Algebra 2
Notes for the course

Sophie Marques

December 4, 2013

Contents

Introduction

Algebra can essentially be considered as doing computation similar to that of arithmetic with non-numerical mathematical objects.

Initially, these objects represented either numbers that were not yet known (unknowns) or unspecified numbers (indeterminate or parameters) allowing one to state and prove properties that are true no matter which number are involved.

For example, in the quadratic equation

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

a, b, c are indeterminates and x is the unknown. Solving this equation amounts to computing with the variables to express the unknowns in terms of the indeterminates. Then, substituting any numbers for the indeterminates, gives the solution of a particular equation after a simple arithmetic computation.

As it developed, algebra was extended to other non-numerical objects, like vectors, matrices, polynomials.

Then the structural properties of these non-numerical objects were abstracted to define algebraic structures like groups, rings, fields and algebras.

Chapter I

Ring theory

1 Generality around rings

1.1 Definitions and first examples

Definition 1.1.1. *1. A non empty set is said to be a* ***ring*** *if there are in R two operations, denoted by $+$ and $\cdot$ respectively such that:*

(a) R is an abelian group under the operation $+$. That is, for any a, b and $c \in R$

i. $a + b \in R$,

ii. $a + b = b + a$,

iii. $(a + b) + c = a + (b + c)$,

iv. there is an element 0 in R such that $a + 0 = a$, for any $a \in R$,

v. there is an element $-a \in R$ such that $a + (-a) = 0$.

(b) R is closed under an associated operation. That is, for any a, b, $c \in R$,

i. $a.b \in R$,

ii. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(c) The multiplication is distributive under the addition. That is, for any a, b, $c \in R$,

i. $a.(b + c) = a.b + a.c$,

ii. $(b + c) \cdot a = b \cdot a + c \cdot a$.

2. If moreover, there is an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for any $a \in a$, we say that R is ***a ring with unit element****.*

3. If the multiplication of R is such that $a \cdot b = b \cdot a$, for every a, $b \in R$, we say that R is a ***commutative ring****.*

Example 1.1.2. *1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ together with usual addition and multiplication are a commutative ring with unit elements.*

2. $2\mathbb{Z}$ is a commutative ring without unit element.

3. *The set $\mathscr{M}_{2,2}(\mathbb{Q})$ of the square matrices of order 2 over $\mathbb{Q}$ together with the usual addition and multiplication of matrices is a non-commutative ring with unit element.*

From the definition of ring, we obtain the easy following lemma which permits to compute in rings but ⚠BE CAREFUL ab is not necessarily equal to ba and the division might not exists:

Lemma 1.1.3. *If R is a ring then for all $a, b \in R$,*

1. $a \cdot 0 = 0 \cdot a = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

If in addition, R has a unit element then,

4. $(-1)a = -a$,
5. $(-1)(-1) = 1$.

Proof. 1. If $a \in R$, then $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, by distributivity. Then, since $(R,+)$ is a group, $a \cdot 0 = a \cdot 0 - a \cdot 0 = 0$. We can do the same to prove that $0 \cdot a = 0$.

2. To show that $a(-b) = -(ab)$, we have to prove that $ab + a(-b) = 0$. But by the distributivity property,$ab + a(-b) = a(b + (-b)) = a.0 = 0$, by 1..

3., 4. and 5. are special cases of 2.. □

Example 1.1.4. *Compute $(x+y)^2$. We have:*

$$(x+y)^2 = (x+y)\cdot(x+y) = x\cdot(x+y) + y\cdot(x+y) = x\cdot x + x\cdot y + y\cdot x + y\cdot y = x^2 + xy + yx + y^2$$

Definition 1.1.5. *A* ***subring*** $(R', +, \cdot)$ ***of a ring*** $(R, +, \cdot)$ *is such that:*

1. $(R', +)$ *is a subgroup of* $(R, +)$,
2. *It is closed under the multiplication. That is, for any $a, b \in R'$, $a \cdot' b \in R'$.*

Remark I.1. ⚠*It is easier to check that a ring is a subring of a well-know ring.*

1.2 Ideals

Definition 1.2.1. *A non-empty subset I of some ring R is said to be a* ***right (reps. left) ideal*** *of R if*

1. *I is a subgroup of R under addition,*
2. *For every $i \in I$ and $r \in R$, $ir \in I$ (resp. $ri \in I$).*

An ***(two-sided) ideal*** *is both left and right ideal.*

Remark I.2. *on a ring R different from the zero ring, there are always at least two ideals the zero-ideal $\{0\}$ and R.*

Example 1.2.2. *The ideals of $\mathbb{Z}$ are exactly, using group theory, of the form $n\mathbb{Z}$, for $n \in \mathbb{Z}$.*

Definition 1.2.3. *An ideal of some ring R is said to be* ***principal*** *if it is of the form aR or Ra, for some $a \in R$. If R is commutative, we write (a) such ideal.*

Definition 1.2.4. *An ideal $M \neq R$ of some ring R is a* ***maximal ideal of*** *R if whenever I is an ideal of R such that $M \subset I \subset R$ then either $R = I$ or $M = I$.*

Example 1.2.5. *The ideals maximal of $\mathbb{Z}$ are exactly the $p\mathbb{Z}$, where p is a prime number. In fact, let p be a prime and $m\mathbb{Z}$ an arbitrary ideal of $\mathbb{Z}$ that $p\mathbb{Z} \subset m\mathbb{Z}$. Then, in particular, $p \in m\mathbb{Z}$, thus there is $n \in \mathbb{Z}$ such that $p = mn$. Since p is prime, this implies that $m = p$ and then $p\mathbb{Z} = m\mathbb{Z}$ or $m = 1$ and then $\mathbb{Z} = m\mathbb{Z}$. So, that $p\mathbb{Z}$ is maximal. Let now $p\mathbb{Z}$ be a maximal ideal and suppose by contradiction that p is not a prime. That is, there are non unit elements of R, a and b such that $p = ab$. But then $p\mathbb{Z} \subset a\mathbb{Z}$. By maximality, or $a\mathbb{Z} = p\mathbb{Z}$, then $p|a$ and $a|p$ thus $a = p$, or $a\mathbb{Z} = \mathbb{Z}$ and $a = 1$ thus $b = p$. As a consequence, p is prime. So, maximal ideals of $\mathbb{Z}$ correspond exactly to the notion of prime number. This is not necessarily true for a general ring.*

1.3 Homomorphisms

Definition 1.3.1. *A mapping ϕ from a ring $(R, +, \cdot)$ to a ring $(R', +', \cdot')$ is said to be a* ***homomorphism of rings*** *if for any $a, b \in R$, we have:*

1. $\phi(a + b) = \phi(a) +' \phi(b)$,
2. $\phi(ab) = \phi(a) \cdot' \phi(b)$.

If $R = R'$, ϕ is an ***endomophism****.*

Directly from the definition, we obtain the following result:

Lemma 1.3.2. *If ϕ is a homomorphism from R to R' then:*

1. $\phi(0) = 0'$,
2. $\phi(-a) = -\phi(a)$ *for every $a \in R$.*

Remark I.3. *From the definition and the previous lemma,*

1. *ϕ is a group homomorphism.*
2. ⚠*If R has a unit 1 and R' a unit $1'$, we do not have necessarily that $\phi(1) = 1'$, unless for example,*
   (a) *R' is an integral domain.*
   (b) *R' is an arbitrary ring but ϕ is onto.*

Lemma 1.3.3. *If ϕ is a homomorphism from R into R', then its kernel $I(\phi)$ is an ideal of R.*

Proof. By group theory, $I(\phi)$ is a subgroup of R. Let $a \in I(\phi)$, $r \in R$, then $\phi(a) = 0$ so that $\phi(a \cdot r) = \phi(a) \cdot' \phi(r) = 0 \cdot' \phi(r) = 0$. Then $a \cdot r \in I(\phi)$. Similarly, $r \cdot a \in I(\phi)$. So, $I(\phi)$ is an ideal. □

Example 1.3.4. 1. *Let $\phi : R \to R'$ be a map defined by $\phi(a) = 0$, for any $a \in R$. Trivially, ϕ is a homomorphism and $I(\phi) = R$. ϕ is called the* ***zero-homomorphism****.*

2. *Let $\phi : R \to R$ be a map defined by $\phi(x) = x$, for any $x \in R$. Trivially, ϕ is a homomorphism and $I(\phi) = (0)$. ϕ is called the* ***identity homomorphism of*** *R.*

3. *Let $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} | m, n \in \mathbb{Z}\} \subset R$ It is a ring for usual addition and multiplication on real numbers. (Verify!) Let $\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ be a map defined by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$. ϕ is a homomorphism and $I(\phi) = (0)$.*

Definition 1.3.5. 1. *A homomorphism from R into R' is said to be an* ***isomorphism*** *if it is one to one mapping. If $R = R'$ then an isomorphism is called an* ***automorphism****.*

2. *Two rings are said to be* ***isomorphic*** *if the is an isomorphism of one into the other.*

1.4 Quotient

Definition 1.4.1 (Proposition)**.** *Given an ideal U of a ring.*

1. *Let R/U be the set of all the distinct cosets $a + U$, for $a \in R$, of U in R (obtained by considering U as a subgroup of R under the addition). R/U is a ring called the* ***quotient ring*** *where*

   (a) *the addition $+$ is defined by $(a + U) + (b + U) = (a + b) + U$, where a, b are in R,*

   (b) *the multiplication . is defined by $(a + U)(b + U) = (ab) + U$*

2. *If R is commutative, so is R/U (The converse is false!).*

3. *If 1 is a unit of R, then $1 + U$ is a unit of R/U.*

4. *There is a homomorphism $\phi : R \to R/U$ given by $\phi(a) = a + U$, for any $a \in R$ whose kernel is exactly U.*

Proof. $(R/U, +)$ is a group, using group theory. . is well defined. That is, for $a' \in R$ an other representative of $a + U$ that is, $a' + U = a + U$ and $b' \in R$ an other representative of $b + U$ that is, $b' + U = b + U$, then $a'b' + U = ab + U$. Since $a + U = a' + U$, then there is $u_1 \in U$ such that $a = a' + u_1$ and since $b + U = b' + U$, then there is $u_2 \in U$ such that $b = b' + u_2$. Then,

$$ab = a'b' + u_1 b' + a' u_2 + u_1 u_2$$

with $u_1 b' + a' u_2 + u_1 u_2 \in U$ since U is an ideal. Then $a'b' + U = ab + U$. The student might check easily that all the ring axioms are verified. □

