^r} - X$ over $\mathbb{Z}/p$.*

5.3 Separable and inseparable extensions

Definition 5.30. Let K be a field.

1. A polynomial P in $K[X]$ is said to be ***separable*** if P splits into a product of distinct linear factors in some (hence any) splitting field for P. A polynomial P is said to be *inseparable* if it is not separable.

2. Let L/K be a field extension, and $\alpha \in L$ be an algebraic element over K. Then α is ***separable*** over K if its minimal polynomial over K is separable. Otherwise, α is an inseparable element.

3. Let L/K be an algebraic extension. Then the extension is said to be ***separable*** if all the elements of L are separable over K.

Remark 5.31. 1. If $char(K) = 0$, then every algebraic element α over K is separable: the minimal polynomial of α over K is irreducible, and by Proposition 2.21, irreducible polynomials have only simple roots in characteristic 0.

2. If $char(K) = p > 0$, let T be any indeterminate. So the extension $K(\sqrt[p]{T})/K(T)$ is not separable: $\sqrt[p]{T}$ is the root of the polynomial $P := X^p - (\sqrt[p]{T})^p = (X - \sqrt[p]{T})^p \in K(T)[X]$. So $\sqrt[p]{T}$ is the unique root of P, so it is the unique root of its minimal polynomial over $K(T)$, and is clearly not in $K(T)$. So $\sqrt[p]{T}$ is not separable over $K(T)$.

The following is easy.

Lemma 5.32. *Let M/K be a separable field extension and L be an intermediate field. Then the extensions M/L and L/K are separable.*

Definition 5.33. A field K is said to be ***perfect*** if every irreducible polynomial over K is separable. Equivalently, a field K is perfect if every algebraic extension of K is separable.

Lemma 5.34. *An algebraic extension of a perfect field is perfect.*

Proof. Follows directly by the Lemmas 5.14 and 5.32. □

Theorem 5.35. *A field K is perfect if and only if $char(K) = 0$, or $char(K) = p > 0$ and the Frobenius homomorphism $x \mapsto x^p$ is surjective. In particular, every finite field is perfect.*

Proof. If $char(K) = 0$, then by Proposition 2.21, an irreducible polynomial over K has only simple roots. Hence fields of characteristic 0 are perfect.

Now suppose that $char(K) = p > 0$. If the Frobenius homomorphism is not surjective, so let $a \in K \setminus K^p$ and let $L := K(\sqrt[p]{a})$. The polynomial $P := X^p - a = (X - \sqrt[p]{a})^p \in K[X]$ is irreducible (exercise) and it admits $\sqrt[p]{a}$ as a multiple root. Hence K is not perfect.

Suppose now that the Frobenius homomorphism is surjective, and let P be any polynomial which is not separable. We show that P is reducible. If it were not the case, then it follows by Proposition 2.21 that $\partial P = 0$. So P is of the form

$$a_n X^{p.n} + a_{n-1} X^{p.(n-1)} + \cdots + a_1 X^p + a_0.$$

Since the Frobenius is surjective, let for $0 \leq i \leq n$ b_i be a p^{th} root of a_i. So

$$\begin{aligned} P &= b_n^p X^{p.n} + b_{n-1}^p X^{p.(n-1)} + \cdots + b_1^p X^p + b_0^p \\ &= (b_n X^n + b_{n-1} X^{(n-1)} + \cdots + b_1 X + b_0)^p. \end{aligned}$$

So P is reducible, contradiction. □

Theorem 5.36. *Let K be a field of characteristic $p > 0$, and $P \in K[X]$ be an irreducible polynomial. Then all the roots of P have the same multiplicity, this multiplicity is a number of the form p^m for some $m \in \mathbb{N}$.*

Proof. Let m be the greatest natural number i such that P is a polynomial in X^{p^i}, and let $Q \in K[X]$ be such that $P(X) = Q(X^{p^m})$. It is clear that Q is irreducible. By the choice of m, Q is not a polynomial in X^p, so $\partial Q \neq 0$ and Q is separable. So in some extension of K, there are distinct elements $a_1, \cdots, a_n$, and an element $c \in K$ such that

$$Q(X) = c \prod_{i=1,\cdots,n} (X - a_i).$$

Let $b_1, \cdots, b_n$ be $p^{m^{th}}$ roots of $a_1, \cdots, a_n$ respectively, in some big extension of K. All the b_i are distinct by injectivity of the Frobenius map. Now we have

$$P(X) = Q(X^{p^m}) = \prod_{i=1,\cdots,n} (X^{p^m} - a_i) = \prod_{i=1,\cdots,n} (X^{p^m} - b_i^{p^m}) = \prod_{i=1,\cdots,n} (X - b_i)^{p^m}.$$

The claim follows directly □

5.4 Galois extensions

Definition 5.37. A field extension L/K is said to be a ***normal extension*** if for every $\alpha \in L$ algebraic over K, the minimal polynomial of α splits in $L[X]$.

Remark 5.38. The above definition is equivalent to: an extension L/K is normal if for every irreducible polynomial $P \in K[X]$, P has one root in L if and only if it has all its roots in L.

Definition 5.39.

1. Let L/K be a field extension. Then the ***Galois group*** $Gal(L/K)$ of the extension L/K is the group of all K-automorphisms of L.

   $$Gal(L/K) = \{\sigma \in Aut(L) : \forall x \in K, \sigma(x) = x\}.$$

   $Gal(L/K)$ is also called *the Galois group of L over K.*

2. Let K be a field and $P \in K[X]$. Then the ***Galois group of the polynomial*** P ***over*** K is the galois group the splitting field of P over K.

Remark 5.40. If $P \in K[X]$ is separable, then the Galois group of P over K is isomorphic to a subgroup of the group of permutations of the roots of P.

Definition 5.41. Let L/K be an algebraic extension, and let α be an element of L. Then the set $\{\sigma(\alpha), \sigma \in Gal(L/K)\}$ is the set of ***Galois conjugates*** of α in L (over K).

Theorem 5.42. *Let K be a field, $P \in K[X]$ and L be a splitting field of P over K. Let α be a root of P. Then the conjugates of α in L over K are the roots the minimal polynomial of α over K. So in particular, if α is separable, then the number of distinct conjugates of α is equal to the degree of α over K.*

Proof. Let Q be the minimal polynomial of α over K, and let β be a conjugate of α over K. Let $\sigma \in Gal(L/K)$ be such that $\sigma(\alpha) = \beta$. The coefficients of Q are in K, so they are fixed under σ. And since σ is a field automorphism, it is easy to check that $\sigma(Q(\alpha)) = Q(\sigma(\alpha))$. Now we have that

$$Q(\beta) = Q(\sigma(\alpha)) = \sigma(Q(\alpha)) = \sigma(0) = 0.$$

This shows that any conjugate of α over K is a root of the minimal polynomial of α over K.

Now let β be any root of Q. The polynomial Q divides P by Proposition 5.6, so β is also a root of P. Corollary 5.27 applies and yields that β is the image of α by some K-automorphism σ of L, thus that β is a conjugate of α over K.

For the last part of the theorem, note that the degree of α over K is the degree of the polynomial Q. So if Q has only simple roots, this is equal to the number of distinct roots of Q, thus the number of distinct conjugates of α over K. $\square$

Exercise 5.43. Determine the Galois groups over $\mathbb{Q}$ of the following extensions or polynomials:

1. $\bigcup_{1\leq n} \mathbb{Q}(\sqrt[n]{2})$ (the n^{th} roots here are real).
2. $X^6 - 1$.
3. $X^5 + X^4 + X^3 + X^2 + X + 1$.

Lemma 5.44. *Let M/K be an algebraic extension, and L be an intermediate field. Then $Gal(M/L)$ is a subgroup of $Gal(M/K)$.*

Proof. If f, g are automorphisms of M fixing L pointwise, then $f \circ g$ and f^{-1} are automorphisms of M, and they fix L pointwise. $\square$

Definition 5.45. Let L be a field and G be a groups of automorphisms of F. Then the ***fixed field*** $Fix(G)$ of G is the field of all the elements of L which are fixed under all the elements of G.

$$Fix(G) = \{x \in L : \forall \sigma \in G, \sigma(x) = x\}.$$

Remark 5.46. The fixed field is a field. (And the Galois group is a group). Note that $K \subset Fix(Gal(L/K))$.

Definition 5.47. Let L/K be an algebraic extension. Then L is a ***Galois extension*** of K if $Fix(Gal(L/K)) = K$. Equivalently, the extension is Galois if for any $x \in L \setminus K$, there is a K-automorphism f of L such that $f(x) \neq x$.

Theorem 5.48. *Let L/K be a finite field extension. Then the following are equivalent:*

1. *The extension L/K is Galois.*
2. *The extension L/K is normal and separable.*
3. *L is the splitting field over K of a separable polynomial $P \in K[X]$.*

Proof.

1. $1 \longrightarrow 2$: Let $a \in L$ and $a_1 = a, \cdots, a_p \in L$ be the different images of a under the action of $Gal(L/K)$. Let $P := (x - a_1).\cdots.(x - a_p)$. The polynomial P is separable since all its roots are distinct, and all the roots of P are in L. Moreover, P is fixed under the action of $Gal(L/K)$. Since the extension is Galois, the coefficients of P are in K and $P \in K[X]$. So for any $a \in L$, a is a root of a separable polynomial $P \in K[X]$, which has moreover all its roots in L. So the extension is normal and separable.

2. $2 \longrightarrow 3$: Let $\alpha_1, \cdots, \alpha_n \in L$ be such that $L = K(\alpha_1, \cdots, \alpha_n)$. Let $P_i \in K[X]$ be the minimal polynomial of α_i, $S := \{P_i : i \leq n\}$ and
$$P := \prod_{Q \in S} Q.$$
Then P is separable and L is the splitting field of P over K.

3. $3 \longrightarrow 1$: Let $B := Fix(Gal(L/K))$. The aim is to show that $B = K$. We do it by induction on the degree of P. If all the roots of P are already in K (so in particular if P has degree 1), then $L = K$ and there is nothing to prove. Suppose then that there is a root α of P which is not in K. We write $P(X) = Q(X).(X - \alpha)$, with $Q \in K(\alpha)[X]$. It is clear that L is the splitting field over $K(\alpha)$ of the polynomial Q, which is separable and with $deg(Q) < deg(P)$. So by the induction hypothesis we have that
$$K(\alpha) = Fix(Gal(L/K(\alpha))).$$
A $K(\alpha)$-isomorphism of L is also a K-isomorphism of L. So an element which is fixed by $Gal(L/K)$ is also fixed by $Gal(L/K(\alpha))$. This means that
$$B \subset Fix(Gal(L/K(\alpha))) = K(\alpha).$$
By the definition of B, the K-automorphisms of L are exactly the B-automorphisms of L, so the number of distinct conjugates of α in L over K is equal to the number of distinct conjugates of α in L over B. The field L is the splitting field –over K, and over B– of the separable polynomial P. So by Theorem 5.42,
$$[K(\alpha) : B] = [K(\alpha) : K].$$
On the other hand, we have that $K \subset B \subset K(\alpha)$. By Proposition 2.6, we have that $[B : K] = 1$ and $B = K$.

□

Proposition 5.49. *Let L/K be a finite separable field extension of degree n, and M be an extension of L. Let $\sigma : K \to M$ be a homomorphism, and assume that for every element $a \in L$ with minimal polynomial $M_a \in K[X]$, then $\sigma(M_a)$ splits in M in linear factors. Then there are exactly n different homomorphisms of L to M extending σ.*

Proof. By induction on n. If $n = 1$, then $L = K$ and the result is obvious. Suppose the result true for all $i < n$ and let $a \in L \setminus K$ be of degree m over K. By separability and Proposition 5.22 of L/K, there are exactly m homomorphisms $\tau_1, \cdots, \tau_m$ from $K(a)$ to M extending σ. The degree $[L : K(a)]$ is strictly smaller than n, so by the induction hypothesis, for each of the τ_i, there are exactly $[L : K(a)]$ homomorphisms from L to M extending τ_i. The number of homomorphisms from L to M extending σ is then $[L : K(a)].m = [L : K(a)].[K(a) : K] = n$.

□

Proposition 5.50. *Let L/K be a finite separable field extension of degree n, and let M be a normal extension of K containing L. Then there are exactly n K-homomorphisms from L to M.*

Proof. Apply the above Proposition 5.49 with $\sigma = id_K$. □

Theorem 5.51. *Let L/K be a finite Galois extension. Then $|Gal(L/K)| = [L : K]$.*

Proof. By Theorem 5.48, a finite Galois extension is a finite normal separable extension. Apply then Proposition 5.50 with $M = L$, and note that since the degree of L/K is finite, then any K-endomorphism of L is in fact a K-automorphism. □

5.5 Simple extensions

Definition 5.52. Let L/K be a field extension, such that $L = K(\alpha)$ for some element α in L. Then L is a ***simple extension*** of K, and α is a ***primitive element*** of L/K.

Proposition 5.53. *Let F be a finite field. Then the multiplicative group F^* of F is cyclic.*

Proof. Let q be the cardinality of F, so the cardinality of F^* is $q-1$. By lemma 10.2, showing that the group F^* is cyclic is equivalent to showing that there is an element $a \in F^*$ with order $q-1$ (by order of an element here we mean the order in the multiplicative group). For a contradiction, suppose that $s < q-1$ is the maximal order of an element of F^*, and let $a \in F^*$ be an element with order s. An element of F^* with order dividing s is an element of the field which is a root of the polynomial $X^s - 1$. So there are at most s elements of F^* with order dividing s. Since $s < q-1$, one can find an element $b \in F^*$ with order t such that t does not divide s.
Write s and t as a product of prime factors,

$$s = p_1^{k_1}.p_2^{k_2}.\cdots.p_n^{k_n},$$

and

$$t = p_1^{l_1}.p_2^{l_2}.\cdots.p_n^{l_n}.$$

We can suppose that for some $j \leq n$, $k_i < l_i$ for $i \leq j$, and $k_i \geq l_i$ for $i > j$. Since s is maximal, we have that $j \neq n$. But t does not divide s, hence $j \neq 0$. Let

$$\alpha := a^{p_1^{k_1}.p_2^{k_2}.\cdots.p_j^{k_j}},$$

and

$$\beta := b^{p_{j+1}^{l_{j+1}}.\cdots.p_n^{l_n}}.$$

It is easy to see that the order o_α of α is $p_{j+1}^{k_{j+1}}.\cdots.p_n^{k_n}$, and that the order o_β of β is $p_1^{l_1}.p_2^{l_2}.\cdots.p_j^{l_j}$. The natural numbers o_α and o_β are relatively prime, so by Lemma 10.3, the order of $\alpha.\beta$ is $o_\alpha.o_\beta > s$, since $o_\alpha.o_\beta$ is the least common multiple of s and t, where t does not divide s. This contradicts the maximality of s. □

Lemma 5.54. *Let K be an infinite field and V be a K-vector space. Let $H_1, \cdots, H_n$ be a finite family of proper subspaces of V. Then $V \neq \bigcup_{i \leq n} H_i$.*

Proof. We prove the result by induction. The result is clear for $n = 1$. Suppose it is proved for n and we show it for $n+1$. Let $H_1, \cdots, H_{n+1}$ be a finite family of proper subspaces of V and suppose for a contradiction that

$$V = \bigcup_{1 \leq i \leq n+1} H_i. \qquad (*)$$

By the induction hypothesis, $V \neq \bigcup_{i \leq n} H_i$. So let $x \in V \setminus \bigcup_{i \leq n} H_i$, and let $y \in V \setminus H_{n+1}$. Since K is infinite, and by $(*)$, we can find $\lambda \neq \delta \in K$ and $i \leq n+1$ such that $x + \lambda y \in H_i$ and $x + \delta y \in H_i$. So both x and y are in H_i. Which is a contradiction.