Referring to group theory for the proof, we mention the following lemma:

Theorem 1.4.2. *Let R, R' be rings and ϕ a surjective homomorphism of R to R' with kernel U. Then, R' is isomorphic to R/U. Moreover, there is a one to one correspondence Φ between the set of ideals of R' and the set of ideals of R which contains U. For W' an ideal of R', we set $\Phi(W')$ to be the ideal $\{x \in R | \phi(x) \in W'\}$ and for an ideal W of R which contains U, we set $\Phi^{-1}(W) = W/I$. Moreover, $R/\phi(W)$ is isomorphic to R'/W'*

Example 1.4.3. *Let $n \in \mathbb{Z}$. Define $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\phi(a) = \bar{a}$ which is the class of a modulo n. It is easy to check that ϕ is an homomorphism and that the kernel $I(\phi)$ of ϕ consist of al the multiples of n.*

2 Important classes of rings

2.1 Integral rings

Definition 2.1.1. *If R is a commutative ring then $a \neq 0 \in R$ is said to be **a zero divisor** if there is a, $b \in R$ such that $b \neq 0$ and $ab = 0$.*

Example 2.1.2. *Let $\mathbb{Z}/6\mathbb{Z}$ be the set of integers mod 6 under the addition and the multiplication mod 6. If we denote the elements in $\mathbb{Z}/6\mathbb{Z}$ by $\bar{0}, \bar{1}, \bar{2}, ..., \bar{5}$, one sees that $\bar{2}\bar{3} = \bar{0}$, yet $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$. Thus $\bar{2}$ and $\bar{3}$ are zero-divisors.*

Definition 2.1.3. *A commutative ring is an **integral domain** if it has no zero divisors.*

Definition 2.1.4. *Let R be an integral domain.*

1. *We say that R has n-**torsion** $n > 0$ if there is an element $a \neq 0 \in R$ such that $na = 0$ and $ma \neq 0$ for $0 < m < n$.*

2. *The characteristic is 0 if $pa = 0$, for every $a \in R$ if and only $p = 0$ or equals the smallest integer p such that $pa = 0$, for any $a \in R$, if it exists such integers (p is then automatically prime, any $a \neq 0 \in R$ are p-torsions). If the characteristic is non-zero, then R is **of finite characteristic**.*

Example 2.1.5. *$\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$ are integral domains.*

2.2 Division ring

Definition 2.2.1. *A ring is said to be a **division ring** if its non-zero elements form a group under the multiplication. We denote a^{-1} the inverse of an element $a \in R$, for the multiplication.*

2.3 Fields

Definition 2.3.1. 1. *A* ***field*** *is a commutative integral division ring.*

2. *A field with finite number of element is called a* ***finite field.***

Example 2.3.2. $\mathbb{C}$, $\mathbb{Q}$ *and the set of the integers mod* 7 *are fields.*

Exercise 2.3.3. *Let*

$$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

Prove that $\mathbb{Q}(\sqrt{2})$ *is a subring of* $\mathbb{R}$*. Show, by writing an explicit formula, that every nonzero element* $a + b\sqrt{2}$ *of* $\mathbb{Q}(\sqrt{2})$ *has a multiplicative inverse in* $\mathbb{Q}(\sqrt{2})$ *(and hence that* $\mathbb{Q}(\sqrt{2})$ *is a field.)*

Solution: $\mathbb{Q}(\sqrt{2})$ *is a subring of* $\mathbb{R}$

1. ***Identity:*** $0 = 0 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
2. ***Inverse:*** *If* $u \in \mathbb{Q}[\sqrt{2}]$ *then* $u = a+b\sqrt{2}$ *for some* $a, b \in \mathbb{Q}$ *so* $-u = (-a)+(-b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.
3. **Sum:** *If* $u, v \in \mathbb{Q}[\sqrt{2}]$ *then* $u = a+b\sqrt{2}$, $v = c+d\sqrt{2}$ *so* $u+v = (a+c)+(b+d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.
4. ***Product:*** *If* $u, v \in \mathbb{Q}[\sqrt{2}]$ *then* $u = a + b\sqrt{2}$, $v = c + d\sqrt{2}$ *so*

$$uv = (ac + 2bd) + (ad + bc)\sqrt{2}$$

To explicit an inverse, we notice that $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Since $\sqrt{2}$ is irrational, $a^2 - 2b^2 \neq 0$ *for any pair a, b of rational numbers not both zero. Hence, we can divide by* $a^2 - 2b^2$ *to get*

$$\left(a + b\sqrt{2}\right)\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) = 1,$$

i.e.,

$$\left(a + b\sqrt{2}\right)^{-1} = c + d\sqrt{2}, \quad \textit{with} \quad c := \frac{a}{a^2 - 2b^2}, \quad d := -\frac{b}{a^2 - 2b^2}$$

c, d are rationals so $\left(a + b\sqrt{2}\right)^{-1} \in \mathbb{Q}[\sqrt{2}]$.

We will now establish some criterium to be a field. We recall first the following very simple minded principle

Lemma 2.3.4 (the Pigeon Hole principle)**.** *We always have the two equivalent assertions:*

1. *If n objects are distributed over m places and if* $n > m$*, then some place receives at least two objects.*
2. *If n object are distributed over n places in such a way that no places receive more than one object, then each place receives exactly one object.*

As a consequence, we have:

Lemma 2.3.5. *A finite integral domain is a field.*

Proof. Let D be a finite integral domain. In order to prove that D is a field, we have to prove that:

1. There is a unit element $1 \in D$ such that $a.1 = a$, for any $a \in D$.

2. For every element $a \neq 0 \in D$, there is an inverse element $b \in D$ such that $ab = 1$.

In fact, let $x_1, .. , x_n$ be all elements of D and $a \neq 0 \in D$. The element $x_1 a, ..., x_n a$ are all in D and all distinct. Indeed, for $i \neq j$, suppose by contradiction that $x_i a = x_j a$, then $(x_i - x_j)a = 0$ and $(x_i - x_j) \neq 0$ and $a \neq 0$ which is impossible since D is an integral ring. Thus, $x_i a \neq x_j b$. By the pigeon hole principle, every $y \in D$ can be written as $x_i a$ for some x_i. In particular, there is an x_{i_0} such that $a = x_{i_0} a = a x_{i_0}$ (D is commutative). Let's prove that x_{i_0} is the unit element. Let $y \in D$, with $y \neq 0$, there is a x_i such that $y = x_i a$ and $y x_{i_0} = (x_i a) x_{i_0} = x_i (a x_{i_0}) = x_i a = y$. This proves that $x_{i_0} = 1$. Now, since $1 \in D$, there is x_j such that $1 = x_j a = a x_j$ and x_j is the inverse of a. □

Corollary 2.3.6. *If p is a prime, the ring $\mathbb{Z}/p\mathbb{Z}$ of the integers modulo p is a field.*

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is finite, by the previous lemma, it is enough to prove that it is integral. Let then $\bar{a}$ and $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$ with a, $b \in \{0, ..., p\}$ representatives of the classes $\bar{a}$ and $\bar{b}$. Suppose that $ab \equiv 0 mod\ p$ then $p|ab$. This implies that either $p|a$ or $p|b$. In other words, or $\bar{a} = 0$ or $\bar{b} = 0$. So, $\mathbb{Z}/p\mathbb{Z}$ has no zero divisor. □

Remark I.4. *We can have an infinity of finite field, but not all finite field are of the form $\mathbb{Z}/p\mathbb{Z}$ with p prime.*

Lemma 2.3.7. *Let R be a commutative ring with unit element whose only ideal are* (0) *and R itself the R is a field.*

Proof. Let $a \neq 0 \in R$. Consider the set $Ra = \{xa | x \in R\}$. We can easily check that Ra is an ideal of R. By assumption, $Ra = (0)$ or $Ra = R$. But $a \neq 0$ and $a = 1.a \in Ra$, then $Ra \neq (0)$. Thus, $Ra = R$. In particular, there is $b \in R$, such that $ba = 1$. □

Theorem 2.3.8. *If R is a commutative ring with unit element and M is an ideal of R then M is a maximal ideal if and only if R/M is a field.*

Proof. We use in the following the 1.1 correspondence ψ of Theorem 1.4.2.

1. Suppose that M is an ideal such that R/M is a field, R/M being a field has only (0) and R/M as ideal so R as also only 2 ideals containing M which are M and R. So M is maximal.

2. If M is maximal, there is only M and R as ideal containing M so there is just two ideal on R/M which must be (0) and R/M and R/M is a field by the previous lemma.

□

2.4 Principal ideal rings

Definition 2.4.1. *An integral domain R with unit element is a principal ideal ring, if every ideal in R is of the form (a) for some $a \in R$.*

Example 2.4.2. *$\mathbb{Z}$ is a principal ideal ring.*

2.5 Euclidean ring

2.5.1 Definition

Definition 2.5.1. *An integral domain R is said to be a* ***Euclidean ring*** *if for every $a \neq 0$ in R, there is defined a non negative integer $d(a)$ such that:*

1. *$\forall a, b \in R$, both non-zero $d(a) \leq d(ab)$,*

2. *$\forall a, b \in R$ both non zero, there exist $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.*

Remark I.5. ⚠ *We do not assign a value to $d(0)$.*

Example 2.5.2. *$\mathbb{Z}$ is a Euclidean ring where d is the usual absolute value.*

Theorem 2.5.3. *Euclidean rings have a unit element and they are principal ideal rings.*

Proof. Let R be an Euclidean ring.

1. We prove first that all ideals of R are principal. Let I be an ideal of R. If $I = (0)$ there I is principal, otherwise there is $a \neq 0 \in R$. Pick $a_0 \in R$ such that $d(a_0)$ is minimal (since d takes on non-negative values thus it is always possible. Let $b \in I$, then by Euclidean rings property, there is $t, r \in R$ such that $a = ta_0 + r$ where either $r = 0$ or $d(r) < d(a_0)$. Since $a_0 \in I$, $a \in I$ and I is an ideal, we have that $r = a - ta_0 \in I$ and from minimality property of a_0, we have that $r = 0$, $a = ta_0$ thus $I = (a_0)$.

2. We prove now that R has a unit element. R is clearly an ideal then $R = (b)$ for some $b \in R$, and then there is also $e \in R$ such that $b = be$. Take now an $a \in R$, there is a $x \in R$ such that $a = xb$. For this, we obtain $ae = (xb)e = x(bc) = xb = a$. Thus, e is seen to be the required unit.

□

2.5.2 Divisibility theory for Euclidean rings

Definition 2.5.4. *If $a \neq 0$ and b are in a commutative ring R then a* ***is said to divide*** *b if there exist $a, c \in R$ such that $b = ac$. We write $a|b$ when a divide b and $a \nmid b$ when a does not divide b.*

Remark I.6. *One can check easily the following properties.*

1. *If $a|b$ and $b|c$ then $a|c$,*

2. *If $a|b$ and $a|c$ then $a|(b \pm c)$,*

3. *If $a|b$ then $a|bx$, for any $x \in R$.*

Definition 2.5.5. *Let R be a commutative ring. If $a, b \in R$, then $d \in R$ is said to be the **greatest common divisor of** a **and** b if*

1. *$d|a$ and $d|b$,*

2. *whenever $c|a$ and $c|b$ then $c|d$.*

We write $d = (a, b)$.

Lemma 2.5.6. *Let R be an euclidean ring then any two elements a and $b \in R$ have a greatest common divisor d. Moreover, $d = \lambda a + \mu b$, for some λ, $\mu \in R$.*

Proof. Let $I := \{ra + sb | r, s \in R\}$, one can easily check that I is an ideal. Since R is a Euclidean ring, it is in particular a principal ideal ring and there is $d \in A$ such that $I = (d)$, in particular, there are λ, $\mu \in R$ such that $d = \lambda a + \mu b$. Since Euclidean rings have unit element, one can write $a = 1.a + 0.b \in I$ and $b = 0.a + 1.b \in I$ so that, $d|a$ and $d|b$. Moreover, if $c|a$ and $c|b$ then $c|\lambda a + \mu b = d$. As a consequence, $d = (a, b)$ as required. □

Definition 2.5.7. *Let R be a commutative ring with unit element. An element $a \in R$ is a **unit** if there exists an element $b \in R$ such that $ab = 1$.*

Remark I.7. ⚠*Do not confuse a unit with a unit element! A unit in a ring is an element whose inverse is also in the ring.*

Lemma 2.5.8. *Let R be an integral domain with a unit element and suppose that for $a, b \in R$ both $a|b$ and $b|a$. Then $a = ub$ where u is a unit in R.*

Proof. Since $a|b$, $b = xa$ for some $x \in R$ and since $b|a$, $a = yb$ for some $y \in R$. Thus $b = x(yb) = (xy)b$, so, $b(1 - xy) = 0$. Since R is an integral domain and $b \neq 0$ then $1 - xy = 0$ and $1 = xy$. y is thus a unit and $a = yb$. □

Definition 2.5.9. *Let R be a commutative ring with unit element. Two elements $a, b \in R$ are said to be **associates** if $b = ua$ for some unit $u \in R$.*

Lemma 2.5.10. *Let R be a Euclidean ring and $a, b \in R$, if $b \neq 0$ is not a unit in R then $d(a) < d(ab)$.*

Proof. Consider the ideal $I = (a) = \{xa | x \in R\}$ of R. By property of Euclidean ring, we have $d(a) \leq d(xa)$, for $x \neq 0 \in R$. By the proof of Theorem 2.5.3, if $d(a) = d(ab)$, we have ab minimal and $I = (ab)$, then $a = abx$, but then since E is integral, $bx = 1$ and b is a unit, this contradict the assumption. □

Definition 2.5.11. *In a Euclidean ring R, a non-unit π is said to be **a prime element of** R if whenever $\pi = ab$ where a, b are in R then one of a or b are a unit.*

Remark I.8. *Let $a \in R$. If π is a prime element and $\pi \nmid a$ then $(a, \pi) = 1$.*

Lemma 2.5.12. *Let R be a Euclidean ring such that for a, b, $c \in R$, $a|bc$ but $(a, b) = 1$ then $a|c$.*

Proof. By Bezout lemma, there are λ, $\mu \in R$ such that $\lambda a + \mu b = 1$. So multiplying by c, we obtain $\lambda ac + \mu bc = c$. Now, $a|\lambda ac$, always and $a|\mu bc$, since $a|bc$ by assumption; therefore $a|(\lambda ac + \mu bc) = c$. □

Lemma 2.5.13. *If π is a prime element in the Euclidean ring R and $\pi|ab$ where a, $b \in R$, then π divides at least one of a or b.*

Proof. Suppose that $\pi \nmid a$ then $(\pi, a) = 1$. Applying the previous lemma, $\pi|b$. □

Corollary 2.5.14. *If π is a prime element in the Euclidean ring R and $\pi|a_1...a_n$ then π divides at least one $a_1, \dots, a_n$.*

Euclidean rings have the unique factorization on prime property.

Theorem 2.5.15 (Factorization theorem). *Every non-zero element of an Euclidean ring R can be uniquely written (up to associates) as a product of prime elements or is a unit.*

Proof.

1. **Existence:** By induction on $d(a)$. If $d(a) = d(1)$ then a is a unit in R. Indeed, otherwise $d(1) < d(1.a)$ and the lemma is proved. We assume that the lemma is true for all element $x \in R$ such that $d(x) < d(a)$. Let prove it for a. If a is a unit or prime, there is nothing to prove, if it is not a unit nor prime, there is b and $c \in R$ which are not units, then $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Using the induction hypothesis, we can write $b = \pi'_1...\pi'_n$ and $c = \pi_1...\pi_m$ where the π''s and the π's are prime. As a consequence, $a = \pi'_1...\pi'_n\pi_1...\pi_m$.

2. **Unicity:** Let $a = \pi_1...\pi_m = \pi'_1...\pi'_n$ be two factorization into primes. Since $\pi_1|\pi_1...\pi_m = \pi'_1...\pi'_n$, then $\pi_1|p'_i$, for some i but π'_i and π_1 are prime, so they are associates. Repeating this argument we prove unicity (up to associates).

□

Lemma 2.5.16. *The ideal $A = (a_0)$ is maximal ideal of the Euclidean ring R if and only if a_0 is a prime element of R.*

Proof. If a_0 is not a prime element, then $a_0 = bc$, b, c non-zero elements of R and non units. Then, $(a_0) \subset (b)$. If $(b) = R$, $1 \in B$ then $1 = xb$, so b is a unit and this contradicts the assumption. If $A = (b)$, $b \in (a_0)$, $b = a_0r = bcr$ so c is a unit and this contracdicts also the assumption. As a consequence, A is not maximal. Conversely, suppose that a_0 is a prime element of R, let U be an ideal of R such that $A = (a_0) \subset U \subset R$. Since R is Euclidean so in particular a principal ideal ring, then $U = (u_0)$. Since $a_0 \in A \subset U = (u_0)$, $a_0 = xu_0$, for some $x \in R$. But, a_0 is a prime element of R then, or x is a unit and $U = A$ or u_0 is a unit and $U = R$. As a consequence, A is maximal. □

3 Polynomial rings

3.1 Definitions

Definition 3.1.1. *A **polynomial in the indeterminate** x **over a field** F is a set of symbols $a_0 + a_1x + ... + a_nx^n$, where n can be any nonnegative integer and where the **coefficients** $a_1, ..., a_n$ are all in F.*

We will define now operation on polynomials. Two polynomials are declared to be equals if and only if their corresponding coefficients are equal. More precisely,

Definition 3.1.2. *If $p(x) = a_0 + a_1x + ... + a_nx^n$ and $q(x) = b_0 + b_1x + ... + b_mx^m$ are two polynomials in the indeterminate x over a field F, $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$.*

To add two polynomial, we add their coefficients. More precisely,

Definition 3.1.3. *If $p(x) = a_0 + a_1x + ... + a_nx^n$ and $q(x) = b_0 + b_1x + ... + b_mx^m$ are two polynomials in the indeterminate x over a field F, $p(x) + q(x) = c_0 + c_1x + ... + c_tx^t$ where for each i, $c_i = a_i + b_i$.*

Example 3.1.4. *To add $1+x$ and $3-2x+x^2$, we consider $1+x$ as $1+x+0x^2$ and add, according to the receipt given in the definition to obtain as their sum $4 - x + x^2$*

The most complicated to formalize, is to define the multiplication. Formally, we define:

Definition 3.1.5. *If $p(x) = a_0 + a_1x + ... + a_nx^n$ and $q(x) = b_0 + b_1x + ... + b_mx^m$ are two polynomials in the indeterminate x over a field F, $p(x)q(x) = c_0 + c_1x + ... + c_kx^k$ where for each i, $c_i = a_ib_0 + a_{i-1}b_1 + a_{i-2}b_2 + ... + a_0b_i$.*

Example 3.1.6. *To multiply $1 + x - x^2$ to $2 + x^2 + x^3$ we can use the definition or just do the distribution and we get $(1 + x - x^2)(2 + x^2 + x^3) = 2 + 2x - x^2 + 2x^3 - x^5$*

The reader can check easily the following fact:

Definition 3.1.7 (Proposition)**.** *Let F be a field. We denote by $F[x]$ the set of the polynomials in the indeterminate x over a field F, together with the addition and the multiplication that we just defined, it forms a ring called **the ring of polynomials in the indeterminate** x **over a field** F.*

On this ring, we can define an important constant which is the degree of a polynomial.

Definition 3.1.8. *If $p(x) = a_0 + a_1x + .. + a_nx^n \neq 0$ and $a_n \neq 0$ then the degree of $p(x)$, written as $deg(p(x))$, is n. That is, the degree of $p(x)$ is the largest integer i for with the i^{th} coefficient of $p(x)$ is not 0. We do not define the degree of the zero polynomial. We say a polynomial is a **constant** if its degree is 0.*

The degree function defined on the nonzero elements of $F[x]$ will provide us with the $d(x)$ function needed in order that $F[x]$ be a Euclidean ring.