□

Theorem 5.55. *Let L/K be a finite separable extension. Then L/K is simple.*

Remark: This result was given (for extensions of $\mathbb{Q}$) by Galois without proof.

Proof. Suppose first that K is finite. Since the extension is finite, then L is a finite field. The wanted result is a direct consequence of Proposition 5.53.

Suppose now that K is infinite, and let $n := [L : K]$. Let M be a normal extension of K containing L. The extension L/K is separable of degree n, so by Corollary 5.50 there are exactly n different K-homomorphisms, $\sigma_1, \cdots, \sigma_n$ from L to M. Now we look at L as a K-vector space, and at the σ_i as K-vector space homomorphisms. For any i, j, $\sigma_i \neq \sigma_j$, so $L_{ij} := ker(\sigma_i - \sigma_j) \neq L$. There are finitely many L_{ij} and all of them are proper K-subspaces of the K-vector space L. The field K is infinite, so by Lemma 5.54 we have

$$U := \bigcup_{1 \leq i < j \leq n} L_{ij} \neq L.$$

Let $a \in L \backslash U$. So for any $i < j \leq n$, $\sigma_i(a) \neq \sigma_j(a)$, thus a has at least n different conjugates over K. By Theorem 5.42, the degree of $K(a)$ over K is at least n. But $K(a) \subset L$ and the degree of L over K is n. So $L = K(a)$. □

Proposition 5.56. *Let L/K be a simple algebraic field extension. Then L/K has finitely many intermediate fields.*

Proof. Let $\alpha \in L$ be such that $L = K(\alpha)$, and let P be the minimal polynomial of α over K. Let A be any intermediate field and Q be the minimal polynomial of α over A. It is clear that Q divides P. Denote by B the subfield of L generated over K by the coefficients of Q. So $B \subset A$, and on the other hand, $Q \in B[X]$, and $Q(\alpha) = 0$. So the degree of α over A, which is the degree of Q, is greater than or equal to the degree of α over B. Therefore $A = B$.
Any intermediate field is thus a subfield of L generated by the coefficients of a normed factor of P. The wanted result follows. □

We have even a method to find the intermediate fields of a simple algebraic extension: if L, K, P and α are as in the proposition with $[L : K] = n$, then an intermediate field A of degree m over K is generated by the coefficients of some normed factor of P having α as a root.

Example. The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is simple, and admits $\sqrt{2} + \sqrt{3}$ as a primitive element.The minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is

$$X^4 - 10X^2 + 1,$$

the other roots of being $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$ and $-\sqrt{2} - \sqrt{3}$. A proper intermediate field has necessarily degree 2 over $\mathbb{Q}$, is thus by the above argument generated by the coefficients of one of the following polynomials:

$(X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3})) = X^2 - 2\sqrt{2}X - 1$
$(X - (\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3})) = X^2 - 2\sqrt{3}X + 1$
$(X - (\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} - \sqrt{3})) = X^2 - (5 + 2\sqrt{6})$.
The proper intermediate fields of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ are thus the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$.

Example. The extension $\mathbb{Q}(i, \sqrt[3]{2})$ is simple and is generated $i + \sqrt[3]{2}$ (exercise). The minimal polynomial of $i + \sqrt[3]{2}$ is

$$P := X^6 + 3X^4 - 4X^3 + 3X^2 + 12X + 5,$$

the other roots being $i + j\sqrt[3]{2}$, $i + j^2\sqrt[3]{2}$, $-i + \sqrt[3]{2}$, $-i + j\sqrt[3]{2}$, $-i + j^2\sqrt[3]{2}$. A proper intermediate field has degree 2 or 3 over $\mathbb{Q}$.

An intermediate field of degree 3 over $\mathbb{Q}$ is generated by the coefficients of one of the following polynomials: $(X - (i + \sqrt[3]{2})).(X - (-i + \sqrt[3]{2}))$, $(X - (i + \sqrt[3]{2})).(X - (\pm i + j\sqrt[3]{2}))$, $(X - (i + \sqrt[3]{2})).(X - (\pm i + j^2\sqrt[3]{2}))$. The last four polynomials are not in $\mathbb{Q}(i, \sqrt[3]{2})$, so the only possible factor is the first one, which is

$$(X - \sqrt[3]{2})^2 + 1 = X^2 - 2\sqrt[3]{2}X + \sqrt[3]{4} + 1.$$

So the only intermediate field of degree 3 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2})$.

The intermediate fields of degree 2 over $\mathbb{Q}$ are given by the factors of degree 3 of P having $i + \sqrt[3]{2}$ as a root, and coefficients in $\mathbb{Q}(i, \sqrt[3]{2})$. The decomposition

$$P = (X^3 - 3iX^2 - 3X - 2 + i).(X^3 + 3iX^2 - 3X - 2 - i)$$

yields the field $\mathbb{Q}(i)$.

Counterexample 1. Let p be a prime number, X, Y be two distinct free variables. Let $L := \mathbb{F}_p(\sqrt[p]{X}, \sqrt[p]{Y})$ and $K := \mathbb{F}_p(X, Y)$. Then the extension L/K has degree p^2, but for every $a \in L$, a has degree p over K since $a^p \in K$. So L/K is not simple.

6 Examples

Fix a field K with $char(K) \neq 2, 3$. The easiest non-trivial example of a Galois group of a polynomial $P \in K[X]$ is the case where P is quadratic, say $P = aX^2 + bX + c$. The splitting field of P is then $K(\sqrt{\Delta})$, where $\Delta = b^2 - 4ac$, and $Gal(K(\sqrt{\Delta})/K)$ is isomorphic to the trivial group or $\mathbb{Z}/2$, depending on whether Δ has a square root in K or not.

6.1 The Galois group of cubic polynomials

Let $P = X^3 + pX + q \in K[X]$, denote by L the splitting field of P over K, and let a, b and c be the roots of P. If P is reducible, then it is the product of a linear and a quadratic polynomial. Therefore, $Gal(L/K)$ is the trivial group or $\mathbb{Z}/2$, depending on whether P splits or not in linear factors over K.

Suppose from now on that P is irreducible. If $L = K(a)$, then $[L : K] = 3$, and $Gal(L/K)$ is a subgroup of S_3 of order three. So $Gal(L/K) = A_3$. If $K(a)$ is a proper subfield of L, then $[L : K] = 6$ (to see this, note that $L = K(a, b)$, and b has degree 1 or 2 over $K(a)$, depending on whether $K(a) = L$ or not.) So $Gal(L/K)$ is a subgroup of order 6 of S_3, is thus equal to S_3.

We give now an easy criterion to determine whether the Galois group of P is A_3 or S_3. Let $\Delta = (a-b)^2(b-c)^2(a-c)^2$ be the discriminant of P. This is a symmetric function of the roots, and a simple calculation shows that $\Delta = -4p^3 - 27q^2$. Let d be a square root of Δ, say $d := (a-b)(a-c)(b-c)$. It is clear that $d \in L$.

We check now that $L = K(d, a)$. Indeed, noting that $a + b + c = 0$ and $abc = -q$, we have

$$(a-b)(a-c) = a^2 - a(b+c) + bc = 2a^2 - \frac{q}{a} \in K(a)$$

is an element of $K(a)$, so $b - c$ is an element of $K(d, a)$. It is clear now that b and c are elements of $K(d, a)$, and this proves our claim.

Now we have two cases:

1. If Δ has a square root in K, so $d \in K$ and $L = K(a)$ has degree three over K. In this case, $Gal(L/K)$ is A_3.
2. If Δ does not have a square root in K, so d has degree 2 over K, and for divisibility reasons, the degree of a over $K(d)$ remains 3. So $[L : K] = 6$ and $Gal(L/K) = S_3$.

Example. The polynomials $X^3 - 3X + 1$ and $X^3 + 3X + 1$ are irreducible over $\mathbb{Q}$. Their discriminants are 81 and -135, their Galois groups over $\mathbb{Q}$ are thus A_3 and S_3 respectively. Any root of the first polynomial is a primitive element of its splitting field. For the second one, a root is not sufficient: one needs also $\sqrt{-135}$ or $i\sqrt{15}$. A primitive element in the second case is for example $a + i\sqrt{15}$, where a denotes a root of $X^3 + 3X + 1$.

6.2 Galois groups over finite fields

Let $p \in \mathbb{N}$ be prime, $r \in \mathbb{N}^*$ and $q := p^r$. Every element of $\mathbb{F}_p$ is invariant under any automorphism of $\mathbb{F}_q$, and the extension $\mathbb{F}_q/\mathbb{F}_p$ is separable and has degree r. Therefore, $Gal(\mathbb{F}_q/\mathbb{F}_p)$ has exactly r elements.

A particular element of $Gal(\mathbb{F}_q/\mathbb{F}_p)$ is the Frobenius map $f_p : x \mapsto x^p$. If $n \in \mathbb{N}$ is such that $(f_p)^n = id$, then $x^{p^n} = x$ holds for every $x \in \mathbb{F}_q$, and since $\mathbb{F}_q$ has p^r distinct elements, then $n \geq r$. This shows that the order of f_p in $Gal(\mathbb{F}_q/\mathbb{F}_p)$ is exactly r, hence $Gal(\mathbb{F}_q/\mathbb{F}_p)$ is a cyclic abelian group generated by f_p. Now if K is any finite field with $char(K) = p$, and if $\mathbb{F}_q$ is an extension of K, then $Gal(\mathbb{F}_q/K)$ is a subgroup of $Gal(F_q/F_p)$, is thus a cyclic abelian group. We showed the following.

Theorem 6.1. *Let L/K be a finite field extension of finite fields. Then $Gal(L/K)$ is a cyclic abelian group.*

Let K be a finite field and $P \in K[X]$ be separable of degree n. The galois group G of P, seen as a group of permutations of the roots of P, is a cyclic subgroup of S_n, generated by some $\sigma \in S_n$. Furthermore, P is irreducible if and only if the action of G on the roots is transitive (Theorem 5.42), if and only if G is generated by some cycle of length n.

If P is reducible, write $P = P_1 . \cdots . P_m$ with the P_i irreducible, and write $\sigma = \sigma_1 . \cdots . \sigma_{m'}$ where the σ_i are disjoint cycles. It is easy to see that the restriction of σ to the set of roots of P_i is one of the σ_j, and we have moreover that the degree of P_i is equal to the length of σ_j. So after permuting the P_i, we can suppose that for ever i, σ_i is a generator of the Galois group of P_i over K.

Example. On $\mathbb{F}_5$ we have:

$$X^5 + 2X^2 + X + 4 = (X^2 + 2)(X^3 + 3X + 2),$$

and the two factors are irreducible. So after renumbering the roots, we have that the Galois group of $X^5 + 2X^2 + X + 4$ over $\mathbb{F}_5$ is the subgroup of S_n generated by $(1, 2)(3, 4, 5)$.

6.3 On the Galois group of binomial equations in characteristic 0

Let $n \in \mathbb{N} \setminus \{0\}$ and $w := e^{2i\pi/n}$. Any element σ of the Galois group of $X^n - 1$ over $\mathbb{Q}$ is determined by the image of w, which is some power of w. Let σ_1, σ_2 be in the Galois group, $\sigma_1(w) = w^{a_1}$ and $\sigma_2(w) = w^{a_2}$ (note that $a_1, a_2 \neq 0$). Then $\sigma_1 \circ \sigma_2(w) = w^{a_1 a_2}$. Therefore, the Galois group of $X^n - 1$ is a subgroup of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of invertible elements in $(\mathbb{Z}/n\mathbb{Z}, .)$. In particular, it is abelian.

Now let $n \in \mathbb{N} \setminus \{0\}$, $w := e^{2i\pi/n}$, K be an extension of $\mathbb{Q}$ containing w, b be an element of K, $a \in \mathbb{C}$ be such that $a^n = b$ and G be the Galois group of $X^n - b$ over K. An element of G is determined by the image of a, which is an element of the form $w^i a$ for some $i \leq n$. Furthermore, if $\sigma_1(a) = w^{i_1} a$ and $\sigma_2(a) = w^{i_2}.a$, then $\sigma_1 \circ \sigma_2(a) = w^{i_1+i_2} a$. Hence, the Galois group of $X^n - a$ is a subgroup of $\mathbb{Z}/n$, it is thus abelian. Furthermore, the degree of splitting field of $X^n - a$, which is the order of the galois group, divides n.

6.4 The Galois group of $X^4 - a$ over $\mathbb{Q}$.

Let $a \in \mathbb{Q}$ and $P = X^4 - a$. Note first that

$$\sqrt[4]{a} = \sqrt[4]{-(-a)} = \frac{1+i}{\sqrt{2}} \sqrt[4]{-a} = \frac{1+i}{2} \sqrt[4]{-4a}.$$

So we get the roots of P by multiplying the roots of $Q := X^4 + 4a$ by $(1+i)/2$. Since i in the splitting fields of both P and Q, these two polynomials have the same splitting field over $\mathbb{Q}$. We can thus suppose without loss of generality that $a > 0$. We have three cases:

1. P **has a root** b **in** $\mathbb{Q}$**:** In this case, we write $P = (X-b)(X+b)(X^2+b^2)$, and the Galois group of P is $\mathbb{Z}/2$.

   Example: $P = X^4 - 1$, the Galois group of P contains the identity, and the transposition exchanging the roots i and $-i$. The polynomial X^4+4 provides another example with Galois group $\mathbb{Z}/2$. To see this, use the above remark and the fact that $-4.(-4) = 16$ is positive, and has a quartic root in $\mathbb{Q}$.

2. P **splits but has no roots in** $\mathbb{Q}$**:** We write P as a product $(X^2+\alpha X+\beta)(X^2+\alpha' X+\beta')$. A simple calculation shows that $\alpha = \alpha' = 0$ and $\beta = -\beta'$ (simple unless you forget that $a > 0$). So $\beta \in \mathbb{Q}$, has no square roots in $\mathbb{Q}$, and $P = (X^2 - \beta)(X^2 + \beta)$. The splitting field is then $\mathbb{Q}(\sqrt{\beta}, i)$, and the Galois group of P is $\mathbb{Z}/2 \times \mathbb{Z}/2$.

   Example: $X^4 - 4$. Number the roots $\sqrt{2}, -\sqrt{2}, i\sqrt{2}, -i\sqrt{2}$ by $1, 2, 3$ and 4 respectively. The Galois group consists of the following permutations of the roots:

   $$id \qquad (1,2) \qquad (3,4) \qquad (1,2)(3,4).$$

3. P **is irreducible:** The splitting field is generated by i and the real quartic root of a, has thus degree 8 over $\mathbb{Q}$. The Galois group G of P is a subgroup of S_4 of order 8. By Sylow (or direct checking) G is isomorphic to the dihedral group D_8.

   Example: $X^4 - 2$. Number the roots $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$ by $1, 2, 3$ and 4 respectively. The Galois group corresponds to the following permutations of the roots:

   $$\begin{array}{cccc} id & (1,2,3,4) & (1,3)(2,4) & (1,4,3,2) \\ (2,4) & (1,2)(3,4) & (1,3) & (1,4)(2,3). \end{array}$$

7 The fundamental theorem of Galois theory

7.1 The main theorem

Theorem 7.1. *(Emil Artin) Let L/K be any field extension, and H be a finite subgroup of $Gal(L/K)$ of order r. Then L is a finite Galois extension of $B := Fix(H)$, and $Gal(L/B) = H$.*

Proof. Let a be an element of L, and $a_1 = a, a_2, \cdots, a_m$, $m \leq r$, be the set of different images of a under the action of H. The separable polynomial

$$P := \prod_{1 \leq i \leq m} (X - a_i)$$

remains unchanged under any $g \in H$, and has thus all its coefficients in B. This shows that for all $a \in L$, a is algebraic separable and normal over B, and $[B(a) : B] \leq r$.

Choose $a \in L$ with maximal degree over B, and denote this degree by s. If $B(a) \neq L$, let $b \in L \setminus B(a)$. The extension $B(a,b)/B$ is finite and separable since both a and b are separable and have finite degree over B. By Theorem 5.55, $B(a,b) = B(c)$ for some $c \in L$. By the choice of b, $B(a,b)$ contains strictly $B(a)$, so $[B(c) : B] > [B(a) : B]$. This contradicts the maximality of s, and shows that $L = B(a)$. Therefore, $[L : B] = s \leq r$, and L/B is a finite normal separable extension, thus a Galois extension by Theorem 5.48.

By Proposition 5.51, $|Gal(L/B)| = s \leq r$. On the other hand, by the definition of B we have that $H \subset Gal(L/B)$. Thus $s = r$, and $Gal(L/B) = H$. □

Theorem 7.2. *(Fundamental theorem of Galois Theory - FTGT)*
Let L/K be a finite Galois extension. Let $\mathcal{F}$ be the set of intermediate fields of L/K, and $\mathcal{G}$ be the set of subgroups of $Gal(L/K)$.
Denote by $Fix : \mathcal{G} \longrightarrow \mathcal{F}$ the application which to a subgroup H of $Gal(L/K)$ associates the fixed field of H, and by $G : \mathcal{F} \longrightarrow \mathcal{G}$ the application which to an intermediate field F associates the Galois group $Gal(L/F)$. Then the following hold:

1. *Fix and G define reciprocal bijections, decreasing for the inclusion.*
2. *Fix and G define by restriction reciprocal bijections between the set $\mathcal{F}'$ of normal extensions of K contained in L, and the set $\mathcal{G}'$ of normal subgroups of $Gal(L/K)$.*
3. *If F and F' are two elements of $\mathcal{F}$, then F' is a normal extension of F if and only if $Gal(L/F')$ is a normal subgroup of $Gal(L/F)$. In this case we have*

$$Gal(F'/F) = \frac{Gal(L/F)}{Gal(L/F')}$$

4. *If F and F' are two elements of $\mathcal{F}$ such that $F \subset F'$, then*

$$[F' : F] = \frac{|Gal(L/F)|}{|Gal(L/F')|}.$$

Proof. 1. It is clear that Fix and G are well defined and decreasing for the inclusion. The fact that $Fix \circ G = id_{\mathcal{F}}$ is a direct consequence of the fact that L/F is a Galois extension, for any $F \in \mathcal{F}$. The fact that $G \circ Fix = id_{\mathcal{G}}$ is exactly what Theorem 7.1 states.

2. - Let $F \in \mathcal{F}'$. Fix an element $\sigma \in G(F)$, and let τ be any element of $Gal(L/K)$. Let x be an element of F. Since F/K is normal, then $\tau(x) \in F$, so $\sigma\tau(x) = \tau(x)$, and $\tau^{-1}\sigma\tau(x) = x$. This shows that $\tau^{-1}\sigma\tau \in G(F)$, so $G(F)$ is a normal subgroup of $Gal(L/K)$, thus $G(F) \in \mathcal{G}'$.
   - Let $H \in \mathcal{G}'$, $x \in Fix(H)$, and y be any root of the minimal polynomial of x over K. The aim is to show that $y \in Fix(H)$. By Theorem 5.42, there is $\tau \in Gal(L/K)$ such that $\tau(x) = y$. Let σ be any element of H. Since H is normal, then $\tau^{-1}\sigma\tau \in H$, thus $\tau^{-1}\sigma\tau(x) = x$, and $\sigma\tau(x) = \tau(x)$. This shows that $y = \tau(x) \in Fix(H)$. Therefore, the extension $Fix(H)/K$ is normal, and $Fix(H) \in \mathcal{F}'$.

3. For the first claim, use *2* with F instead of K. For the second part, note that if F' is a normal extension of F, then the restriction operation

$$\varphi := \begin{cases} Gal(L/F) & \to Gal(F'/F) \\ \sigma & \mapsto \sigma|F' \end{cases}$$

is a well defined epimorphism, and $Ker(\varphi) = Gal(L/F')$. The wanted result follows.

4. Since L/F and L/F' are Galois extensions, by Theorem 5.51 we have the following:

$$[F' : F] = \frac{[L : F]}{[L : F']} = \frac{|Gal(L/F)|}{|Gal(L/F')|}.$$

□

Example. Let $L = \mathbb{Q}(\sqrt[3]{2}, j)$ be the splitting field of $X^3 - 2$. We number the roots $\sqrt[3]{2}, j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$ by $1, 2$ and 3 respectively. We have seen that $Gal(L/\mathbb{Q}) = S_3$. The group S_3 has 6 subgroups:

$$\{id\} \qquad A_3 \qquad S_3 \qquad \{id, (1,2)\} \qquad \{id, (1,3)\} \qquad \{id, (2,3)\}.$$

The first three of these subgroups are normal, and the last three are not. They correspond by the Galois correspondence to the following intermediate fields of L/K respectively

$$\mathbb{Q}(\sqrt[3]{2}, j) \qquad \mathbb{Q}(j) \qquad \mathbb{Q} \qquad \mathbb{Q}(j^2\sqrt[3]{2}) \qquad \mathbb{Q}(j\sqrt[3]{2}) \qquad \mathbb{Q}(\sqrt[3]{2}).$$

The first three of those fields are normal extensions of $\mathbb{Q}$, and the last three are not. Those are all the intermediate fields of the extension.

7.2 Example: the Galois group as a direct product

Let M/K be a finite Galois extension, and L_1, L_2 be intermediate fields, which are normal extensions of K. Denote by $G := Gal(M/K)$, $G_1 := Gal(M/L_1)$ and $G_2 := Gal(M/L_2)$. Then we have the following

Fact: If $L_1 \cup L_2$ generates M and $L_1 \cap L_2 = K$, then $G \simeq G_1 \times G_2$. Furthermore, we have that

$$G = Gal(M/K) \simeq Gal(L_1/K) \times Gal(L_2/K).$$

It is sufficient to show that G_1, G_2 are normal subgroups of G, that $G_1 \cap G_2 = \{1\}$ and $G_1.G_2 = G$. The fact that G_1 and G_2 are normal subgroups is given by the second point of Theorem 7.2, and the fact that $G_1 \cap G_2 = \{1\}$ and $G_1.G_2 = G$ follows by the first point of the same theorem. The third point of the theorem yields now directly that

$$Gal(M/K) \simeq Gal(L_1/K) \times Gal(L_2/K).$$

Application: let $p < q$ be two prime natural numbers such that p does not divide $q-1$, and $K := \mathbb{Q}(e^{2i\pi/p}, e^{2i\pi/q})$. Let a, b be two elements of K not having p^{th} and q^{th} roots respectively in $\mathbb{Q}$. Let α, β be a p^{th} and a q^{th} root of a, b respectively, and set $L := K(\alpha, \beta)$.

Claim. α has degree p over K:

By Section 6.3, the degree of $e^{2i\pi/p}$ over $\mathbb{Q}$ divides $p-1$, and the degree of $e^{2i\pi/q}$ over $\mathbb{Q}(e^{2i\pi/p})$ divides $q-1$. So the degree of $K/\mathbb{Q}$ is prime to p, which is the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$. This shows that $\alpha \notin K$. Furthermore, again by Section 6.3, the degree of α over K divides p, which is a prime number. So the degree of α over K is necessarily p, and this proves our claim.

A similar argument shows that β has degree q over K. Now since p and q are relatively prime, we have that $K(\alpha) \cap K(\beta) = K$. By the above fact, $Gal(L/K) = \mathbb{Z}/p \times \mathbb{Z}/q$. Furthermore, $\mathbb{Z}/p \times \mathbb{Z}/q$ has exactly four subgroups: $\{0\}, \mathbb{Z}/p \times \{0\}$, $\{0\} \times \mathbb{Z}/q$ and $\mathbb{Z}/p \times \mathbb{Z}/q$, which correspond to the four intermediate fields: K, $K(\beta)$, $K(\alpha)$ and L. In particular, if $x \in L \setminus K(\alpha) \cup K(\beta)$, then x has degree pq over K.

Example: $\sqrt[5]{3} + \sqrt[7]{5}$ is a primitive element of $\mathbb{Q}(\sqrt[5]{3}, \sqrt[7]{5})/\mathbb{Q}$.

8 Applications

8.1 The fundamental theorem of algebra

We show in this section that the field $\mathbb{C}$ is algebraically closed. We use that in $\mathbb{R}$, a polynomial of odd degree has at least one real root.

Lemma 8.1. *An element of $\mathbb{C}$ has its square roots in $\mathbb{C}$.*

Proof. Let $a = r.e^{i\theta}$ be an element of $\mathbb{C}$, and let $b := \sqrt{r}.e^{i\theta/2}$. Then $b^2 = a$. □

Proposition 8.2. *A polynomial $P \in \mathbb{R}[X]$ splits in $\mathbb{C}$ in linear factors.*

Proof. Let $P \in \mathbb{R}[X]$, and let L be the splitting field of $(X^2+1)P$ over $\mathbb{R}$. We want to show that $L = \mathbb{C}$. The field $\mathbb{R}$ has characteristic zero, so $L/\mathbb{R}$ is separable, thus Galois. By Theorem 10.6, let H be a Sylow 2-subgroup of $Gal(L/\mathbb{R})$, and $K := Fix(H)$. The index of H in G is odd, so by Theorem 7.2, $[K : \mathbb{R}]$ is odd. Let $\alpha \in K$ be a primitive element of the extension $K/\mathbb{R}$, and $Q \in \mathbb{R}[X]$ be its minimal polynomial. Then $deg(Q)$ is odd, and Q has a root in $\mathbb{R}$. Since Q is irreducible, then Q is linear. This shows that $K = \mathbb{R}$, and $Gal(L/\mathbb{R})$ is a 2-group. Since $Gal(L/\mathbb{C})$ is a subgroup of $Gal(L/\mathbb{R})$, then the same holds for $Gal(L/\mathbb{C})$.

If L is a proper extension of $\mathbb{C}$, then $Gal(L/\mathbb{C})$ is non trivial. By Proposition 10.4, there is a subgroup of $Gal(L/\mathbb{C})$ of index 2, which corresponds by Theorem 7.2 to an extension of $\mathbb{C}$ of degree 2, thus a non trivial extension of $\mathbb{C}$ by a square root. Contradiction. □

Theorem 8.3. *The field $\mathbb{C}$ is algebraically closed.*

Proof. Let $P \in \mathbb{C}[X]$, say $P = \sum a_i X^i$. Let b_i be the complex conjugate of a_i, and $Q := \sum b_i X^i$. The polynomial PQ remains unchanged under complex conjugation, thus PQ is in $\mathbb{R}[X]$. By Proposition 8.2, the polynomial PQ splits in $\mathbb{C}$ in linear factors. In particular, P splits in $\mathbb{C}$ in linear factors. □

8.2 Cyclotomic extensions

8.2.1 The group $(\mathbb{Z}/n\mathbb{Z})^\times$ of invertibles of $\mathbb{Z}/n\mathbb{Z}$

An element x is invertible in $\mathbb{Z}/n\mathbb{Z}$ if and only if it is prime to n. The set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$. It is a multiplicative group. The order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$, where φ is the Euler function defined by: $\varphi(n) := |\{m : m < n, gcd(m,n) = 1\}|$.

Proposition 8.4.

1. *If $n = rs$ with $gcd(r,s) = 1$, then $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times$ and $\varphi(n) = \varphi(r)\varphi(s)$.*
2. *If $n = p^k$ for some prime $p > 2$, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic of order $\varphi(p^k) = p^k - p^{k-1}$.*
3. *For $k \geq 2$, $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.*
4. *If $\{p_i : i \in I\}$ is the set of distinct prime factors of n, then $\varphi(n) = n.\prod_{i\in I}(1 - \frac{1}{p_i})$.*

Example. $1400 = 2^3.5^2.7$, so $\varphi(1400) = 1400.(1-\frac{1}{2}).(1-\frac{1}{5}).(1-\frac{1}{7}) = 480$.

8.2.2 Möbius inversion formula

A function $f : \mathbb{N}^* \to \mathbb{R}$ is said to be multiplicative if for all m, n with $gcd(m,n) = 1$, we have $f(mn) = f(m).f(n)$.

Example. The Euler phi function is multiplicative.

We define the Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ as follows:
$\mu(1) = 1$
$\mu(n) = 0$ if n has a square factor.
$\mu(n) = (-1)^r$ if n has no square factors, where r is the number of the different prime factors of n.

Proposition 8.5. *The Möbius function is multiplicative, and for every $n > 1$ we have*

$$\sum_{d\in D(n)} \mu(d) = 0.$$

Proof. Let $n := \prod_{i=1,\cdot,r} p_i^{k_i}$ be the decomposition of m as a product of distinct prime factors, and let $m := \prod_{i=1,\cdot,r} p_i$. Then

$$\sum_{d\in D(n)} \mu(d) = \sum_{d\in D(m)} \mu(d) = \sum_{0\leq k\leq r} \binom{r}{k}(-1)^k = (1-1)^r.$$

□

Proposition 8.6. *Let $(G, .)$ be an abelian group, $g : \mathbb{N}^* \to G$ be a function, and $f : \mathbb{N}^* \to G$ be the function defined by:*

$$f(n) := \sum_{d|n} g(d).$$

Then for every $n \in \mathbb{N}^*$,

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) f(d).$$

Remark 8.7. If the operation of G is denoted multiplicatively, then the result states that if

$$f(n) := \prod_{d|n} g(d),$$

then for every $n \in \mathbb{N}^*$,

$$g(n) = \prod_{d|n} [f(\frac{n}{d})]^{\mu(d)} = \prod_{d|n} [f(d)]^{\mu(\frac{n}{d})}.$$

This is known as the Möbius inversion formula.