Lemma 3.1.9. *If $p(x)$, $q(x)$ are two nonzero elements of $F[x]$, then $deg(p(x), q(x)) = deg(p(x)) + deg(q(x))$.*

Proof. Suppose that $p(x) = a_0 + a_1x + ...a_mx^m$, $q(x) = b_0 + b_1x + ...b_nx^n$ and that $a_m \neq 0$ and $b_n \neq 0$. Therefore $deg(p(x)) = m$ and $deg(q(x)) = n$. By definition, $p(x)q(x) = c_0 + c_1x + ... + c_kx^k$ where where for each i, $c_i = a_ib_0 + a_{i-1}b_1 + a_{i-2}b_2 + ... + a_0b_i$. We have $c_{m+n} = a_mb_n \neq 0$ by definition. For $i > m+n$, c_i is the sum of terms of the form a_jb_{i-j}; since $i = j + (i-j) > m+n$ then either $j > m$ or $i - j > n$. But then one of a_j or b_{i-j} is 0 and the result follows. □

Corollary 3.1.10. *If $p(x)$, $q(x)$ are non zero elements in $F[x]$ then $deg(p(x)) \leq deg(p(x)q(x))$.*

Corollary 3.1.11. *$F[x]$ is an integral domain.*

Lemma 3.1.12 (The division algorithm)**.** *Given two polynomials $p(x)$ and $q(x) \neq 0$ in $F[x]$, then there exist two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $p(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) < deg(q(x))$.*

Proof. If the degree of $p(x)$ is smaller than that of $q(x)$ there is nothing to prove for merely put $t(x) = 0$, $r(x) = p(x)$, and we certainly have that $p(x) = 0q(x) + p(x)$ where $deg(p(x)) < deg(g(x))$ or $p(x) = 0$.

So we may assume that $p(x) = a_0 + a_1x + ... + a_mx^m$ and $q(x) = b_0 + b_1x + ... + b_nx^n$ where $a_m \neq 0$, $b_n \neq 0$ and $m \geq n$.

Let $f_1(x) = f(x) - (a_m/b_n)x^{m-n}q(x)$; thus $deg(f_1(x)) \leq m-1$, so by induction on the degree of $p(x)$ we may assume that $p_1(x) = t_1(x)q(x) + r(x)$ where $r(x) = 0$ or $deg(r(x)) < deg(q(x))$. But then $p(x) - (a_m/b_n)x^{m-n}q(x) = t_1(x)q(x) + r(x)$. Then, $p(x) = t(x)q(x) + r(x)$, where $t(x) = (a_m/b_n\text{à}x^{m-n} + t_1(x)$, we do indeed have that $f(x) = t(x)q(x) + r(x)$ where $t(x), r(x) \in F[x]$ and where $r(x) = 0$ or $deg(r(x)) < deg(q(x))$. This proves the lemma. □

Taking $d = deg$, we have proven that:

Theorem 3.1.13. *$F[x]$ is a Euclidean ring.*

So, the results on the general Euclidean rings are translated as follows.

Lemma 3.1.14. *$F[x]$ is a principal ideal ring.*

.

Lemma 3.1.15. *Given two polynomials $p(x)$, $q(x)$ in $F[x]$, they have a greatest common divisor $d(x)$ which can be realized as $d(x) = \lambda(x)p(x) + \mu(x)q(x)$.*

A prime element of $F[x]$ is said irreducible, we recall here the definition:

Definition 3.1.16. *A polynomial $p(x)$ in $F[x]$ is said to be **irreducible** over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ or $b(x)$ has degree 0 (i.e., is a constant).*

Remark I.9. *1. A polynomial of degree 1 is always irreducible.*

2. ⚠*A polynomial $p(x)$ of degree 2 or 3 is irreducible over F if it has no roots on F (i.e. for any $f \in F$, $p(f) \neq 0$). This is not true for degree greater than 3.*

3. ⚠*Irreducibility depends on the field; for instance the polynomial $x^2 + 1$ is irreducible on $\mathbb{R}[x]$ but not on $\mathbb{C}[x]$, since $x^2 + 1 = (x - i)(x + i)$ where $i^2 = -1$.*

Lemma 3.1.17. *Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomials in $F[x]$.*

Lemma 3.1.18. *The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.*

3.2 Polynomials over the rational field

We shall be concerned with their irreducibility.

Definition 3.2.1. *The polynomial $p(x) = a_0 + a_1x + ... + a_nx^n$ in $\mathbb{Z}[x]$ is said to be* ***primitive*** *if the greatest common divisor of $a_0, a_1, ..., a_n$ is 1.*

Lemma 3.2.2. *If $p(x)$ and $q(x)$ are primitive polynomials, then $p(x)q(x)$ is a primitive polynomial.*

Proof. Let $p(x) = a_0 + a_1x + ...a_nx^n$ and $q(x) = b_0 + b_1x + .. + b_mx^m$. Suppose that the lemma was false; then all the coefficients of $p(x)q(x)$ would be divisible by some integer larger than 1, hence by some prime p. Since $p(x)$ is primitive, there is a_i such that $p \nmid a_i$, let a_j the first coefficient such that this occur. Similarly, let b_k be the first coefficient of $q(x)$ which p does not divide. In $p(x)q(x)$ the coefficient of x^{j+k}, c_{j+k} is

$$c_{j+k} = a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + ... + a_0b_{j+k})$$

Now by our choice of b_k, $p|(a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0)$ and by our choice of a_j, $p|(a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + ... + a_0b_{j+k})$. By assumption, $p|c_{j+k}$. Thus $p|a_jb_k$, which is a nonsense since $p \nmid a_j$ and $p \nmid b_k$. This proves the lemma. □

Definition 3.2.3. *The* ***content*** *of the polynomial $p(x) = a_0 + a_1x + ... + a_nx^n$ in $\mathbb{Z}[x]$ is the greatest common divisor of the integers $a_0, a_1, ..., a_n$*

Remark I.10. *Clearly, given any polynomial $p(x)$ in $\mathbb{Z}[x]$ it can be written as $p(x) = dq(x)$ where d is the content of $p(x)$ and where $q(x)$ is a primitive polynomial.*

Theorem 3.2.4 (Gauss' Lemma)**.** *If the primitive polynomial $p(x)$ can be factorized as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.*

Proof. Suppose that $p(x) = u(x)v(x)$ where $u(x)$ and $v(x)$ have rational coefficients. By clearing denominators and taking out common factor, we can write $p(x) = (a/b)\lambda(x)\mu(x)$, where a and b are integers and where both $\lambda(x)$ and $\mu(x)$ have integer coefficients and are primitive. Thus $bp(x) = a\lambda(x)\mu(x)$. The content of the left-hand side is b, since $p(x)$ is primitive; since both $\lambda(x)$ and $\mu(x)$ are primitive, by the previous lemma $\lambda(x)\mu(x)$ is primitive, so the content of the right side is a. Therefore $a = b$, $(a/b) = 1$, and $p(x) = \lambda(x)\mu(x)$ where $\lambda(x)$ and $\mu(x)$ have integer coefficients. This is the assertion of the theorem. □

Definition 3.2.5. *A polynomial is said to be* ***integer monic*** *if all its coefficients are integers and its highest coefficient is* 1.

Remark I.11. *Thus an integer monic polynomial is merely one of form* $x^n + a_1x^{n-1} + ... + a_n$ *where the* $a_i^{\prime}s$ *are integers. Clearly an integer monic polynomial is primitive.*

Corollary 3.2.6. *If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.*

The proof is left to the reader. The question of deciding whether a given polynomial is irreducible or not can be a difficult and laborious one. We end this section with the Eisentein criterion which declare a way to say that a polynomial is irreducible.

Theorem 3.2.7 (The Eisenstein criterion)**.** *Let* $p(x) = a_0 + a_1x + ... + a_nx^n$ *be a polynomial with integer coefficients. Suppose that for some prime number* p, $p \nmid a_n$, $p|a_1$, $p|a_2$, ..., $p|a_0$, $p^2 \nmid a_0$. *Then* $p(x)$ *is irreducible over the rationals.*

Proof. Without loss of generality we may assume that $p(x)$ is primitive, for taking out the greatest common factor of its coefficients does not disturb the hypotheses, since $p \nmid a_n$. If $p(x)$ factors as a product of two rational polynomials having integer coefficients. Thus if we assume that $p(x)$ is reducible, then

$$p(x) = (b_0 + b_1x + ... + b_rx^r)(c_0 + c_1x + .. + c_sx^s),$$

where the b's and the c's are integers and where $r > 0$ and $s > 0$. Reading off the coefficient we first get $a_0 = b_0c_0$. Since $p|a_0$, p must divide one of b_0 or c_0. Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0. Suppose that $p|b_0$, $p \nmid c_0$. Not all the coefficients b_0, ... , b_r can be divisible by p; otherwise since $p \nmid a_n$. Let b_k be the first b not divisible by p, which manifestly false since $p \nmid a_n$. Let b_k be the first b not divisible by p, $k \le r < n$. Thus, $p|b_{k-1}$ and earlier b's. But $a_k = b_kc_0 + b_{k-1}c_1 + b_{k-2}c_2 + ... + b_0c_k$, which conflicts with $p|b_kc_0$. This contradiction proves that we could not have factored $p(x)$ and so $p(x)$ is indeed irreducible. □

Chapter II

Vector space

Vector spaces owe their importance to the fact that many models arising in solutions of specific problems turn out to be vector spaces. Among the fundamental notions that make vector spaces so important are those of linearly dependence, basis and dimension.

1 Definitions and first examples

Definition 1.0.8. *A nonempty set V is said to be a* ***vector space over a field*** *F if V is an abelian group under an operation which we denote by $+$, and if for every $\alpha \in F$, $v \in V$ there is defined an element, written αv, in V subject to*

1. $\alpha(v+w) = \alpha v + \alpha w$*;*

2. $(\alpha+\beta)v = \alpha v + \beta v$*;*

3. $\alpha(\beta v) = (\alpha\beta)v$*;*

4. $1.v = v$.

for all α, $\beta \in F$, v, $w \in V$ (where the 1 represents the unit element of F under multiplication). We say that an element $\alpha \in F$ is a ***scalar*** *and an element $v \in V$ is a* ***vector****.*

Remark II.1. *Fields are vector spaces over themself.*

From the definition, we get the following properties for V:

Lemma 1.0.9. *If V is a vector space over F then*

1. $\alpha 0 = 0$ *for any $\alpha \in F$;*

2. $0v = 0$ *for any $v \in V$;*

3. $(-\alpha)v = -(\alpha v)$*, for any $\alpha \in F$, $v \in V$;*

4. *If $v \neq 0$, then $\alpha v = 0$ implies that $\alpha = 0$.*

Remark II.2. *We denote similarly the* 0 *of* V *and the* 0 *of* F*, since how the lemma states multiplication by both of them leads to the* 0 *of* V*.*

Proof. This proof is analogue to the one we have done on the rings. Let's recall quickly the process.