Proof. $\displaystyle\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(d) \Bigg(\sum_{e|\frac{n}{d}} g(e) \Bigg) = \sum_{e|n} g(e) \Bigg(\sum_{d|\frac{n}{e}} \mu(d) \Bigg) = g(n).$ □

8.2.3 Roots of Unity

In this section we work in characteristic zero. An n^{th} root of unity is thus an element of $\mathbb{C}$ of the form $e^{2ki\pi/n}$. The set of n^{th} roots of unity form an abelian multiplicative group χ_n, which is isomorphic to $\mathbb{Z}/n$. An n^{th} root of unity is said to be ***primitive*** if it generates $(\chi_n, .)$. It is easy to check that an n^{th} root $e^{2ki\pi/n}$ is primitive if and only if $gcd(n, k) = 1$. There are thus exactly $\varphi(n)$ primitive n^{th} roots of unity. The n^{th} ***cyclotomic polynomial*** is the polynomial of degree $\varphi(n)$ defined by

$$\Phi_n(X) := \prod_{\alpha \text{ primitive}} (X - \alpha).$$

Proposition 8.8.

1. $X^n - 1 = \displaystyle\prod_{d|n} \Phi_d(X)$.

2. $\Phi_n(X) = \displaystyle\prod_{d|n} (X^d - 1)^{\mu(n/d)}$, *and if n is prime, then* $\Phi_n(X) = \displaystyle\sum_{0 \leq i \leq n-1} X^i$.

3. $\Phi_n(X) \in \mathbb{Z}[X]$.

4. $\Phi_n(X)$ *is irreducible over* $\mathbb{Q}$.

Proof. 1. $X^n - 1 = \displaystyle\prod_{\alpha \in \chi_n} (X - \alpha) = \prod_{d|n} \prod_{\alpha \in \chi_n, ord(\alpha) = d} (X - \alpha) = \prod_{d|n} \Phi_d(X)$.

2. Follows directly by *1* and Möbius formula.

3. Follows directly by *2*: $\Phi_n(X)$ is a unitary polynomial which is the quotient of two unitary polynomials over $\mathbb{Z}$.

4. Let α be a primitive n^{th} root of unity. Let P be the minimal polynomial of α over $\mathbb{Q}$, A be the set of roots of P, and B be the set of n^{th} primitive roots of unity. It is enough to show that $A = B$.

   Since $\Phi_n \in \mathbb{Z}[X]$ and $\Phi_n(\alpha) = 0$, then P is a factor of Φ_n and $A \subset B$.

   For the other direction, we show first that for every prime number p not dividing n, A is stable by taking p^{th} powers. Suppose it were not the case for some p, and let α be a primitive n^{th} root of unity such that $P(\alpha^p) \neq 0$. Let $Q \in \mathbb{Q}[X]$ be such that $P.Q = X^n - 1$. Since the leading coefficient of P is 1, it is easy to check that $Q \in \mathbb{Z}[X]$.

   $P(\alpha^p) \neq 0$, and $\alpha^p \in \chi_n$, so $Q(\alpha^p) = 0$. Since P is irreducible, then $P(X)$ divides $Q(X^p)$. Let $R \in \mathbb{Z}[X]$ be such that $P(X).R(X) = Q(X^p)$. We reduce modulo p, let P_1, Q_1 and R_1 be the corresponding polynomials. We have the following:

$$P_1(X).R_1(X) = Q_1(X^p) = (Q_1(X))^p.$$

   Therefore, any irreducible factor U of P_1 is a factor of $(Q_1(X))^p$, thus of Q_1 since $\mathbb{F}_p[X]$ is a factorial domain. It follows that the polynomial $X^n - 1 \in \mathbb{F}_p[X]$ has double roots, thus is not prime to its derivative. This can only happen if its derivative is 0 in $\mathbb{F}_p[X]$, i.e. if $p|n$. Contradiction.

   We showed that A is stable under taking p^{th} power, for every prime p not dividing n. By induction, one sees easily that A is stable under taking m^{th} powers for every natural number m such that $gcd(m, n) = 1$. Since $\alpha \in A$, then all the other primitive roots of unity are in A, so $B \subset A$.

□

Example.

$$\begin{aligned}\Phi_{30}(X) &= \frac{(X^{30}-1)(X^5-1)(X^3-1)(X^2-1)}{(X^{15}-1)(X^{10}-1)(X^6-1)(X-1)} \\ &= \frac{(X^{15}+1)(X+1)}{(X^5+1)(X^3+1)} \\ &= X^8 + X^7 - X^5 - X^4 - X^3 + X + 1.\end{aligned}$$

Corollary 8.9. *Let $n > 1$ and α be a primitive n^{th} root of unity. Then*

$$Gal(\mathbb{Q}(\alpha)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

Proof. We saw in Section 6.3 that $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Proposition 8.8 shows that the degree of α over $\mathbb{Q}$ is equal to the degree of Φ_n, namely $\varphi(n)$. On the other hand, the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$. The statement follows. □

8.3 Constructible numbers

8.3.1 A Characterization of constructible numbers

We showed that $a \in \mathbb{C}$ is constructible with straightedge and compass if and only if there is a tower of subfields of $\mathbb{C}$:

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_n$$

such that $a \in K_n$, and for any $0 < i \leq n$, K_i is generated by $\sqrt{a_i}$ over K_{i-1}, for some $a_i \in K_{i-1}$. So in particular, if a is constructible, then the degree of a over $\mathbb{Q}$ is of the form 2^r for some $r \in \mathbb{N}$. Now we show a partial converse.

Theorem 8.10. *Let $a \in \mathbb{C}$. If a is contained in a Galois extension L of $\mathbb{Q}$ of degree 2^r for some $r \in \mathbb{N}$, then a is constructible.*

Proof. The extension $L/\mathbb{Q}$ is Galois, and has degree 2^r. So $Gal(L/\mathbb{Q})$ is a 2-group of order 2^r. By Proposition 10.4, there is a sequence of subgroups of $Gal(L/\mathbb{Q})$,

$$G_0 = Gal(L/\mathbb{Q}) \supset G_1 \supset \cdots \supset G_r = \{1\}$$

such that ever G_i has index 2 in G_{i-1}. For every i, let $F_i := Fix(G_i)$. So by Theorem 7.2 we have a tower of subfields of $\mathbb{C}$

$$F_0 = \mathbb{Q} \subset F_1 \subset \cdots \subset F_r = L.$$

Furthermore, $[F_i : F_{i-1}] = 2$, so F_i is generated by $\sqrt{a_i}$ over F_{i-1}, for some $a_i \in F_{i-1}$. Thus a is constructible. □

Lemma 8.11. *Let $n > 1$ be a natural number having an odd factor $a > 1$. Then $2^n + 1$ is not prime.*

Proof. Write $n = ab$. The number a is odd, so $(-1)^a + 1 = 0$. Thus the polynomial $X^a + 1$ is divisible by $X + 1$. Applying this fact for $X = 2^b$, it follows that $2^n + 1 = (2^b)^a + 1$ is divisible by $2^b + 1$. Thus $2^n + 1$ is not prime. □

Definition 8.12. A ***Fermat prime*** F_n is a prime number of the form $2^{2^n} + 1$.

This terminology is due to the fact that Fermat conjectured that all the F_n are prime numbers. In fact, the first five members of the list, namely $3, 5, 17, 257, 65537$, are all prime. Euler showed that $F_5 = 4294967297$ is divisible by 641. It is an open question whether there are prime numbers of the form F_k with $k > 4$, or whether there are infinitely many Fermat primes.

Theorem 8.13. *The regular n-gon is constructible if and only if $n = 2^r.p_1.\cdots.p_k$, where the p_i are distinct Fermat primes.*

Proof. Let n be such that the regular n-gon is constructible. Write $n = 2^r.p_1^{r_1}.\cdots.p_k^{r_k}$ where the p_i are distinct odd primes and $r_i \geq 1$. We show that for every i, $r_i = 1$ and p_i is a Fermat Prime.

The degree of $e^{2i\pi/n}$ over $\mathbb{Q}$ is of the form 2^m for some $m \in \mathbb{N} \setminus \{0\}$. It follows by Proposition 8.8 that the degree of $e^{2i\pi/n}$ over $\mathbb{Q}$ is $\varphi(n)$. Proposition 8.4 yields that $\varphi(n)$

is divisible by $p_i^{r_i-1}$, thus $r_i = 1$ for every i. Furthermore, by multiplicativity, $\varphi(p_i)$ is a power of 2 for all i. The fact that the p_i are Fermat primes follows by Lemma 8.11.

The converse follows by Theorem 8.10. □

Example. The regular 7-gon, 9-gon, 25-gon are not constructible. The regular pentagon, 17-gon, 65537-gon are constructible

8.3.2 Fifth roots of unity

We showed that the fifth roots of unity are constructible. Now we will calculate them explicitely. The expressions we will find involve only the basic arithmetic operations and extracting squareroots. This yields an explicit method for constructing the regular pentagon.

Let α be a primitive 5^{th} root of unity. The minimal polynomial of α is the fifth cyclotomic polynomial

$$\Phi_5(X) = 1 + X + X^2 + X^3 + X^4,$$

the other roots being α^2, α^3 and α^4. Denote by G the galois group of $\mathbb{Q}(\alpha)/\mathbb{Q}$. The group G is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic of order 4, thus isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

An element σ of G is determined by the image of α. We look first for a generator σ of G, which comes to the same as finding a generator of the group $(\mathbb{Z}/5\mathbb{Z})^\times$. It is clear that 2 is such a generator, since the successive powers of 2 in $\mathbb{Z}/5\mathbb{Z}$ are $(2, 4, 3, 1)$. So the element $\sigma \in G$ determined by $\sigma(\alpha) = \alpha^2$ is a generator of G, the sequence of succesive images of α by σ being $(\alpha^2, \alpha^4, \alpha^3, \alpha)$.

The group G has one proper intermediate subgroup: $\{id, \sigma^2\}$. So by Theorem 7.2, the extension $\mathbb{Q}(\alpha)/Q$, which is Galois, admits exactly one proper intermediate field F. Furthermore, F has degree two over $\mathbb{Q}$, so F is generated over $\mathbb{Q}$ by any element of $Fix(\{id, \sigma^2\}) \setminus Fix(G)$, thus any element of $\mathbb{Q}(\alpha)$ fixed by σ^2 but not by σ. An easy choice is

$$\lambda_1 := \alpha + \sigma^2(\alpha) = \alpha + \alpha^4.$$

The element λ_1 has degree two over $\mathbb{Q}$, it has thus exactly one conjugate λ_2 by G.

$$\lambda_2 = \sigma(\lambda_1) = \sigma(\alpha) + \sigma(\alpha^4) = \alpha^2 + \alpha^3.$$

A direct calculation gives

$$\lambda_1 + \lambda_2 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = -1,$$

and

$$\lambda_1\lambda_2 = (\alpha + \alpha^4)(\alpha^2 + \alpha^3) = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = -1.$$

λ_1 and λ_2 are thus the roots $(-1-\sqrt{5})/2$ and $(-1+\sqrt{5})/2$ of the polynomial $X^2 + X - 1$. This shows in particular that $F = \mathbb{Q}(\sqrt{5})$.

Now α has zwei conjugates over F: α and $\sigma^2(\alpha)$. The sum $\alpha + \sigma^2(\alpha) = \lambda_1$, and the product $\alpha.\sigma^2(\alpha) = 1$. Thus α is a root of the polynomial

$$X^2 - \lambda_1 X + 1.$$

So

$$\alpha = \frac{\lambda_1 - \sqrt{\lambda_1^2 - 4}}{2}.$$

8.3.3 Seventh roots of unity

The seventh cyclotomic polynomial is

$$\Phi_7(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6.$$

Let ω be any primitive seventh root of unity. Then the other primitive roots are $\omega^2, \omega^3, \omega^4$, ω^5 and ω^6. Denote by G the Galois group of $\mathbb{Q}(\omega)/\mathbb{Q}$. So G is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^\times$ which is a cyclic group of order 6. The group G is thus isomorphic to $(\mathbb{Z}/6\mathbb{Z}, +)$. The element 3 is a generator of $(\mathbb{Z}/7\mathbb{Z})^\times$, and the powers of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$ are $(3, 2, 6, 4, 5, 1)$. Denote by σ the element of G such that $\sigma(\omega) = \omega^3$. Then σ is a generator of G, $G = \{id, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$.

The unique subgroup of order 3 of G is the group $H = \{id, \sigma^2, \sigma^4\}$, and it is the galois group of an intermediate field K which is an extension of degree 2 of $\mathbb{Q}$. So K is generated by any element fixed by H but not by G, for example the element

$$\alpha := \omega + \sigma^2(\omega) + \sigma^4(\omega) = \omega + \omega^2 + \omega^4.$$

Note that $\alpha \notin \mathbb{Q}$, since this would contradict the irreducibility of Φ_7. Furthermore, α admits exactly one conjugate over $\mathbb{Q}$, namely

$$\sigma(\alpha) := \omega^3 + \omega^6 + \omega^5 = -1 - \alpha.$$

A direct calculation shows that $\alpha.\sigma(\alpha) = 2$. So α and $\sigma(\alpha)$ are the roots of the polynomial

$$X^2 + X + 2,$$

say $\alpha = \frac{-1+\sqrt{-7}}{2}$. We showed in particular that the unique intermediate field of dimension 2 over $\mathbb{Q}$ is $\mathbb{Q}(i\sqrt{7})$.

The Galois group of $\mathbb{Q}(\omega)/\mathbb{Q}(\alpha)$ is H, thus $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)]$ and $\mathbb{Q}(\omega)$ is generated over $\mathbb{Q}(\alpha)$ by any element which is not fixed by H. We will choose an element which is a third root over $\mathbb{Q}(\alpha, j)$. Let

$$\beta = \omega + j\omega^2 + j^2\omega^4.$$

The conjugates of β by H are $\beta, j\beta$ and $j^2\beta$, this shows that $\beta^3 \in \mathbb{Q}(j, i\sqrt{7})$. A direct calculation gives

$$\begin{aligned}
\beta^3 &= 6 + (1 + 3j^2)(\omega^3 + \omega^5 + \omega^6) + 3j(\omega + \omega^2 + \omega^4) \\
&= 6 + \sigma(\alpha) + 3(j\alpha + j^2\sigma(\alpha)) \\
&= 7 - \frac{3}{2}\sqrt{21} - \frac{\sqrt{-7}}{2}.
\end{aligned}$$

This shows in particular that the seventh cyclotomic is contained in the extension

$$\mathbb{Q}\left(j, \sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{\sqrt{-7}}{2}}\right).$$

We calculate the roots explicitely. Let

$$\gamma := \omega + j^2\omega^2 + j\omega^4.$$

It is easy to check that $\beta.\gamma = \alpha - \sigma(\alpha) = \sqrt{-7}$. Now we have

$$\begin{aligned} \omega + \omega^2 + \omega^4 &= \alpha \\ \omega + j\omega^2 + j^2\omega^4 &= \beta \\ \omega + j^2\omega^2 + j\omega^4 &= \gamma. \end{aligned}$$

So

$$\begin{aligned} \omega &= \frac{1}{3}\left(\frac{-1+\sqrt{-7}}{2} + \beta + \frac{\sqrt{-7}}{\beta}\right) \\ &= \frac{1}{3}\left(\frac{-1+\sqrt{-7}}{2} + \sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{\sqrt{-7}}{2}} + \frac{\sqrt{-7}}{\sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{\sqrt{-7}}{2}}}\right). \end{aligned}$$

8.3.4 Seventeenth roots of unity and the construction of the regular heptadecagon

The seventeenth cyclotomic polynomial is

$$\Phi_{17}(X) = 1 + X + X^2 + \cdots + X^{16},$$

has degree $16 = 2^4$. So, as mentioned above, the seventeenth roots of unity are constructible. Let ω be any primitive seventh root of unity. Then the other primitive roots are the $\omega^i, 1 \leq i \leq 16$. Denote by G the Galois group of $\mathbb{Q}(\omega)/\mathbb{Q}$. So G is isomorphic to $(\mathbb{Z}/17\mathbb{Z})^\times$ which is a cyclic group of order 16. The group G is thus isomorphic to $(\mathbb{Z}/16\mathbb{Z}, +)$. The element 3 is a generator of $(\mathbb{Z}/17\mathbb{Z})^\times$, and the powers of 3 in $(\mathbb{Z}/17\mathbb{Z})^\times$ are

$$(3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1).$$

Denote by σ the element of G such that $\sigma(\omega) = \omega^3$. Then σ is a generator of G,

$$G = \{\sigma^i : 1 \leq i \leq 16\}.$$

Denote by $[\sigma^i]$ the subgroup of G generated by σ^i. To the decreasing chain of subgroups

$$G = [\sigma] \supset [\sigma^2] \supset [\sigma^4] \supset [\sigma^8] \supset [\sigma^{16}] = \{id\}$$

corresponds a tower of fields, each field being a quadratic extension of the previous one:

$$\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset K_4 = \mathbb{Q}(\omega).$$

The field K_1 is generated over $\mathbb{Q}$ by any element of $\mathbb{Q}(\omega)$ fixed by σ^2 but not by σ, as for instance the element

$$x_1 := \sum_{i=1}^{8} \sigma^{2i}(\omega) = \sum_{i=1}^{8} \omega^{3^{2i}} = \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2 + \omega.$$

Let $\theta := 2\pi/17$. So

$$x_1 = 2\big(\cos\,\theta + \cos\,2\theta + \cos\,4\theta + \cos\,8\theta\big).$$

The unique conjugate of x_1 over $\mathbb{Q}$ is

$$x_2 := \sigma(x_1) = \sum_{i=1}^{8} \omega^{3^{2i+1}} = 2\big(\cos\,3\theta + \cos\,5\theta + \cos\,6\theta + \cos\,7\theta\big).$$

A direct calculation yields $x_1 + x_2 = -1$ and $x_1x_2 = -4$, thus x_1, x_2 are the roots of the polynomial

$$X^2 + X - 4,$$

so $K_1 = \mathbb{Q}(\sqrt{17})$, $x_1 = \frac{-1+\sqrt{17}}{2}$ and $x_2 = \frac{-1-\sqrt{17}}{2}$.

Now we determine K_2. The field K_2 is generated over K_1 by any element of $\mathbb{Q}(\omega)$ fixed by σ^4 but not by σ^2. a candidate is

$$y_1 = \omega + \sigma^4(\omega) + \sigma^8(\omega) + \sigma^{12}(\omega) = \omega + \omega^4 + \omega^{13} + \omega^{16} = 2(\cos\,\theta + \cos\,4\theta).$$

The unique conjugate of y_1 over K_1 is

$$y_2 := \sigma^2(y_1) = \sigma^2(\omega) + \sigma^6(\omega) + \sigma^{10}(\omega) + \sigma^{14}(\omega) = \omega^2 + \omega^8 + \omega^9 + \omega^{15}.$$

We have: $y_1 + y_2 = x_1$ and $y_1 y_2 = -1$, thus y_1, y_2 are the roots of the polynomial

$$X^2 - x_1 X - 1,$$

so $K_2 = K_1(\sqrt{x_1^2+4}) = \mathbb{Q}(\sqrt{2(17-\sqrt{17})})$, $y_1 = \frac{x_1+\sqrt{x_1^2+4}}{2}$ and $y_2 = \frac{x_1-\sqrt{x_1^2+4}}{2}$.

The same method is used for determining the field K_3, generated over K_2 by any element of $\mathbb{Q}(\omega)$ fixed by σ^8 but not by σ^4. We choose the element

$$z_1 := \omega + \sigma^8(\omega) = \omega + \omega^{16} = 2cos\theta.$$

The unique conjugate of z_1 over K_2 is the element

$$z_2 := \sigma^4(z_1) = \sigma^4(\omega) + \sigma^{12}(\omega) = \omega^4 + \omega^{13}.$$

$z_1 + z_2 = y_1$ and $z_1 z_2 = \omega^3 + \omega^5 + \omega^{12} + \omega^{14}$. Note that $z_1 z_2$ can be calculated from x_2 the same way y_1 is calculated from x_1. Thus

$$z_1 z_2 = \frac{x_2 + \sqrt{x_2^2+4}}{2} = -\frac{1+\sqrt{17}}{4} + \frac{1}{2}\sqrt{\frac{17+\sqrt{17}}{2}} =: \alpha.$$

Therefore, z_1, z_2 are the zeros of the polynomial

$$X^2 - y_1 X + \alpha,$$

and $K_3 = K_2(\sqrt{y_1^2 - 4\alpha})$. Now

$$cos\left(\frac{2\pi}{17}\right) = \frac{z_1}{2} = \frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}}}{16}.$$

In order to compute $\mathbb{Q}(\omega)$, one can proceed as above, or just note that

$$\omega = cos\ \theta + i.sin\ \theta = cos\ \theta + i\sqrt{1 - cos^2\ \theta}.$$

These computations give an explicit way for constructing the regular 17-gon with compass and straightedge, since we see that only square roots are involved in the formulas.

8.4 Solvability by Radicals

8.4.1 The Galois characterization of solvable polynomials

All the fields of this section have characteristic 0.

Definition 8.14. Let K be a field and $P \in K[X]$. The polynomial P is said to be ***solvable by radicals*** if there exists a field L in which P splits in linear factors, and a tower of subfields of L:

$$K_0 = K \subset K_1 \subset \cdots \subset K_n = L$$

such that for any $1 \leq i \leq n$, K_i is of the form $K_{i-1}(\sqrt[n_i]{a_i})$, for some $a_i \in K_{i-1}$ and $n_i \in \mathbb{N}^*$.

Theorem 8.15. *Let K be a field of characteristic 0 and $P \in K[X]$ be a solvable polynomial. Then the Galois group G_P of P is solvable.*

Proof. By Proposition 10.9 , it suffices to show that G_P is a quotient of a solvable group by a normal subgroup. Let

$$K_0 = K \subset K_1 \subset \cdots \subset K_n$$

be a tower of fields such that K_n contains all the roots of P, and for every $1 \leq i \leq n$, K_i is of the form $K_{i-1}(\sqrt[n_i]{a_i})$, for some $a_i \in K_{i-1}$ and $n_i \in \mathbb{N}^*$. Set $m := \prod n_i$, and let α be a primitive m^{th} root of unity. Let M be a finite Galois extension of K containing $K_n(\alpha)$ - define M for instance as the splitting field over K of the minimal polynomial of a primitive element of $K_n(\alpha)/K$. Let L be in M the Galois closure of $K_n(\alpha)$ over K. Thus L/K is a finite Galois extension containing all the roots of P, so by Theorem 7.2, G_P is a quotient of $Gal(L/K)$. It is then sufficient to show that $Gal(L/K)$ is solvable.

It is easy to see that L is the smallest subfield of M containing all the $\sigma\big(K_n(\alpha)\big)$ for $\sigma \in Gal(M/K)$, so L is generated over K by α and all the $\sigma(\sqrt[n_i]{a_i})$ for $\sigma \in Gal(M/K)$ and $i \leq n$. We adjoin these elements one by one to K and to obtain a finite sequence of subfields:

$$K \subset K(\alpha) \subset K(\alpha, \sqrt[n_1]{a_1}) \subset K(\alpha, \sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}) \subset \cdots \subset K_n(\alpha) \subset K_n(\alpha, \sigma(\sqrt[n_1]{a_1})) \subset \cdots$$

where each field E' is generated over its predecessor E by an m^{th} root of unity for the first one, and by some n_i^{th} root for the rest, and E contains the n_i^{th} roots of unity. Therefore, E'/E is Galois, and by Section 6.3, $Gal(E'/E)$ is abelian. The corresponding sequence

$$G = Gal(L/K) \supset Gal(L/K(\alpha)) \supset Gal(L/K(\alpha, \sqrt[n_1]{a_1})) \supset \cdots \supset Gal(L/L) = \{id\}$$

is then a composition series for $Gal(L/K)$, and the quotient of $Gal(L/E)$ by its successor $Gal(L/E')$ is by Theorem 7.2 isomorphic to the abelian group $Gal(E'/E)$. This shows that $Gal(L/K)$ is solvable. $\square$

Now we prove a converse to Theorem 8.15. We start by a particular case.

Definition 8.16. An extension L/K is said to be ***cyclic*** if $Gal(L/K)$ is cyclic.

Proposition 8.17. *Let p be a prime number, K be a field containing a primitive p^{th} root of unity, and L/K be a cyclic Galois extension of order p. Then $L = K(\sqrt[p]{a})$ for some $a \in K$.*

Proof. The extension L/K is finite and Galois, thus normal and separable. Let x_0 be a primitive element of L/K (in fact any element of $L \setminus K$ is primitive) and $P \in K[X]$ be the minimal polynomial of x_0 over K. Then the degree of P is p, and by separability, P has p distinct roots $x_0, \cdots, x_{p-1}$ all of which are in L by normality.

The group $Gal(L/K)$ is cyclic and has order p, it is thus generated by a permutation σ of order p of the x_i. The order of a product of disjoint cycles is the least common multiple of the lengths of these cycles. So since p is prime, σ is a cycle of length p, and without loss of generality we can assume that $\sigma = (x_0, x_1, \cdots, x_{p-1})$.

Let $\alpha \in K$ be a primitive p^{th} root of unity, and let

$$x := x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{p-1} x_{p-1}.$$

For all $i \leq p$, $\sigma^i(x) = \alpha^{-i}x$. So

$$\sigma^i(x^p) = (\sigma^i(x))^p = (\alpha^{-i}x)^p = \alpha^{-pi}x^p = x^p.$$

Since σ generates $Gal(L/K)$, then $x^p \in Fix(Gal(L/K)) = K$, and x is a p^{th} root on K. It remains to show that x can be chosen to be a primitive element of the extension L/K. Since $[L : K]$ is prime, it suffices to show that x can be chosen in $L \setminus K$.

If $x \in K$, then $x = \sigma(x) = \alpha^{-1}x$, thus $x = 0$.

For $i = 0, \cdots, p-1$, denote by

$$x(\alpha^i) := x_0 + \alpha^i x_1 + (\alpha^i)^2 x_2 + \cdots + (\alpha^i)^{p-1} x_{p-1}.$$

It suffices then to show that for some $i = 1, \cdots, p-1$, $x(\alpha^i) \neq 0$. If this were not the case, then we have

$$x(1) = x(1) + \sum_{i=1}^{p-1} x(\alpha^i) = px_0 + \sum_{i=1}^{p-1}\left(x_i \sum_{j=0}^{p-1} \alpha^{ij}\right) = px_0 + \sum_{i=1}^{p-1} x_i.0 = px_0.$$

Since $x(1) = \sum x_i \in K$, then $x_0 \in K$ and this contradicts the choice of x_0 as a primitive element of L/K. □

Theorem 8.18. *Let K be a field of characteristic 0, and $P \in K[X]$ be such that the Galois group G_P of P is solvable. Then P is solvable.*

Proof. Let n be the order of G_P and α be a primitive n^{th} root of unity. The Galois group G of P over $K(\alpha)$ is a subgroup of G_P, thus it is solvable. Let

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_q = \{1\}$$

be a composition series for G such that for G_i/G_{i+1} is cyclic of prime order p_i, for every $i \leq q-1$. Let $K_i = Fix(G_i)$. We have then a tower of subfields

$$K_0 = K(\alpha) \subset K_1 \subset K_2 \subset \cdots \subset K_q,$$

where K_q is the splitting field of P over $K(\alpha)$. The extension K_q/K_0 is Galois, so Theorem 7.2 applies. For all $i < q$, G_{i+1} is a normal subgroup of G_i, so K_{i+1} is a normal extension of K_i. Furthermore,

$$Gal(K_{i+1}/K_i) \simeq G_i/G_{i+1},$$

which is a cyclic group of prime order p_i, and p_i divides n. So K_i contains a primitive p_i^{th} root of unity, and Proposition 8.17 applies. Therefore, for every $i \leq q-1$, $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ for some $a_i \in K_i$, thus P is solvable. □

We have showed the following.

Theorem 8.19. *Let K be a field of characteristic 0, and $P \in K[X]$. Then P is solvable if and only if its Galois group is solvable.*

8.4.2 Examples of non-solvable polynomials

Theorem 8.20 (Abel-Ruffini)**.** *Let K be a field of characteristic 0 and $n \geq 5$. Then the general polynomial of degree n on K is not solvable.*

Proof. Let $x_1, \cdots, x_n$ be distinct indeterminates and $s_1, \cdots, s_n$ be their elementary symmetric polynomials. The general polynomial of degree n is (by definition) the polynomial $P_n(X) \in K(s_1, \cdots, s_n)$ defined by

$$P_n(X) := X^n - s_1 X^{n-1} + s_2 X^{n-2} + \cdots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n,$$

and the Galois group of P_n is the symmetric group S_n. For $n \geq 5$, S_n is not solvable, so by Theorem 8.15, the polynomial P_n is not solvable. □

Proposition 8.21. *Let K be a subfield of $\mathbb{R}$, and let $P \in K[X]$ be an irreducible polynomial of prime degree $p \geq 5$. Suppose moreover that P has exactly two non-real roots. Then P is not solvable.*

Proof. For this we show that the Galois group G of P is S_p, and by Lemma 10.11, it suffices to show that G contains a cycle of length p and a transposition.

Since P is irreducible and has order p, then the order of G is divisible by p, thus G contains a permutation σ of order p. Since p is prime, then σ is a cycle of length p. As for the transposition, note that the complex conjugation is an $\mathbb{R}$-automorphism, so a fortiori a K-automorphism, exchanging the two non-real roots of P and fixing the others. Thus G contains the transposition which exchanges the two non-real roots of P and fixes the others. □

Example. The polynomial $P = X^5 - 4X + 2 \in \mathbb{Q}[X]$ is not solvable.

In order to see this, note first that by Eisenstein's criterion, P is irreducible. Furthermore, the derivative P' of P is $5X^4 - 4$, so P' changes sign twice on $\mathbb{R}$. Now $P(0)$ and $P(2)$ are positive, $P(-2)$ and $P(1)$ are negative, so P has three real and two complex non-real roots. The non solvability of P follows by Proposition 8.21.

Theorem 8.22. *[Galois] Let K be a field of characteristic 0 and $P \in K[X]$ be an irreducible polynomial of prime degree p. Then P is solvable if and only if all its roots are rational functions of any two them.*

Proof. Denote by L the splitting field of P over K, and by G the group $Gal(L/K)$. The group G is regarded as a permutation group on the set S of roots of P. Since P is irreducible, then G is transitive in its action on S. Note that $|S| = p$.

Suppose first that P is solvable, and let x and y be any two distinct roots of P. We want to show that $L = K(x, y)$. By Theorem 8.19, the group $Gal(L/K)$ is solvable. From Exercise 10.12 it follows that $Gal(L/K(x, y)) = \{id\}$. Therefore $K(x, y) = L$ by Theorem 7.2.