1. Since $\alpha 0 = \alpha(0+0) = \alpha 0 + \alpha 0$, we get $\alpha 0 = 0$.
2. Since $0v = (0+0)v = 0v + 0v$. We get $0v = 0$.
3. Since $0 = (\alpha + (-\alpha))v = \alpha v + (-\alpha)v$, $(-\alpha)v = -(\alpha v)$.
4. If $\alpha v = 0$ and $\alpha \neq 0$ then $0 = \alpha^{-1}0 = \alpha^{-1}(\alpha v) = (\alpha^{-1}\alpha)v = 1v = v$.

□

The notion of subspace arises naturally from the one of vector space:

Definition 1.0.10. *If* V *is a vector space over* F *and if* $W \subset V$*, then* W *is a* ***subspace of*** V *if under the operations of* V*,* W*, itself, forms a vector space over* F*. Equivalently,* W *is a subspace of* V *whenever* w_1*,* $w_2 \in W$*,* α*,* $\beta \in F$ *implies that* $\alpha w_1 + \beta w_2 \in W$*.*

Example 1.0.11.

1. *Let* F *be a field and* K *be a field which contains* F *as a subfield. We consider* K *as a vector space over* F*, using as the* $+$ *of the vector space the addition of the elements of* K*, and by defining, for* $\alpha \in F$*,* $v \in K$*,* αv *to be the product of* α *and* v *as elements in the field* K*. Axioms* 1*,* 2 *and* 3 *for a vector space are then consequences of the right-distributive law, left distributive and associative law, respectively, which hold for* K *as a ring.*

2. *Let* F *be a field and let* V *be the totality of all ordered* n*-tuples,* $(\alpha_1,...,\alpha_n)$ *where the* $\alpha_i \in F$*. Two elements* $(\alpha_1,...,\alpha_n)$ *and* $(\beta_1,...,\beta_n)$ *of* V *are declared to be equal if and only if* $\alpha_i = \beta_i$ *for each* $i = 1,2,...,n$*. Now introduce the requisite operations in* V *to make of it a vector space by defining:*

   (a) $(\alpha_1,...,\alpha_n) + (\beta_1,...,\beta_n) = (\alpha_1+\beta_1, \alpha_2+\beta_2,...,\alpha_n+\beta_n)$.

   (b) $\gamma(\alpha_1,....,\alpha_n) = (\gamma\alpha_1,...,\gamma\alpha_n)$*, for* $\gamma \in F$*.*

   It is easy to verify that with these operations, V *is a vector space over* F*. Since it will keep reappearing, we assign a symbol to it, namely* $F^{(n)}$

3. *Let* F *be any field and let* $V = F[x]$ *the set of polynomials in* x *over* F*. We just consider the abelian group* $(V,+)$ *and for any* $P(x) = a_0 + a_1x + ... + a_kx^k$ *and* $\alpha \in F$*,* $\alpha P(x) = \alpha a_0 + \alpha a_1 x + ... + \alpha a_k x^k$*. With these operation* $F[x]$ *is a vector space over* F*.*

4. *In* $F[x]$ *let* V_n *be the set of all the polynomials of degree less than* n*.* V_n *can be seen as a subspace of* $F[x]$*. We can notice an analogy with* V_{n-1} *and* $F^{(n)}$ *but in order to compare the two objects we need to define morphisms between vector spaces.*

We recall that a morphism is a mapping preserving all the algebraic structure of our system.

2 Homomorphisms of vector spaces

Definition 2.0.12. *If U and V are vector spaces over F then, the mapping t of U into V, denoted by $t : U \to V$ is said to be a **homomorphism** or a **linear map** if*

1. $t(u_1 + u_2) = t(u_1) + t(u_2)$;

2. $t(\alpha u_1) = \alpha t(u_1)$;

That is equivalent to, require only that $t(\alpha_1 u_1 + \alpha_2 u_2) = \alpha_1 t(u_1) + \alpha_2 t(u_2)$, for any $\alpha_1, \alpha_2 \in F$ and any $u_1, u_2 \in U$.
We denote by $Hom(U,V)$ the set of all homomorphisms of U into V.
*If t, in addition, is one-to-one, t is said to be an **isomorphism**. The **kernel** of t is defined as $\{u \in U | t(u) = 0\}$ where 0 is the identity element of the addition in V (it is a subspace of U). Two vectors space are said to be **isomorphic** if there is an isomorphism of one onto the other.*

Example 2.0.13.

1. *We have a isomorphism between V_n and F^{n+1} defined by sending each polynomial $P(x) = a_0 + a_1 x + ... + a_k x^k$ to the n-tuples $(a_0, ..., a_n)$. (Verify!)*

2. *The identity of some vector space is a morphism.*

3. *The maps $\mathbb{R}$ to $\mathbb{R}$ defined by $x \mapsto x + 1$ and $x \mapsto x^2$ are not linear.*

4. *The (definite) integral is a linear map from the space of all real-valued integrable functions on some interval to $\mathbb{R}$.*

5. *Differentiation is a linear map from the space of all differentiable functions to the space of all functions.*

3 Quotient spaces

Let V a vector space over F and let W be a subspace of V. Considering these merely as abelian groups construct the quotient group V/W. We have then the following lemma, we can get inspired of the previous chapter for proving that the laws are well-defined and that the following lemma and theorem hold.

Lemma 3.0.14. *If V is a vector space over F and if W is a subspace of V, then V/W is a vector space over F, where $v_1 + W, v_2 + W \in V/W$ and $\alpha \in F$,*

1. $(v_1 + W) + (v_2 + W) = (v_1 + v_2) + W$;

2. $\alpha(v_1 + W) = \alpha v_1 + W$. *$V/W$ is called the **quotient space of** V **by** W.*

Theorem 3.0.15. *If t is a homomorphism which is onto from U to V with kernel W, then V is isomorphic to U/W. Conversely, if U is a vector space and W a subspace of U, then there is a homomorphism which is onto from U to U/W.*

Definition 3.0.16. *Let V_1, ... V_n be vector spaces. We call V the* ***direct sum of** V_1**, ... ,** V_n, denoted by writing $V_1 \oplus V_2 ... \oplus V_n$, the set of all the n-tuples $(v_1, ..., v_n)$ where $v_i \in V_i$. V is then a vector space for the addition defined by $(v_1, ..., v_n) + (v'_1, ..., v'_n) = (v_1 + v'_1, ..., v_n + v'_n)$ and for the multiplication by a scalar defined by $\alpha(v_1, ..., v_n) = (\alpha v_1, ..., \alpha v_n)$, for any $(v_1, ..., v_n)$, $(v'_1, ..., v'_n) \in V_1 \oplus V_2 ... \oplus V_n$ and any $\alpha \in F$. (We note that two elements $(v_1, ..., v_n)$ and $(v'_1, ..., v'_n)$ are equal in $V_1 \oplus V_2 ... \oplus V_n$ if and only if $v_i = v'_i$, for any $1 \le i \le n$.)*

4 Linear independence and bases

Definition 4.0.17. *If V is a vector space over F and if v_1, ... , $v_n \in V$ then any element of the form $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$, where the $\alpha_i \in F$, is a linear combination over F of v_1, ..., v_n, where the $\alpha_i \in F$, is a* ***linear combination over** F **of** v_1**, ... ,**v_n.*

Definition 4.0.18. *If S is a non empty subset of the vector space V, then $L(S)$,* ***the linear span of** S, is the set of all linear combinations of finites sets of elements of S.*

We put after all, into $L(S)$ the elements required by the axioms of a vector space, so it is not surprising to find:

Lemma 4.0.19. *If S is a non empty subset of the vector space V, then $L(S)$ is a subspace of V.*

Proof. If v and w are in $L(S)$, then $v = \lambda_1 s_1 + ... + \lambda_n s_n$ and $w = \mu_1 t_1 + ... + \mu_m t_m$ where the λ's and the μ's are in F and the s_i and t_i are all in S. Thus, for α, $\beta \in F$, $\alpha v + \beta w = \alpha(\lambda_1 s_1 + ... + \lambda_n s_n) + \beta(\mu_1 t_1 + ... + \mu_m t_m) = (\alpha\lambda_1)s_1 + ... + (\alpha\lambda_n)s_n + (\beta\mu_1)t_1 + ... + (\beta\mu_m)t_m$ and so is again in $L(S)$. $L(S)$ has been shown to be a subspace of V. □

Definition 4.0.20. *The vector space V is said to be* ***finite-dimensional over** F if there is a finite subset S in V such that $V = L(S)$. We say the S* ***spans (generates)** V or* ***forms a sets of generators of** V.*

Example 4.0.21.

1. *Every subspace of a finite-dimensional space is finite-dimensional.*
2. *Note that $F^{(n)}$ is finite-dimensional over F, for if S consists of the n vectors $(1,0,...,0)$, $(0,1,0,...,0)$, ..., $(0,0,...,0,1)$, then $V = L(S)$.*

Definition 4.0.22. *If V is a vector space and if v_1, ..., v_n are non zero element of V, we say that they are* ***linearly dependent over** F if there exist elements λ_1, ... , λ_n in F, not all of them 0, such that $\lambda_1 v_1 + ... + \lambda_n v_n = 0$. Otherwise they are said to be* ***linearly independent over** F.*

Remark II.3. ⚠*The linear dependence depends not only of the vectors but also on the field over which we are working. For example, the elements $v_1 = 1$, $v_2 = i$ in it are linearly independent over the reals but are linearly dependent over the complexes, since $i v_1 + (-1) v_2 = 0$.*

Example 4.0.23.

1. *In $F^{(3)}$, it is easy to prove that $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are linearly independent while $(1,1,0)$, $(3,1,3)$ and $(5,3,3)$ are linearly dependent.*

Linear independence is a basic concept for vector space, very important. We will give some of its properties.

Lemma 4.0.24. *If $v_1,.., v_n \in V$ are linearly independent, then every element in their linear span has a unique representation in the form $\lambda_1 v_1 + ..; + \lambda_n v_n$ with the $\lambda_i \in F$.*

Proof. Let $a \in L(v_1, ..., v_n)$, suppose that it admits two representation, $a = \alpha_1 v_1 + ... + \alpha_n v_n = \lambda_1 v_1 + ..; + \lambda_n v_n$. Then, $(\lambda_1 - \alpha_1)v_1 + ... + (\lambda_n - \alpha_n)v_n = 0$. Then, by linear independence, $\lambda_i = \alpha_i$, for any i. □

The following theorem, although very easy has consequences which form the foundation of the subject.

Theorem 4.0.25. *If $v_1, \dots, v_n$ are in V then either they are linearly independent or some v_k is a linear combination of the preceding ones, $v_1, ..., v_{k-1}$.*

Proof. If $v_1, ..., v_n$ are linearly independent there is, of course, nothing to prove. Suppose then that $\alpha_1 v_1 + ... + \alpha_n v_n = 0$ where not all the α's are 0. Let k be the largest integer for which $\alpha \neq 0$. Since $\alpha_i = 0$ for $i > k$, $\alpha_1 v_1 + ... + \alpha_k v_k = 0$ which, since $\alpha_k \neq 0$, implies that $v_k = \alpha_k^{-1}(-\alpha_1 v_1 - \alpha_2 v_2 - ... - \alpha_{k-1} v_{k-1}) = (-\alpha_k^{-1}\alpha_1)v_1 + ... + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$. Thus v_k is a linear combination of its predecessors. □

Corollary 4.0.26. *If $v_1,..., v_n$ in V have W as linear span, then we can find a subset of v_1, ..., v_n of the form $v_1, v_2, ..., v_k, v_{i_1}, ..., v_{i_r}$ consisting of linearly independent elements whose linear span is also W.*

Proof. If $v_1, ..., v_n$ are linearly independent we are done. If not, weed out from this set the first v_j, which is linear combination of its predecessors. Since $v_1, \dots, v_k$ are linearly independent, $j > k$. The subset so constructed, $v_1,..., v_k, ..., v_{j-1}, v_{j+1}, ..., v_n$ has $n-1$ elements. Clearly its linear span contained in W. However, we claim that it is actually equal to W; for given $w \in W$, w can be written as a linear combination of $v_1, ..., v_n$. But in this linear combination we can replace v_j by a linear combination of $v_1, ..., v_{j-1}$. That is, w is a linear combination of $v_1, ..., v_{j-1}, v_{j+1}, ..., v_n$.
Continuing this weeding out process, we reach a subset $v_1,..., v_k, v_{i_1}, ..., v_{i_r}$ whose linear span is still W but in which no element is a linear combination of the preceding ones. By the previous theorem, the elements $v_1, \dots, v_k, v_{i_1}, ..., v_{i_r}$ must be linearly independent. □

Definition 4.0.27. *A subset S of a vector space V is called a **basis of** V if S consist of linearly independent elements and $V = L(S)$.*

Example 4.0.28. 1. *$(1,0,...,0), ..., (0,...,0,1)$ is a basis of $F^{(n)}$*

2. *$(1, x, x2, ...)$ is a basis of $F[x]$.*

3. *Let $e_{i,j}$ be the (n,m)-matrices with 1 at the position (i,j) and $zero$ anywhere else. This is a basis of the vector space of matrices (n,m) over a field F.*

Lemma 4.0.29. *If $v_1, ..., v_n$ is a basis of V over F and if $w_1, ..., w_m$ in V are linearly independent over F, then $m \leq n$.*

Proof. Every vector in V, so in particular w_n, is a linear combination of v_1, ..., v_n. Therefore the vectors w_m, v_1, ..., v_n are linearly dependent. Moreover, they span V since v_1,..., v_n already do so. Thus some proper subset of these w_m, v_{i_1}, ..., v_{i_k} with $k \leq n-1$ forms a basis of V. We have "traded off" one w_m, in forming this new basis for at least one v_i. Repeat this procedure with the set w_{m-1}, w_m, v_{i_1}, ..., v_{i_k}. From this linearly dependent set, by the first corollary of the last theorem, we can extract a basis of the form w_{m-1}, w_m, v_{j_1}, ... , v_{j_s}, $s \leq n-2$. Keeping up this procedure we eventually get down to a basis of V of the form w_2, ..., w_{m-1}, w_m, v_α, v_β, ...; since w_1 is not linear combination of w_2, ... w_{m-1} the above basis must actually include some v. To get to this basis we introduced $m-1$ w's, each such introduction having cost us at least one v, and yet there is a v. Thus $m-1 \leq n-1$ and so $m \leq n$. □

As a direct consequence of this lemma we get the following corollary:

Corollary 4.0.30. *If V is a finite-dimensional vector space over F, then two basis have the same number of elements.*

Definition 4.0.31. *The number of elements of a basis of V is an important invariant of a vector space called the* ***dimension of*** *V* ***over*** *F, denoted by $dim_F(V)$.*

Corollary 4.0.32. *If V is a finite-dimensional vector space over F and if u_1, ..., u_m span V then some subset of u_1, ..., u_m forms a basis of V.*

Lemma 4.0.33. *A isomorphism of finitely dimensional vector spaces send bases into bases. In particular, two isomorphic vector space have the same dimension. More precisely, two finitely dimensional vector space are isomorphic if and only if they have same dimension.*

Proof. Consider $\alpha : U \to V$ an isomorphism between two finitelevector spaces U and V. Let u_1, ..., u_n a base of U. We want to prove that $\alpha(u_1)$, ... , $\alpha(u_n)$ is a basis of V. Let $v \in V$. Then, from the surjectivity of α, there is a $u \in U$ such that $\alpha(u) = v$. Since u_1, ..., u_n is a base of U, in particular it generates U then there are λ_1, ... , $\lambda_n \in F$ such that $u = \lambda_1 u_1 + ... + \lambda_n u_n$. But then $v = \alpha(u) = \lambda_1\alpha(u_1) + ... + \lambda_n\alpha(u_n)$ (since α is a morphism of vector spaces. As a consequence, $\alpha(u_1)$, ... , $\alpha(u_n)$ generates V. Now, we prove the linearly independence, let λ_1, ... , $\lambda_n \in F$, such that $\lambda_1\alpha(u_1) + ... + \lambda_n\alpha(u_n) = 0$, since α is a morphism, we get $\alpha(\lambda_1 u_1 + ... + \lambda_n u_n) = 0$. But α is an isomorphism, thus $\lambda_1 u_1 + ... + \lambda_n u_n = 0$, and by linearly independence of u_1, ..., u_n, we get that $\lambda_i = 0$, for any i, as required.

Now, we want to prove that two finitely dimensional vector space are isomorphic if and only if they have same dimension. If they have not same dimension then they cannot be isomorphic since basis are sent to basis. Let U and V two vector space of the same dimension n. We put u_1, ..., u_n (resp. v_1, ..., v_n) the basis of U (resp. V). Then defining the mapping $\alpha : U \to V$ by $\alpha(u_i) = v_i$, for any i and extending it by linearity such that it defines a morphism. Then it is not hard to prove that it is an isomorphism. (Verify!). □

Corollary 4.0.34. *$F^{(n)}$ is isomorphic to $F^{(m)}$ if and only if $n = m$.*

Corollary 4.0.35. *If V is a finite-dimensional vector space over F then V is isomorphic to $F^{(n)}$, where n is the dimension of V.*

Lemma 4.0.36. *If V is a finite-dimensional vector space over F and if u_1, ..., $u_m \in V$ are linearly independent, then we can find vectors $u_{m+1}, ..., u_{m+r}$ in V such that u_1, u_m, $u_{m+1}, ...,$ u_{m+r} is a basis of V.*

Proof. Since V is finite-dimensional it has a basis; let $v_1, ..., v_n$ be a basis of V. Since these span V, the vector $u_1, ..., u_m, v_1, ..., v_n$ also span V. Then we can find a subset of the form $u_1, ..., u_m, v_{i_1},..., v_{i_r}$ which consists of linearly independent elements which span V. □

Lemma 4.0.37. *If V is finite-dimensional and if W is a subspace of V, then W is finite-dimensional, $dim(W) \leq dim(V)$ and $dim(V/W) = dim(V) - dim(W)$.*

Proof. Write $r := dim(W)$ and $n := dim(V)$. Let $w_1, ..., w_r$ be a basis of W. By the previous lemma, we can find $v_r + 1, ..., v_n \in V$ such that $w_1, ..., w_r$, $v_{r+1},..., v_n$ form a basis of V. Then we want to prove that the $n-r$ elements $\bar{v_{r+1}},..., \bar{v_n}$ image in V/W of $v_{r+1},..., v_n$. Let $\bar{v} \in V/W$ where v is a representative of $\bar{v}$ in V. Then, $v = \alpha_1 w_1 + ... + \alpha_r w_r + \beta_1 v_{r+1} + ... + \beta_n v_n$ (since $w_1, ..., w_r$, $v_{r+1},..., v_n$ form a basis of V). But then $\bar{v} = \beta_1 \bar{v_{r+1}} + ... + \beta_n \bar{v_n}$ (since $w_i \in W$, $\bar{w_i} = 0$ for any i). Thus, $v_{r+1},..., v_n$ span V/W. We want to prove now the linearly independence. Take $\lambda_1 \bar{v_{r+1}} + ... + \lambda_r \bar{v_n} = 0$. then $\lambda_1 v_{r+1} + ... + \lambda_n v_n \in W$, thus there are $\gamma_i \in F$ and $w_i \in W$ such that $\lambda_1 v_{r+1} + ... + \lambda_n v_n = \gamma_1 w_1 + ... + \gamma_r v_r$. Then $\lambda_1 v_{r+1} + ... + \lambda_n v_n - \gamma_1 w_1 - .... - \gamma_r v_r = 0$ and since $w_1, ..., w_r$, $v_{r+1},..., v_n$ are linearly independent then $\lambda_i = 0$ and $\gamma_i = 0$ for any i. □

Corollary 4.0.38. *If A and B are finite dimensional subspaces of a vector space V, then $A + B$ is finite-dimensional and $dim(A + B) = dim(A) + dim(B) - dim(A \cap B)$.*

Proof. We have a isomorphism

$$\frac{A+B}{B} \simeq \frac{A}{A \cap B} \text{ (Verify!)}$$

Then $dim(\frac{A+B}{B}) = dim(\frac{A}{A \cap B})$. And the result follows naturally. □

Chapter III

Field theory

Fields play an important role in algebra or in number theory. We underline in this chapter some of their properties.