Suppose now that $L = K(x, y)$ for any two distinct roots x, y of P. So the unique permutation of G fixing two elements of S is the identity. Exercise 10.12 yields that G is solvable. By Theorem 8.19, the polynomial P is solvable. □

Corollary 8.23. *[Galois] Let K be a subfield of $\mathbb{R}$ and $P \in K[X]$ be irreducible of prime degree. Furthermore, we assume that P has at least two real roots, and at least one non-real root. Then P is not solvable.*

Proof. Let x, y be distinct real roots and z be a non-real root of P. Since $K \subset \mathbb{R}$, then $z \notin K(x, y)$. By Theorem 8.22, P is not solvable. □

Example. The polynomial $X^{11} - 6X + 3$ is not solvable.

8.4.3 Cubic equations revisited

We saw the Cardano formulas expressing the roots of a cubic polynomial $P = X^3 + pX + q$ involve non-real radicals, even in the case where all the roots are real. We show now that if P is irreducible, then such radicals cannot be avoided in a formula expressing the roots.

Notation: For a field F and a polynomial $P \in F[X]$, we denote by $G(F)$ the Galois group of P over F.

Proposition 8.24. *Let $K \subset \mathbb{R}$ be a field, and $P \in K[X]$ be irreducible of odd degree n. Assume that the splitting field L of P is generated by one of the roots. Let p be a prime number, c be an element of K, and $\sqrt[p]{c}$ be the real p^{th} root of c. Then the Galois group of P is not reduced by the addition of $\sqrt[p]{c}$, (i.e. $G(K) \simeq G(K(\sqrt[p]{c}))$).*

Proof. Since P is irreducible and L is generated by one root, then L is generated by any root. The polynomial P has odd degree, so it has a real root x_1. Therefore $L = K(x_1)$ is a real field. Suppose, towards a contradiction, that

$$|G(K(\sqrt[p]{c}))| < |G(K)|.$$

From this it follows that

$$[K(\sqrt[p]{c}, x_1) : K(\sqrt[p]{c})] < [K(x_1) : K].$$

Since K is a real field and $\sqrt[p]{c} \notin K$, then the polynomial $X^p - c$ is irreducible on K, and $[K(\sqrt[p]{c}) : K] = p$. Now we have the following.

$$[K(x_1, \sqrt[p]{c}) : K] = [K(x_1, \sqrt[p]{c}) : K(\sqrt[p]{c})].p = [K(x_1, \sqrt[p]{c}) : K(x_1)].[K(x_1) : K],$$

so $[K(x_1, \sqrt[p]{c}) : K(x_1)] < p$. Since p is a prime, it is easy to check that $\sqrt[p]{c} \in K(x_1)$. But the extension $K(x_1)/K$ is Galois, since it contains $\sqrt[p]{c}$, it has to contain all its complex conjugates. Contradiction.

□

To prove our statement on the cubic equations, apply Proposition 8.24 for an irreducible cubic polynomial $P \in \mathbb{R}[X]$ having only real roots (in which case the discriminant $-4p^3 - 27q^2$ is positive). Take for K the field generated by the coefficients of P and a square root d of the discriminant. By Section 6.1, the splitting field of P is generated on K by any one of the roots. The claim follows directly.

9 Infinite Galois theory

9.1 Topological groups

Definition 9.1. A set G endowed with a group structure and a topology is said to be a ***topological group*** if the maps

$$(g, h) \mapsto g.h$$

and

$$g \mapsto g^{-1}$$

are continuous.

If G is a topological group and $a \in G$, then the maps $x \mapsto a.x$, $x \mapsto x.a$, $x \mapsto a^{-1}.x$ and $x \mapsto x.a^{-1}$ are continuous, for they are compositions of continuous maps. From this it follows that if H is a subgroup of G, then the cosets of H are open (respectively closed) if H is open (respectively closed). Since $G \setminus H$ is a union of such cosets, then H is clopen if it is open, or closed of finite index.

Proposition 9.2. *Let G be a topological group and $\mathcal{V}$ be a neighbourhood base for the identity element e of G. Then we have the following.*

1. *For all $V_1, V_2 \in \mathcal{V}$, there is $V' \in \mathcal{V}$ such that $e \in V' \subset V_1 \cap V_2$.*
2. *For all $V \in \mathcal{V}$, there exists a $V' \in \mathcal{V}$ such that $V'V' \subset V$.*
3. *For all $V \in \mathcal{V}$, there exists a $V' \in \mathcal{V}$ such that $V' \subset V^{-1}$.*
4. *For all $V \in \mathcal{V}$ and all $g \in G$, there exists a $V' \in \mathcal{V}$ such that $V' \subset g^{-1}Vg$.*
5. *For all $g \in G$, the set $\{g.V : V \in \mathcal{V}\}$ is a neighbourhood base for g.*

Conversely, if $\mathcal{V}$ is a nonempty family of subgroups of G satisfying the properties $1, 4$, then there is a unique topology on G for which 5 holds. For this topology, all the $V \in \mathcal{V}$ are open.

Proof. If G is a topological group and $\mathcal{V}$ is an in the statement, then $1, 2, 3, 4$ and 5 are clear. Suppose now that $\mathcal{V}$ is a set of subsets of G satisfying the properties $1 - 4$, and define

$$\mathcal{T} := \{O \subset G : \forall x \in O \exists U \in \mathcal{V}(xU \subset O)\}.$$

The empty set, G, and the union of a family of elements of $\mathcal{T}$ are clearly in $\mathcal{T}$. Furthermore, it follows by 1 that the intersection of two elements of $\mathcal{T}$ is again in $\mathcal{T}$. This shows that $\mathcal{T}$ is a topology on G, and from the definition of $\mathcal{T}$ it follows that the set $\{g.V : V \in \mathcal{V}\}$ is a neighbourhood base for g, for all $g \in G$.

Let abV be a neighbourhood of ab. Let V' be such that $V'V' \subset V$, V_1 be such that $b^{-1}V_1b \subset V'$ and $V_2 = V'$. Then $b^{-1}V_1bV_2 \subset V'V' \subset V$, and $aV_1bV_2 \subset abV$. This shows that the application $(a, b) \mapsto ab$ is continuous.

In order to show that the application $x \mapsto x^{-1}$ is continuous, it suffices to show that for all $a \in G$ and $V \in \mathcal{V}$, there exists $U \in \mathcal{V}$ such that $U^{-1}a^{-1} \subset a^{-1}V$. Fix a^{-1} and V. Let $U' \in \mathcal{V}$ be such that $U' \subset a^{-1}Va$, and let $U \in \mathcal{V}$ be such that $U^{-1} \subset U'$. It is clear then that $U^{-1} \subset a^{-1}Va$, thus $U^{-1}a^{-1} \subset a^{-1}V$. ∎

9.2 The Krull topology on the Galois group

Proposition 9.3. *If L is a normal separable extension of a field K, then L is a normal separable extension of any intermediate field of the extension L/K.*

Proof. Clear. □

Proposition 9.4. *Let K be a field, $S \subset K[X]$ be a set of separable polynomials, and L be a splitting field of S over K (note that the condition on L holds if L/K is any normal separable algebraic extension). Let K_1, K_2 be two intermediate fields, and $\sigma : K_1 \mapsto K_2$ be a K-isomorphism. Then σ extends to a K-automorphism σ' of L.*

Proof. This is an application of Zorn's Lemma. Let

$$X := \{(E, \tau) : K_1 \text{ is a subfield of } E \text{ and } \tau \text{ is an isomorphism extending } \sigma\}.$$

Define and ordering $\leq$ on X in the obvious way. It is easy to check that $(X, \leq)$ is an inductive set, so has by Zorn's lemma a maximal element (E_0, τ_0). We claim that $E_0 = L$ and τ_0 is an automorphism.

If $E_0 \subsetneq L$, let $Q \in S$ be such that there exists $\alpha \in L \setminus E_0$ with $Q(\alpha) = 0$. Let P be the minimal polynomial of α over E_0. Since $\tau_0 P$ is a factor of Q, and since Q splits in linear factors in L, then we can choose a root $\beta \in L$ of the polynomial $\tau_0 P$. By Proposition 5.22, τ_0 extends to an isomorphism $\tau_1 : E_0(\alpha) \to \tau_0(E_0)(\beta)$, contradicting the maximality of τ_0.

Let $a \in L$, P be its minimal polynomial over K, and n be the degree of P. Since L contains exactly n roots of P, the same holds for $\tau_0(L)$. Therefore, a is an element of $\tau_0(L)$, and τ_0 is an automorphism of L. □

Theorem 9.5. *Let L/K be a field extension. Then the following are equivalent:*

1. *The extension L/K is Galois.*
2. *The extension L/K is normal and separable.*
3. *L is the splitting field over K of a set of separable polynomials.*

Proof.

1. $1 \longrightarrow 2$: Let a be an element of L, and let Q be the minimal polynomial of a over K. The image of a by an element of $Gal(L/K)$ is again a root of Q, thus a has finitely many distinct images under the action of $Gal(L/K)$, say $a_1 = a, \cdots, a_p$. Let $P := (x - a_1). \cdots .(x - a_p)$. The polynomial P is separable since all its roots are distinct, and has clearly all its roots in L. Furthermore, P is fixed under the action of $Gal(L/K)$. Since the extension is Galois, then $P \in K[X]$. We showed that every $a \in L$ is a root of a separable polynomial $P \in K[X]$ having all its roots in L. So the extension L/K is normal and separable.
2. $2 \longrightarrow 3$: Clear.
3. $3 \longrightarrow 1$: Let a be an element of $L \setminus K$, and let $A \subset L$ be the splitting field of some separable polynomial over K, with $a \in A$. By Theorem 5.48, the extension A/K is Galois, normal and separable. Let $\sigma_0 \in Gal(A/K)$ be such that $\sigma_0(a) \neq a$. By Proposition 9.4, σ_0 extends to an element $\sigma \in Gal(L/K)$, and it is clear that

$\sigma(a) \neq a$. This shows that $Fix(Gal(L/K)) = K$, thus that the extension L/K is Galois.

□

Proposition 9.6. *Let L/K be a Galois extension, and F be an intermediate field. Then L/F is a Galois extension.*

Proof. Clear by Theorem 9.5. □

Proposition 9.7. *Let L/K be a Galois extension. Then there is a unique topological group structure on $Gal(L/K)$ for which a neighbourhood base of 1 is given by the sets of the form $Gal(L/F)$, where F/K is a finite intermediate extension. For this topology, the sets $Gal(L/F)$ with F/K normal and finite, form a neighbourhood base of 1 consisting of open normal subgroups.*

Proof. Let L/K be a Galois extension. It suffices to show that conditions $1-4$ of Proposition 9.2 hold for

$$\mathcal{V} := \{Gal(L/F) : K \subset F \subset L \ \wedge \ [F:K] < \infty\}.$$

Condition 1 is satisfied because the field generated by two finite dimensional extensions of K is again finite dimensional over K. Conditions 2 and 3 are satisfied since $Gal(L/F)$ is a group. Now let F be a finite intermediate extension, and F' be the normal closure of F in L. It is easy to check that F'/F is a finite Galois extension. Therefore, for all $\tau \in Gal(L/K)$, $\tau Gal(L/F')\tau^{-1} \subset Gal(L/F') \subset Gal(L/F)$, thus $Gal(L/F') \subset \tau^{-1}Gal(L/F)\tau$. This proves 4 and the second statement.

□

Definition 9.8. Let L/K be a Galois extension. Then the ***Krull topology*** on $Gal(L/K)$ is the topology given by Proposition 9.7. Namely, for $\sigma \in Gal(L/K)$, a neighbourhood base of σ is given by the sets of the form

$$\{\sigma.Gal(L/F) : K \subset F \subset L \ \wedge \ [F:K] < \infty\}.$$

From now on, the Galois group of an extension L/K will be considered with its Krull topology.

Proposition 9.9. *Let L/K be a Galois extension, and F/K be an intermediate finite Galois extension. Then the map*

$$\begin{cases} Gal(L/K) & \to Gal(F/K) \\ \quad \sigma & \mapsto \sigma|F \end{cases}$$

is continuous and onto ($Gal(F/K)$ is endowed with the discrete topology).

Proof. Because F/K is normal, the map is well defined. Surjectivity follows by Proposition 9.4, and continuity by the fact the the inverse image of 1, namely $Gal(L/F)$, is an open subset of $Gal(L/K)$. □

Proposition 9.10. *Let L/K be a Galois extension. Then $Gal(L/K)$ is a compact totally disconnected group.*

Proof. We show first that $Gal(L/K)$ is Hausdorff. Let $\sigma \neq \tau \in Gal(L/K)$, and let $a \in L$ be such that $\sigma(a) \neq \tau(a)$. Then $\sigma Gal(L/K(a))$ and $\tau Gal(L/K(a))$ are disjoint neighbourhoods of σ and τ.

For every finite extension F of K, the group $Gal(L/F)$ is open, then it is also closed. The same holds for all the cosets $\sigma Gal(L/F)$ for $\sigma \in Gal(L/K)$. This shows that the group $Gal(L/K)$ has a topology base consisting of clopen set, this group is then totally disconnected. (This is also equivalent to say that the connected components of $Gal(L/K)$ are the singletons.)

Let $\mathcal{F}$ be the set of intermediate fields F such that F/K is finite and Galois. Define the map

$$\varphi := \begin{cases} Gal(L/K) & \to \prod_{F\in\mathcal{F}} Gal(F/K) \\ \sigma & \mapsto (\sigma|F)_{F\in\mathcal{F}} \end{cases}.$$

The group $\prod Gal(F/K)$ is endowed with the product topology. Note that φ is an injective group homomorphism. Let $\mathcal{F}_0 \subset \mathcal{F}$ be finite, and

$$V := \prod_{i\in\mathcal{F}_0} \{a_i\} \times \prod_{F\in\mathcal{F}\setminus\mathcal{F}_0} Gal(F/K)$$

be a basic open neighbourhood of 1 (so all the a_i are 1). Then $\varphi^{-1}(V)$ is $Gal(L/M)$, where M is the finite extension of K generated by the subfields of $\mathcal{F}_0$. This shows that φ is continuous. On the other hand, if $M \in \mathcal{F}$, then

$$\varphi(Gal(L/M)) = \varphi(Gal(L/K)) \cap \left(\{1\} \times \prod_{F\in\mathcal{F}\setminus\{M\}} Gal(F/K)\right).$$

Thus φ defines an homeomorphism between $Gal(L/K)$ and its image. It suffices then to show that $\varphi(Gal(L/K))$ is compact.

For $F \in \mathcal{F}$, the group $Gal(F/K)$ is finite, thus compact. By Tychonoff's theorem, the product $\prod Gal(F/K)$ is compact. In order to show that the group $\varphi(Gal(L/K))$ is compact, it suffices to show that it is closed in $\prod Gal(F/K)$. But the set $\varphi(Gal(L/K))$ is the subset of $\prod Gal(F/K)$ of sequences $(\sigma_F)_F$ such that, if F is a subfield of F', then $\sigma_{F'}|F = \sigma_F$. By Proposition 9.9, the restriction operation is continuous. Therefore $\varphi(Gal(L/K))$ is an intersection of closed sets of $\prod Gal(F/K)$, so it is a closed set. □

9.3 The fundamental theorem of infinite Galois theory

Lemma 9.11. *Let L/K be a Galois extension, H be a subgroup of $Gal(L/K)$, $F \subset L$ be a finite Galois extension of K, and σ be an element of $Gal(L/K)$ be such that*

$$\sigma Gal(L/F) \cap H = \emptyset.$$

Then there is an element of F fixed by H but not by σ.