1 Extension fields

If F is a field and $F[X]$ is the set of all polynomials over F, that is polynomials with coefficients in F, we know that $F[X]$ is an Euclidean domain, and therefore a principal ideal domain and a unique factorization domain. Thus any nonzero polynomial f in $F[X]$ can be factored uniquely as a product of irreducible polynomials. Any root of f must be a root of one of the irreducible factors, but at this point we have no concrete information about the existence of roots and how they might be found. For example, X^2+1 has no real roots but if we consider the larger field of complex numbers, we get two roots $+i$ and $-i$. It appears that the process of passing to a larger field may help produce roots, and this turn out to be correct.

Definition 1.0.39. *Let F be a field; a field is said to be an* ***extension of*** *F if K contains F. Equivalently, K is an extension of F if F is a subfield of K.*

Throughout this chapter F will denote a given field and K an extension of F.

Remark III.1. *If K is an extension of F, then, under the ordinary field operation in K, K is a vector space over F. As a vector space we may talk about linear dependence, dimension, bases, etc., in K relative to F.*

Definition 1.0.40. *The* ***degree of*** *K* ***over*** *F denoted by $[K:F]$ is the dimension of K as a vector space over F. If it is finite (i.e. K is finite dimensional as a vector space over F), we say that K* ***is a finite extension of*** *F.*

As we announced in the introduction of this part, if f is a non constant polynomial over the field F, and f has no roots in F, we can always produce a root of f in an extension field of F. We do this after a preliminary result.

Lemma 1.0.41. *Let $f : F \to K$ be a homomorphism of fields, i.e. $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ for any $a, b \in F$ and $f(1_F) = 1_E$. Then f is a monomorphism.*

Proof. Taking I to be the kernel of F, I it is an ideal and we remember that the only ideals of the field F being (0) and F. But since $f(1) = 1$ then $I \neq F$ so $I = (0)$ and f is a injective. □

For a tower of extensions, we have this simple but powerful theorem.

Theorem 1.0.42. *If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover, $[L : F] = [L : K][K : F]$.*

Proof. Suppose that $[L : K] = n$ and that $[K : F] = m$. Let $v_1, \dots, v_n$ be a basis of L as vector space over K and let $w_1, \dots, w_m$ be a basis of K as vector space over F. We want to prove that $\{v_i w_j\}_{1\le i\le n, 1\le j\le m}$ is a basis of L as vector space over F, and thus $[L : F] = mn$.
We prove first that $\{v_i w_j\}_{1\le i\le n, 1\le j\le m}$ generates L. Let $t \in L$, since $\{v_i\}_{1\le i\le n}$ is a basis of L over K, there are elements $k_i \in K$, where $1 \le i \le n$ such that $t = \sum_{i=1}^{n} k_i v_i$, but $\{w_j\}_{1\le j\le m}$ is a basis of K over F, then there are elements $f_{i,j} \in F$, such that $k_i = \sum_{j=1}^{m} f_{i,j} w_j$ where $1 \le j \le m$. As a consequence, $t = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{i,j} v_i w_j$ and $\{v_i w_j\}_{1\le i\le n, 1\le j\le m}$ generates L over F.
We prove now that $\{v_i w_j\}_{1\le i\le n, 1\le j\le m}$ are linearly independent. Suppose that we have elements $f_{i,j}$ for $1 \le i \le n, 1 \le j \le m$ such that $\sum_{i=1}^{n} \sum_{j=1}^{m} f_{i,j} v_i w_j = 0$. By associativity, we have $\sum_{i=1}^{n} (\sum_{j=1}^{m} f_{i,j} w_j) v_i = 0$ with $\sum_{j=1}^{m} f_{i,j} w_j \in K$, since $\{v_i\}_{1\le i\le n}$ are linearly independent over K then $\sum_{j=1}^{m} f_{i,j} w_j = 0$ for any $1 \le i \le n$ but now $\{w_j\}_{1\le j\le m}$ are also linearly independent over F so we get that $f_{i,j} = 0$, for any $1 \le i \le n$ and $1 \le j \le m$. □

Remark III.2. *In the previous proof, we have seen that if L is a finite extension of K and if K is a finite extension of F, and given $\{\alpha_i\}_i$ a basis of K over F and $\{\beta_j\}_j$ a basis of L over K then $\{\alpha_i \beta_j\}_{i,j}$ form a basis of L over F.*

Corollary 1.0.43. *If L is a finite extension of F and K is a subfield of L which contains F, then $[K : F] | [L : F]$.*

Remark III.3. *By the previous result, if L is an extension of F such that $[L : F]$ is prime then there is no proper subextension of L over F.*

2 Roots of polynomials

Definition 2.0.44. *If $p(x) \in F[x]$, then an element a lying in some extension field of F is called root of $p(x)$ if $p(a) = 0$.*

Lemma 2.0.45. *If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$, $p(x) = (x-b)q(x) + p(b)$ where $q(x) \in K[x]$ and where $deg(q(x)) = deg(p(x)) - 1$.*

Proof. We can compute the Euclidean division of $p(x)$ by $(x-b)$ in the Euclidean ring $K[x]$, then $p(x) = (x-b)q(x) + r$, where $q(x) \in K[x]$ and $deq(q(x)) < deq(p(x))$, and $r = 0$ or $deg(r) < deg(x-b) = 1$. Thus either $r = 0$ or $deg(r) = 0$; in either cases $r \in K$. Thus, $p(b) = (b-b)q(b) + r = r$. □

Corollary 2.0.46. *If $a \in K$ is a root of $p(x) \in K[x]$, where $F \subset K$, then in $K[x]$, $(x-a)|p(x)$.*

Proof. We have that $p(x) = (x-a)q(x) + p(a)$ but we know that $p(a) = 0$, since a is a root of $p(x)$. Thus, $(x-a)|p(x)$ in $K[x]$. □

Definition 2.0.47. *The element $a \in K$ is a root of $p(x) \in F[x]$ of multiplicity m if $(x-a)^m|p(x)$, whereas $(x-a)^{m+1} \nmid p(x)$.*

We have a bound for the number of roots of a polynomial given by its degree. More precisely,

Lemma 2.0.48. *A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof. We proceed by induction on n, the degree of the polynomial $p(x)$. If $p(x)$ is of degree 1, then it must be of the form $\alpha x + \beta$, where α and β are in a field F with $\alpha \neq 0$. Thus, a root a of $p(x)$ is such that $p(a) = 0$, thus $a = -\beta/\alpha$ whence the conclusion of the lemma certainly holds in this case.
Assuming the result to be true in any field for all polynomials of degree less than n, let us suppose that $p(x)$ is of degree n over F. Let K be any extension of F. If $p(x)$ has no roots in K, then we are certainly done, for the number of roots in K, namely zero, is definitively at most n. So, suppose that $p(x)$ has at least one root $a \in K$, and that a has multiplicity m. Since $(x-a)^m|p(x)$, $m \leq n$ follows. Now $p(x) = (x-a)^m q(x)$, where $q(x) \in K[x]$ is of degree $n-m$. From the fact that $(x-a)^{m+1} \nmid p(x)$, we get that $(x-a) \nmid q(x)$, and by the previous corollary, a is not a root of $q(x)$. If $b \neq a$ is a root, in K, of $p(x)$, then $0 = p(b) = (b-a)^m q(b)$; however, since $b-a \neq 0$ and since we are in a field, we conclude that $q(b) = 0$. That is, any root of $p(x)$, in K, other than a, must be a root of $q(x)$. Since $q(x)$ is of degree $n-m < n$, by our induction hypothesis $q(x)$ has at most $n-m$ roots in K, which, together with the other root a, counted m times, tells us that $p(x)$ has at most $m + (n-m) = n$ roots in K. This completes the induction and proves the lemma. □

Remark III.4. *Commutativity is essential. If we consider the ring of real quaternion (i.e. $R =< i, j, k >$ where $i^2 = j^2 = k^2 = ijk = -1$), which falls short of being a field only in that it fails to be commutative, then the polynomial x^2+1 has at least 3 roots, i, j, k (in fact, it has an infinite number of roots). In a somewhat direction we need, even when the ring is commutative, that it be an integral domain, for if $ab = 0$ with $a \neq 0$ with $a \neq 0$ and $b \neq 0$ in the commutative ring R, then the polynomial ax of degree 1 over R has at least two distinct roots $x = 0$ and $x = b$ in R.*

Definition 2.0.49. *If $f(x) = \alpha_n x^n + \alpha_{n-1}x^{n-1} + ... + \alpha_1 x^1 + \alpha_0$ in $F[x]$, then the **derivative of** $f(x)$ written as $f'(x)$ is the polynomial $f'(x) = n\alpha_{n-1}x^{n-1} + (n-1)\alpha_{n-2}x^{n-2} + ... + \alpha_1$ in $F[x]$.*

Remark III.5. *Let F be a field of characteristic $p \neq 0$. In this case, the derivative of the polynomial x^p is $px^{p-1} = 0$. Thus the usual result from the calculus that a polynomial x^p is $px^{p-1} = 0$. Thus the usual result from the calculus that a polynomial whose derivative is 0 must be a constant no longer need hold true. However, if the characteristic of F is 0 and if $f'(x) = 0$ for $f(x) \in F[x]$, it is indeed true that $f(x) = \alpha \in F$. Even when the characteristic of F is $p \neq 0$, we can still describe the polynomials with zero derivative. (exercise!).*

It is easy to show that then

Lemma 2.0.50. *For any $f(x)$, $g(x) \in F[x]$ and any $\alpha \in F$,*

1. *$(f(x)+g(x))' = f'(x)+g'(x)$;*

2. *$(\alpha f(x))' = \alpha f'(x)$;*

3. *$(f(x)g(x))' = f'(x)g(x)+f(x)g'(x)$.*

Lemma 2.0.51. *The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial (that is, of positive degree) common factor.*