Proof. Let $H_F := \{h|F : h \in H\}$ $(H_F \subset Gal(F/K))$, and H'_F be the subgroup of $Gal(F/K)$ generated by H_F and $\sigma|F$. The condition on σ and H implies that no element of H coincides with σ on F, thus that $H_F \subsetneq H'_F$. By Theorem 7.1, $Fix(H'_F) \subsetneq Fix(H_F) \subset F$. The claim follows. □

Theorem 9.12. *Let L/K be a Galois extension, and $G := Gal(L/K)$.*

1. *Let F be an intermediate field. Then $Gal(L/F)$ is a closed subgroup of G, and*
$$Fix(Gal(L/F)) = F.$$

2. *Let H be a subgroup of G. Then $Gal(L/Fix(H)) = \bar{H}$, where $\bar{H}$ denotes the closure of H in G for the Krull topology.*

Proof. 1. For every finite extension M/K with $M \subset F$, $Gal(L/M)$ is open, hence it is also closed. So the $Gal(L/F)$ is closed, as it is the intersection of closed sets. The extension L/F is Galois by Proposition 9.6, and the second statement follows immediately.

2. $Gal(L/Fix(H))$ is a closed subgroup of $Gal(L/K)$ containing H, so it contains $\bar{H}$. For the other direction, let $\sigma \in Gal(L/K) \setminus \bar{H}$. It suffices to show that $\sigma \notin Gal(L/Fix(H))$. Let $F \subset L$ be a finite Galois extension of K such that $\sigma Gal(L/F) \cap H = \emptyset$. Then by Lemma 9.11, there is an element $\alpha \in Fix(H)$ with $\sigma(\alpha) \neq \alpha$. The required result follows directly.

□

We state now the fundamental theorem of infinite Galois theory.

Theorem 9.13. *Let L/K be a Galois extension. Let $\mathcal{F}$ be the set of intermediate fields of L/K, and $\mathcal{G}$ be the set of closed subgroups of $Gal(L/K)$.*
Denote by $Fix : \mathcal{G} \longrightarrow \mathcal{F}$ the application which to a subgroup H of $Gal(L/K)$ associates the fixed field of H, and by $G : \mathcal{F} \longrightarrow \mathcal{G}$ the application which to an intermediate field F associates the Galois group $Gal(L/F)$. Then the following hold:

1. *Fix and G define reciprocal bijections, decreasing for the inclusion.*

2. *Fix and G define by restriction reciprocal bijections between the set $\mathcal{F}'$ of normal extensions of K contained in L, and the set $\mathcal{G}'$ of normal subgroups of $Gal(L/K)$.*

3. *If F and F' are two elements of $\mathcal{F}$, then F' is a normal extension of F if and only if $Gal(L/F')$ is a normal subgroup of $Gal(L/F)$. In this case we have*
$$Gal(F'/F) = \frac{Gal(L/F)}{Gal(L/F')}.$$

4. *A closed subgroup H of $Gal(L/K)$ is open if and only if $Fix(H)$ has finite degree over K, in which case $[Fix(H) : K] = (Gal(L/K) : H)$.*

Proof. 1. This is a direct consequence of Theorem 9.12.

2. • Let $F \in \mathcal{F}'$. Then the operation from $Gal(L/K)$ to $Gal(F/K)$, which to every σ associates its restriction to F, is a well defined group homomorphism, and admits $Gal(L/F)$ as its kernel. Hence $G(F) = Gal(L/F)$ is a normal subgroup of $Gal(L/K)$, it is thus an element of $\mathcal{G}'$.

- Let $H \in \mathcal{G}'$, $x \in Fix(H)$, and y be any root of the minimal polynomial of x over K. The aim is to show that $y \in Fix(H)$. By Theorems 5.42 and 9.4, there is $\tau \in Gal(L/K)$ such that $\tau(x) = y$. Let σ be any element of H. Since H is normal, then $\tau^{-1}\sigma\tau \in H$, thus $\tau^{-1}\sigma\tau(x) = x$, and $\sigma\tau(x) = \tau(x)$. This shows that $y = \tau(x) \in Fix(H)$. Therefore, the extension $Fix(H)/K$ is normal, and $Fix(H) \in \mathcal{F}'$.

3. Use the same arguments as the first part of 2 with F replacing K and F' replacing F. Note that if $f : G \to H$ is a group homomorphism, then $G/Ker(f) \simeq Im(f)$.

4. Let H be a subgroup of $Gal(L/K)$. Then $Gal(L/K)$ is the disjoint union of the cosets of H. If H is open, then these cosets are open. Since $Gal(L/K)$ is compact, then there are finitely many such cosets. Thus H has finite index in $Gal(L/K)$. Conversely, we already noted that a closed subgroup of $Gal(L/K)$ of finite index is open.

   Let H be such a group. Then the left cosets of H corresponds to the K-embedding of $Fix(H)$ in L. But the number of K-embedding of $Fix(H)$ in L is equal to the degree of $Fix(H)/K$. Therefore, the index of H in $Gal(L/K)$ is equal to the degree of $Fix(H)/K$.

□

9.4 Galois groups as inverse limits

Definition 9.14. An ordered set $(I, \leq)$ is said to be ***directed*** if for any elements $i, j \in I$, there is some $k \in I$ such that $k \geq i$ and $k \geq j$.

Definition 9.15. Let $(I, \leq)$ be a directed set, and $\mathcal{C}$ be a category.

1. An ***inverse system*** in $\mathcal{C}$ is a family $(A_i)_{i\in I}$ indexed by I together with morphisms $p_{ij} : A_i \to A_j$, for all $i \geq j$, such that $p_{ii} = id_{A_i}$ and for $i \geq j \geq k$, $p_{jk} \circ p_{ij} = p_{ik}$.

2. Let $(A_i)_{i\in I}$ be an inverse system in $\mathcal{C}$. Let A be an object of $\mathcal{C}$, together with a family morphisms $(p_i : A \to A_i)_{i\in I}$. Suppose that for all $i \geq j$, $p_{ij} \circ p_i = p_j$. Then A is said to be an ***inverse limit*** or a ***projective limit*** of the directed system $(A_i)_{i\in I}$ if it has the following universal property: for any object B of $\mathcal{C}$ together with a family morphisms $(q_i : B \to A_i)_{i\in I}$ such that for all $i \geq j$, $p_{ij} \circ q_i = q_j$, then there is a unique morphism $f : B \to A$ such that for every $i \in I$, $p_i \circ f = q_i$.

Remark 9.16. If an inverse limit of a directed system $(A_i)_{i\in I}$ exists, then it is unique up to isomorphism, and will be denoted by $\underset{\longleftarrow}{Lim}\, A_i$.

Remark 9.17. 1. Let $(G_i, p_{ij})_{i\in I}$ be an inverse system of groups, and let G be the subgroup of $\prod_{i\in I} G_i$ of the sequences $(g_i)_i$ such that, for every $i \geq j$, $p_{ij}(g_i) = g_j$. For every element $i \in I$, let $p_i : G \longrightarrow G_i$ be the projection. If $(H, (q_i)_{i\in I})$ is such that for all $i \geq j$, $q_i \circ p_{ij} = q_j$, then there exists a unique group homomorphism $f : H \to G$ such that for every $i \in I$, $p_i \circ f = q_i$: set $f(x) := (q_i(x))_{i\in I}$. Therefore, $(G, (p_i)_{i\in I})$ is the inverse limit of the G_i.

2. Let $(G_i, p_{ij})_{i\in I}$ be an inverse system of topological groups, and let G be as above. The group G is a subset of the topological group $\prod_I G_i$, so we endow G with the subspace topology. The projections $p_i : G \longrightarrow G_i$ are continuous, and if $(H, (q_i)_{i\in I})$ – $q_i : H \longrightarrow G_i$ continuous– is such that for all $i \geq j$, $q_i \circ p_{ij} = q_j$, then as above, $f(x) := (q_i(x))_{i\in I}$ is the unique group homomorphism from H to G such that for every $i \in I$, $p_i \circ f = q_i$. Furthermore, f is continuous. Therefore, $(G, (p_i)_{i\in I})$ is the inverse limit of the G_i.

Definition 9.18. A topological group G is said to be ***profinite*** if it is the inverse limit of a directed system of finite groups, each endowed with the discrete topology.

Proposition 9.19. *Profinite groups are totally disconnected and compact.*

Proof. Let $G := \underleftarrow{Lim}\, G_i \subset \prod_I G_i$, where all the G_i are finite. Then the subgroups of G of the form

$$\big((1)_{i\in I_0} \times \prod_{I\setminus I_0} G_i\big) \cap G,$$

where I_0 is a finite subset of I, is neighbourhood base of 1 consisting of subgroups which are open, thus clopen. This shows that G is totally disconnected. For the compactness, we repeat the same argument as in the the proof of Proposition 9.10. □

Example. Let $\mathcal{G} := \{(\mathbb{Z}/n\mathbb{Z}, +) : n \in \mathbb{N}^*\}$. For any two natural numbers $n, m > 0$ such that $n|m$, we define the group homomorphism p_{mn} as being the natural projection from $(\mathbb{Z}/m\mathbb{Z}, +)$ to $(\mathbb{Z}/n\mathbb{Z}, +)$. It is easy to check that $\mathcal{G}$ is an inverse system. Its inverse limit is denoted by $\hat{\mathbb{Z}}$.

Remark 9.20. Let L/K be a Galois extension, and $\mathcal{F}$ be the set of subfields F of L which are finite Galois extension of K. Let $(\mathcal{G}, \leq)$ be the set of groups of the form $Gal(F/K), F \in \mathcal{F}$, and $\leq$ be defined as follows:

$$Gal(F/K) \leq Gal(F'/K) \iff F \subset F'.$$

The partially ordered set $(\mathcal{G}, \leq)$ is clearly directed. For any two elements $Gal(F/K) \leq Gal(F'/K) \in \mathcal{G}$, we define a group homomorphism from $Gal(F'/K)$ to $Gal(F/K)$, which to an element of the first group associates its restriction to F. This operation is well defined since F/K is Galois, and thus $\mathcal{G}$ is an inverse system of finite groups. The inverse limit of $\mathcal{G}$ is isomorphic to $Gal(L/K)$: this has been shown in the course of the proof of Proposition 9.10.

So we have the following:

Theorem 9.21. *Let L/K be a Galois extension. Then $Gal(L/K)$ is a profinite group, for it is the inverse limit of the finite groups $Gal(F/K)$, where $F \subset L$ is a finite Galois extension of K.*

Definition 9.22. Let K be a perfect field, and K^{alg} be the algebraic closure of K. The ***absolute Galois group*** of K is the Galois group of K^{alg} over K.

Example. The absolute Galois group of $\mathbb{R}$ is $\mathbb{Z}/2$, and that of $\mathbb{C}$ is trivial. The absolute Galois group of a perfect field K is trivial, if and only if K is algebraically closed.

Let q be a power of a prime number. We showed in Section 5.2.1 that for every $n > 0$, the field F_{q^n} is the unique field of cardinality q^n, thus F_q has exactly one extension of degree n, and this extension is Galois. Furthermore, the Galois group of F_{q^n}/F_q is cyclic of order n, thus it is $\mathbb{Z}/n\mathbb{Z}$. It is easy to check that F_{q^n} is a subfield of F_{q^m} if and only if $n|m$, in which case the restriction operation from $Gal(F_{q^m}/F_q)$ to $Gal(F_{q^n}/F_q)$ corresponds to the natural projection from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$. So the union (or the direct limit, to be more exact) of all the F_{q^n} is the algebraic closure of F_q, denoted by F_q^{alg}, thus the absolute Galois group of F_q is $\hat{\mathbb{Z}}$.

9.5 Artin-Schreier Theorem

Theorem 9.23. *[Artin-Schreier] Let K be a field of characteristic zero with finite absolute Galois group. Then $K^{alg} = K(\sqrt{-1})$, and the absolute Galois group of K is either $\mathbb{Z}/2$ or $\{1\}$. Furthermore, if $K^{alg} \neq K$, then for every $a \in K \setminus \{0\}$, exactly one of a or $-a$ is a square in K.*

Proof. Let G be the absolute Galois group of K. We show first that the order of G is of the form 2^n, then we prove that n is 0 or 1.

Let p be a prime number dividing $|G|$. The aim is to show that $p = 2$. By the theorems 10.6 and 7.1, there is an intermediate field F of K^{alg}/K such that $[K^{alg} : F] = p$. Note that K^{alg}/F is a Galois extension. Let $\omega \in K^{alg}$ be a primitive p^{th} root of unity. Now ω has degree at most $p-1$ over F, and this degree divides the prime number p, for $p = [K^{alg} : F]$. Therefore, the degree of ω over F is 1, so $\omega \in F$, and it follows Proposition 8.17 that $K^{alg} = F(\sqrt[p]{a})$ for some $a \in F$. Let $b := \sqrt[p]{a}$, $c := \sqrt[p]{b}$, and σ be a generator of $Gal(K^{alg}/F)$. Since $c^{p^2} \in F$, then

$$(\sigma(c))^{p^2} = \sigma(c^{p^2}) = c^{p^2},$$

thus $\sigma(c) = \gamma c$ for some p^2-th root of unity γ. Thus γ^p is a p^{th} root of unity, so it lies in F. Furthermore, since $b \notin F$, then

$$b \neq \sigma(b) = \sigma(c^p) = (\sigma c)^p = \gamma^p c^p = \gamma^p b,$$

so $\gamma^p \neq 1$. It follows directly that γ is a primitive p^2-th root of unity, and that γ^p is a primitive p^{th}- root of unity.

Because $\gamma^p \in F$, then $\gamma^p = \sigma(\gamma^p) = (\sigma(\gamma))^p$, so for some $k \in \mathbb{Z}$,

$$\sigma(\gamma) = \gamma^{1+pk}.$$

Let

$$m := \sum_{j=0,\cdots,p-1} (1+pk)^j.$$

Since $\sigma^p = id$, an easy calculation shows that

$$c = \sigma^p(c) = \gamma^m c,$$

thus $m \equiv 0$ modulo p^2. The binomial formula yields for $j \leq p-1$, that

$$(1+pk)^j \equiv 1 + jpk \text{ modulo } p^2,$$

so

$$0 \equiv m \equiv \sum_{j=0,\cdots,p-1} (1+jpk) \equiv p + \frac{kp^2(p-1)}{2} \text{ modulo } p^2,$$

thus

$$1 + \frac{kp(p-1)}{2} \equiv 0 \text{ modulo } p.$$

This last identity shows that p cannot be odd, so $p = 2$, and that $k \neq 0$ modulo p. Furthermore, since $p = 2$, then $\gamma = \sqrt{-1}$. Thus $\sigma(\sqrt{-1}) \neq \sqrt{-1}$, so $\sqrt{-1} \notin K$.

Suppose now that $|G| = 2^n$ for some $n \geq 2$. Let F be an intermediate field of K^{alg}/K with $[K^{alg} : F] = 4$, and $L \subset K^{alg}$ be an extension of degree two of F. By the same argument as above, $\sqrt{-1} \notin L$, thus $\sqrt{-1} \notin F$. This is yields an immediate contradiction since we can take $L = F(\sqrt{-1})$.

For the second part of the theorem, suppose that for some $a \in K$, neither $\sqrt{a}$ nor $\sqrt{-a}$ are in K. Since $[K^{alg} : K] = 2$, then $K^{alg} = K(\sqrt{a}) = K(\sqrt{-a})$. So there exist elements $x, y \in K$ such that $\sqrt{-a} = x + y\sqrt{a}$. Squaring the to sides of the equality, we get $2xy\sqrt{a} = -a - x^2 - ay^2$. Thus $2xy\sqrt{a} \in K$. Since $\sqrt{a} \notin K$, then $x = 0$ or $y = 0$. The fact $\sqrt{-a}$ is not in K forces y not to be 0. So $x = 0$, and y is equal to $\sqrt{-1}$. Thus $\sqrt{-1} \in K$. Contradiction.
If for some $a \neq 0$, both $\sqrt{a}$ and $\sqrt{-a}$ are in K, then $\sqrt{-1} = \sqrt{-a}/\sqrt{a} \in K$. Contradiction. □

Corollary 9.24. *The field $\mathbb{R}$ admits no proper subfield of which it is a finite extension.*

Proof. If such a subfield K exists, then $\mathbb{C}/K$ is a finite extension with degree strictly greater than 2. This contradicts Theorem 9.23. □

Definition 9.25. A field K is said to be real closed if every polynomial of odd degree on K has a root in K, and for every $a \in K^*$, exactly one of a or $-a$ has a square root in K.

Example. The field $\mathbb{R}$ of the reals is a real closed field.

Let K be a field of characteristic 0 with a non trivial finite absolute Galois group. We showed that for every $a \in K^*$, exactly one of a or $-a$ has a square root in K. Furthermore, we showed that the absolute Galois group of K has order 2, thus $[K^{alg} : K] = 2$. Therefore, an irreducible polynomial of $K[X]$ has degree at most 2. It follows that every polynomial $P \in K[X]$ is the product of polynomials of $K[X]$ of degree 1 or 2. So if $P \in K[X]$ has odd degree, then P has a root in K. This shows that K is a real closed field.

We proved the following theorem.

Theorem 9.26. *Let K be a field of characteristic 0 and finite absolute Galois group. Then K is either algebraically closed, or real closed.*

10 Results from group theory

10.1 Basics

Definition 10.1. Let $(G, .)$ be a group, $a \in G$ and $n \in \mathbb{N} \setminus \{0\}$. We say that the order of a is n if and only if n is the smallest natural number with $a^n = 1$.

Lemma 10.2. *Let $(G, .)$ be a group.*

1. *Let $a \in G$ and $n \in \mathbb{N} \setminus \{0\}$. If $a^n = 1$, then the order of a is defined, and n is a multiple of the order of a.*

2. *If $(G, .)$ is finite of cardinality m, then for any $x \in G$, we have that $x^m = 1$. So if G is finite, every $x \in G$ has an order, and this order divides the cardinality of G.*

3. *For $a \in G$ and $n \in \mathbb{N}\setminus\{0\}$, a has order n if and only if the cardinality of the subgroup of G generated by a is n.*

Proof. □

Lemma 10.3. *Let $(G, .)$ be an abelian group, a, b be elements of G of order $p, q \in \mathbb{N}$, with $p \wedge q = 1$. Then $a.b$ has order $p.q$.*

Proof. Let m be the order of $p.q$. Since G is abelian, it is clear that $(a.b)^{p.q} = 1$. So m divides $p.q$. It is enough to show that $p.q$ divides m. Now since $p \wedge q = 1$, it is enough to show that both p and q divide m. By commutativity and the definition of m have that

$$a^m.b^m = 1.$$

By the definitions of p, q we have that

$$a^p.b^q = 1.$$

Raise the first equation to the power p, the second to the power m, divide the first by the second and use commutativity to get that

$$b^{m.(p-q)} = 1.$$

So by lemma 10.2 we have that q divides $m.(p-q)$. But q is prime to $p-q$ since prime to p. So q divides m. We show in the same way that p divides m. □

Proposition 10.4. *Let p be a prime number, and $n \in \mathbb{N} \setminus \{0\}$. A group of order p^n has subgroups of order p^m for all $m \leq n$.*

Definition 10.5. Let G be a group and p be a prime number. A subgroup H of G is said to be ***a Sylow p-subgroup of*** G if the order of H is the maximal power of p dividing the order of G. Equivalently, H is a Sylow p-subgroup of G if the order of H is a power of p, and the index of H in G is prime to p.

Theorem 10.6. *[Sylow I] Let G be a group, p be a prime and $r \in \mathbb{N}$ be such that p^r divides the order of G. Then there exists a subgroup of G of order p^r.*

Definition 10.7. A ***composition series*** for a group G is a finite sequence of subgroups

$$G \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\},$$

with G_{i+1} normal in G_i for every $1 \leq i \leq n-1$. The group G is said to be ***solvable*** if it has a composition series with each quotient G_i/G_{i+1} abelian.

Example. Every abelian group is solvable.

Proposition 10.8. *A finite group is solvable if and only if it has a composition series satisfying one of the following properties:*

1. G_{i-1}/G_i *is solvable for each* i.
2. G_{i-1}/G_i *is abelian for each* i.
3. G_{i-1}/G_i *is cyclic for each* i.
4. G_{i-1}/G_i *is cyclic of prime order for each* i.

Proof. It is clear that if G is solvable, then G has a composition series as in *1*. Now if G has a composition series as in *1*, then by refining this composition series we have one as in *2*, which in turn can be refined to have *3* and *4* (for *4* use Sylow for example, or just the fact that a simple abelian group is one of the $\mathbb{Z}/p$ for some prime p). It is clear that a group having a composition series as in *4* is solvable. □

Proposition 10.9.

1. *Let G be a solvable group and H be a subgroup of G. Then H is solvable.*
2. *Let G be a solvable group and N be a normal subgroup of G. Then G/N is solvable.*
3. *Let G be a group, and N be a normal subgroup of G. Suppose furthermore that N and G/N are solvable. Then G is solvable.*

Let G be a group and $x, y \in G$. The ***commutator*** $[x, y]$ of x and y is the element $x^{-1}y^{-1}xy$. It is easy to see that x and y commute if and only if $[x, y] = 1$.

The ***first derived subgroup*** of G is the subgroup $[G, G]$ of G generated by the commutators. This group, also denoted by $G^{(1)}$, is a normal subgroup of G. By induction, we define the ***the*** n^{th} ***derived subgroup*** of G by

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}].$$

Let H be any normal subgroup of G. It is easy to check that G/H is abelian if and only if $[G, G] \subset H$. From this it follows that G is solvable if and only if $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}$.

10.2 On the symmetric group

S_n denotes the group of permutations of $\{1, \cdots, n\}$. A permutation of the form (i, j) with $i \neq j$ is called ***transposition***. Every permutation σ is a (not uniquely determined) product of transposition, and the number of transpositions needed to represent σ is either always odd, in which case σ is said to be ***odd***, or always even, in which case σ is said to be ***even***.

Let h be the group homomorphism from G to $(\mathbb{Z}_2, +)$, which to σ associates 0 if σ is even, and 1 if σ is odd. The kernel of h is a normal subgroup of S_n of index 2, it is called the ***alternating group*** A_n.

It is easy to check that A_n is the subgroup generated by the cycles of length three. For this, one checks that the product of two transposition $(i, j)(k, l)$ is (i, j, l) if $j = k$, $(i, j, k)(j, k, l)$ if all i, j, k, l are distinct, and id if $(i, j) = (k, l)$.

The following result is due to Galois.

Proposition 10.10. *The groups A_n and S_n are not solvable for $n \geq 5$.*

Proof. It suffices to show that A_n is not solvable. For this, we show that the commutator subgroup $[A_n, A_n]$ of A_n is equal to A_n. Let (a, b, c) be any cycle of length three, and d, e be distinct of a, b, c. Then

$$[(a, c, d)(b, c, e)] = (a, d, c)(b, e, c)(a, c, d)(b, c, e) = (a, b, c).$$

Any cycle of length three is in $[A_n, A_n]$, so $[A_n, A_n] = A_n$. □

Lemma 10.11. *Let $n \in \mathbb{N}^*$, and S_n be the group of permutations of $\{1, \cdots, n\}$. Then S_n is generated by any cycle of length n together with a transposition.*

Proof. The equalities like

$$(1, 2, \cdots, n)(1, 2)(1, 2, \cdots, n)^{-1} = (2, 3)$$

show that a cycle of length n and a transposition generate all the transpositions, thus all the permutations. □

The results of the following exercise are due to Galois.

Exercise 10.12. Let p be a prime number. Denote by $E = \{0, \cdots, p-1\}$ the elements of the field $\mathbb{Z}/p$ and by S_p the group of permutations of E.
Let $GA(p)$ be the group of affine bijective functions on $\mathbb{Z}/p$, thus the functions f_{ab} defined by $f_{ab}(x) = ax + b$, where $a \neq 0$. Let $t := f_{1,1}$ and $m_a := f_{a,0}$. The aim of this exercise is to show that for any subgroup G of S_p, then G is solvable and transitive iff it is conjugate to a subgroup H of $GA(p)$.

1. (a) Show that $m_a t = t^a m_a$.
   (b) Show that every element of $GA(p)$ can be written in a unique way as a product $t^b m_a$, for some $1 \leq a \leq p-1$, $0 \leq b \leq p-1$. Conclude that $|GA(p)| = p(p-1)$.
   (c) Show that the group $[t]$ generated by t is a normal subgroup of $GA(p)$

(d) Show that $GA(p)$ is a transitive solvable group.

2. Let G be a transitive subgroup of S_p. Prove that every normal non-trivial subgroup H of G is transitive.

3. (a) Let G be a solvable subgroup of S_p acting transitively on E. Let $(H_i)_{0\leq i\leq r}$ be a composition series for G satisfying condition *4* of Proposition 10.8. Show that H_{r-1} is conjugate to the group $[t]$.

   (b) Deduce that G is conjugate to a subgroup of S_p containing t.

4. Let $\sigma \in S_p$ be such that $\sigma t \sigma^{-1} \in GA(p)$. Show that $\sigma \in GA(p)$

5. Show that a transitive solvable subgroup G of S_p is conjugate to a subgroup H of $GA(p)$.

6. Let G be a transitive subgroup of S_p.

   (a) Show that if G is solvable, then the unique element of G fixing at least two points is the identity.

   (b) Show the converse. Hint: show first that if the unique element of G fixing at least two points is the identity, then there is $\tau \in G$ which has no fixed points.

Proof. 1. (a) Clear.

(b) If $f(x) = ax + b$, then $f = t^b m_a$. The rest is clear.

(c) Let $t^b m_a$ be an element of $GA(p)$ and $q \in \mathbb{N}$. Then

$$(t^b m_a)^{-1} t^q t^b m_a = m_a^{-1} t^{q-b+b} m_a = t^{qa^{-1}} \in [t].$$

(d) It is clear that $GA(p)$ is transitive. As for the solvability, $[t]$ is a normal abelian subgroup of $GA(p)$, and the quotient $GA(p)/[t]$ is the group of the elements of the form $m_a, a \neq 0$, which is isomorphic to the multiplicative group of $\mathbb{Z}/p$. So $GA(p)/[t]$ is abelian and $GA(p)$ is solvable.

2. Let $x, y \in E$ and $f \in G$ be such that $f(x) = y$. If $h \in H$, then $f^{-1}hf \in H$. This shows that the orbit $f^{-1}H(y)$ is a subset of the orbit $H(x)$. From this it follows that $|H(y)| \leq |H(x)|$, and by symmetry we get $|H(y)| = |H(x)|$ for all $x, y \in E$. On the other hand, it follows from the fact that $H \neq \{1\}$ that each H-orbit contains at least two elements. Since E is a disjoint union of orbits and $|E|$ is prime, then E consists of one orbit of H, so H is transitive on E.

3. (a) H_{r-1} is a non-trivial normal subgroup of the transitive group G. By what has been proved above, H_{r-1} is transitive on E. Since H_{r-1} is cyclic and transitive, it is then generated by one cycle of length p, and is therefore conjugate to $[t]$.

   (b) Clear.

4. If $\sigma t \sigma^{-1} = t^b m_a$, it is then easy to check for $k \geq 1$, that $\sigma t^k \sigma^{-1} = t^n m_{a^k}$, where $n = \sum_{0\leq i\leq k-1} a^i b$. Let $k = p-1$, and suppose that $a \neq 1$. Then we have $n = 0$ modulo p, so $\sigma t^{p-1}\sigma^{-1} = id$, so $t^{p-1} = id$, contradiction.

   Thus $a = 1$ and $\sigma t \sigma^{-1} = t^b$, and $\sigma t = t^b \sigma$. For $x \in E$, we have then $\sigma(x+1) = \sigma(x) + b$, so $\sigma(x) = b.x + \sigma(0)$ and $\sigma = t^{\sigma(0)} m_b \in GA(p)$.

5. Let $(H_i)_{0\leq i\leq r}$ be a composition series for G satisfying condition *4* of Proposition 10.8. We saw that there exists $\sigma \in S_p$ such that $\sigma H_{r-1}\sigma^{-1} = [t]$. Now $[t] = \sigma H_{r-1}\sigma^{-1}$ is normal in $\sigma H_{r-2}\sigma^{-1}$. So for $\tau \in \sigma H_{r-2}\sigma^{-1}$,

$$\tau^{-1}t\tau \in [t] \subset GA(p),$$

so by *4*, $\tau \in GA(p)$. We showed that $\sigma H_{r-2}\sigma^{-1} \subset GA(p)$. By induction we show that for all i, $\sigma H_i\sigma^{-1} \subset GA(p)$, so $\sigma G\sigma^{-1} \subset GA(p)$.

6. (a) Clear.

   (b) Suppose that no other permutation than id fixes two points of $\mathbb{Z}/p$. Let $A \subset G$ be the set of permutations with no fixed points. For $i \in \mathbb{Z}/p$, let $S(i) \subset G$ be the set of permutations fixing i, and q be the cardinality of $S(0)$.

   By transitivity, $|G| = p|S(i)|$. So all the $S(i)$ have cardinality q, and G has order pq. By the assumptions, the group G is the disjoint union of A, the $S(i) \setminus \{id\}$ and $\{id\}$. Thus

$$pq = |A| + p.(q-1) + 1.$$

   So $|A| = p - 1$, and there is $\tau \in G$ having no fixed points.

   Let n be the order of τ. Then for all $k < n$, $\tau^k \in A$ (if τ^k fixes i, then it fixes $\tau(i)$, thus $\tau^k = id$). This shows that the orbits under the action of τ have all cardinality n. Since p is prime, $\mathbb{Z}/p$ is a disjoint union of orbits and $\tau \neq id$, then $n = p$ and τ is a p-cycle.

   Therefore, G contains an element which is conjugate to t. Up to conjugation, we can suppose that $t \in G$ and that $A = [t]$. Let $\sigma \in G$. Since t has no fixed points, then the same holds for $\sigma t\sigma^{-1}$. So $\sigma t\sigma^{-1} \in [t]$. By *4*, $\sigma \in GA(p)$. Therefore, G is a subgroup of $GA(p)$, so G is solvable.

□

Index