Proof. If $f(x)$ has a multiple root α, then $f(x) = (x-\alpha)^m q(x)$, where $m > 1$. However, as is easily computed, $((x-\alpha)^m)' = m(x-\alpha)^{m-1}$ whence by the previous lemma, $f'(x) = (x-\alpha)^m q'(x) + m(x-\alpha)^{m-1}q(x) = (x-\alpha)r(x)$, since $m > 1$. But this says that $f(x)$ and $f'(x)$ have the common factor $x-\alpha$, thereby proving the lemma in one direction.
On the other hand, suppose that $f(x)$ has no multiple root, then in the splitting field K of F, $f(x) = (x-\alpha_1)...(x-\alpha_r)$ where its root α_r are all distinct. But

$$f'(x) = \sum_{i=1}^{r}(x-\alpha_1)...\overline{(x-\alpha_i)}...(x-\alpha_r)$$

where $\overline{\cdot\cdot}$ denotes the term is omitted. No root of $f(x)$ is a root of $f'(x)$, indeed for any root of $f(x)$ α_i, we have that

$$f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j) \neq 0$$

since the roots are all distinct. However, if $f(x)$ and $f'(x)$ have a nontrivial common factor in F, they have a common root, namely, any root of this common factor. The net result is that $f(x)$ and $f'(x)$ have no nontrivial common factor, and so the lemma has been proved in the other direction. □

Corollary 2.0.52. *If $f(x)$ is irreducible, then*

1. *If the characteristic of F is 0, $f(x)$ has no multiple roots.*

2. *If the characteristic of F is $p \neq 0$, $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.*

Proof. Since $f(x)$ is irreducible, its only factors in $F[x]$ are 1 and $f(x)$. If $f(x)$ has a multiple root, then $f(x)$ and $f'(x)$ have a nontrivial common factor, hence $f(x)|f'(x)$. However, since the degree of $f'(x)$ is less than that of $f(x)$, then only possible way that this can happen is for $f'(x)$ to be 0. In characteristic 0, this implies that $f(x)$ is a constant, which has no roots; in characteristic $p \neq 0$, this forces $f(x) = g(x^p)$. □

Theorem III.6. *Let f be a non constant polynomial over the field F. Then there is an extension K/F and an element $a \in K$ such that $f(a) = 0$.*

Proof. Since f can be factored into irreducibles, we may assume without loss of generality that f itself is irreducible. The ideal $I =< f(X) >$ in $F[X]$ is maximal. Thus $K := F[X]/I$ is a field. Define a homomorphism $h : F \to K = F[X]/I$ by sending a to $a + I$; by the previous lemma h is a monomorphism, so we may identify F with a subfield of K. Now let $\alpha = X + I$; if $f(X) = \alpha_0 + \alpha_1 X + ... + \alpha_n X^n$, then

$$\begin{aligned} f(a) &= (\alpha_0 + I) + \alpha_1(X + I) + ... + \alpha_n(X + I)^n \\ &= (\alpha_0 + \alpha_1 X + ... + \alpha_n X^n) + I \\ &= f(X) + I \end{aligned}$$

which is zero in K. if a is not algebraic over F, then K is said to be an algebraic extension of f. (The extension K is sometimes said to be obtained from F by adjoining a root a of f.) □

Here further connection between roots and extensions.

Proposition 2.0.53. *Let f and g be polynomials over the field F. Then f and g are relatively prime if and only if f and g have no common root in any extension of F.*

Proof. If f and g are relatively prime, their greatest common divisor is 1, so there are polynomials $a(X)$ and $b(X)$ over F such that $a(X)f(X) + b(X)g(X) = 1$. If α is a common root of f and g, then the substitution of α for X yields $0 = 1$, a contradiction. Conversely, if the greatest common divisor $d(X)$ of $f(X)$ and $g(X)$ is non constant, let K be an extension of F in which $d(X)$ has a root α (by the previous theorem, it exists). Since $d(X)$ divides both $f(X)$ and $g(X)$, α is a common root of f and g in K. □

Corollary 2.0.54. *Let f and g are distinct monic irreducible polynomials over the field F. Then f and g have no common root in any extension of F.*

Proof. This follows directly by the previous proposition, since f and g are thus relatively prime. Indeed if h is a non constant divisor of the irreducible polynomials f and g then up to multiplication by constants, h coincides with both f and g, so that f is a constant multiple of g. This is impossible because f and g are monic and distinct. Thus f and g are relatively prime. □

3 Algebraic elements

Definition 3.0.55. *An element $a \in K$ is said to be* ***algebraic over*** *F if there exist elements α_0, α_1,...,$\alpha_n \in F$, not all 0, such that $\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$. In other words, $a \in K$ is algebraic over F if there is a nonzero polynomial $p(x) \in F[x]$ which a satisfies, that is, for which $p(a) = 0$. The monic polynomial of lowest positive degree satisfied by a is called the* ***minimal polynomial****, we write it as $min(\alpha, F)$. (A monic polynomial is a polynomial such that the highest power of x is 1.) If α is not algebraic over F, it is said to be* ***transcendental over*** *F. If every element of K is algebraic over F, then K is said to be* ***an algebraic extension of*** *F.*

Remark III.7. *Suppose that $a \in K$ is algebraic over F and let I be the set of all polynomials g over F such that $g(a) = 0$. If g_1 and g_2 belongs to I, so does $g_1 \pm g_2$, and if $g \in I$ and $c \in F[X]$, then $cg \in I$. Thus I is an ideal of $F[X]$ is a PID, I consist of all multiples of some $m(X)$ be monic, then $m(X)$ is unique. The polynomial $m(X)$ has the following properties:*

1. *If $g \in F[X]$, then $g(a) = 0$ if and only if $m(X)$ divides $g(X)$; Indeed, $g(\alpha) = 0$ if and only if $g(X) \in I = (m(X))$.*

2. *$m(X)$ is the monic polynomial of least degree such that $m(a) = 0$;*

3. *$m(X)$ is the unique monic irreducible polynomial such that $m(a) = 0$.Indeed, note that if $m(X) = h(X)k(X)$ with $deg(h(X))$ and $deg(k(X))$ less than $deg(m(X))$, then either $h(a) = 0$ or $k(a) = 0$, so that either $h(X)$ or $k(X)$ is a multiple of $m(X)$, which is impossible. Thus $m(X)$ is irreducible, and uniqueness of $m(X)$ follows from the lemma stating that two distinct monic irreducible polynomial have no common roots.*

It correspond to the minimal polynomial of a over F.

Definition 3.0.56. *An element $a \in K$ is said to be **algebraic of degree** n **over** F if $min(a, F)$ has degree n (that is a satisfies a nonzero polynomial over F of degree n but no nonzero polynomial of lower degree.)*

Remark III.8. *F is algebraic over F, any element of F is algebraic of degree 1 over F. Indeed, we can always consider the polynomial of degree 1 $x - a \in F[x]$, for any $a \in F$.*

Definition 3.0.57. *For $a \in K$. We denote $F(a)$ the smallest subfield of K containing both F and a, that is*

$$F(a) = \{f(a)/g(a) | f, g \in F[X] \text{ and } g(a) \neq 0\}$$

By induction, we can define $F(a_1, ..., a_n)$ for any a_1, a_2, ... $a_n \in K$.

Lemma 3.0.58. *If $a \in K$ is algebraic over F, and the minimal polynomial $m(X)$ of a has degree n, $F(a)$ corresponds to the set of polynomials in a with coefficients in F. We write $F[a]$ such a set instead of $F(a)$, in this case. More precisely, $F[a]$ correspond to the set $F_{n-1}[a]$ of all polynomial of degree at most $n-1$ with coefficient in F, and $1, a, ..., a^{n-1}$ form a basis for the vector space $F[a]$ over the field F. Consequently, $[F[a] : F] = n$.*

Proof. Let $f(X)$ be any nonzero polynomial over F of degree $n-1$ or less. Then since $m(X)$ is irreducible and $deg(f(X)) < deg(m(X))$ and $m(X)$ are relatively prime, there are polynomials $c(X)$ and $b(X)$ over F such that $c(X)f(X) + b(X)m(X) = 1$. But then $c(a)f(a) = 1$, so that any nonzero element of $F_{n-1}[a]$ has a multiplicative inverse. It follows that $F_{n-1}[a]$ is a field. (This may not be obvious, since the product of two polynomials of degree $n-1$ or less can have degree greater than $n-1$ but if $deg(g(X)) > n-1$, then divide $g(X)$ by $m(X)$ to get $g(X) = q(X)m(X) + r(X)$ where $deg(r(X)) < deg(m(X)) = n$. Replace X by a to get $g(a) = r(a) \in F_{n-1}[a]$. Less abstractly, if $m(a) = a^3 + a + 1 = 0$, then $a^3 = -a - 1$, $a^4 = -a^2 - a$, and so on.

Now any field containing F and a must contain all polynomials in a, in particular all polynomials of degree at most $n-1$. Therefore, $F_{n-1}[a] \subseteq F[a] \subseteq F(a)$. But $F(a)$ is the smallest field containing F and a, so $F(a) \subseteq F_{n-1}[a]$, and we conclude that $F(a) = F[a] = F_{n-1}[a]$. Finally, the elements $1, a, ..., a^{n-1}$ certainly span $F_{n-1}[a]$, and they are linearly independent because if a nontrivial linear combination of these elements were zero, we would have a nonzero polynomial of degree less than that of $m(X)$ with a as a root. □

Theorem 3.0.59. *The element $a \in K$ is algebraic if and only if $F(a)$ is a finite extension of F.*

Proof. Suppose that $F(a)$ is a finite extension of F and that $[F(a) : F] = m$. Consider the elements 1, a, ..., a^m; they are all in $F(a)$ and are $m+1$ in number. So they are linearly dependent over F. So, there are elements α_0, α_1,..., α_m in F, not all 0, such that $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + ... + \alpha_m a^m = 0$. Hence a is algebraic over F.
The converse is proven by the previous lemma. □

Theorem III.9. *If K is a finite extension of F, then K is an algebraic extension of F.*

Proof. Let $a \in K$ and let $n = [K : F]$. Then $1, a, a^2, ..., a^n$ are $n+1$ vectors in an n-dimensional vector space, so they must be linearly dependent. Thus a is a root of a nonzero polynomial with coefficients in F, which means that a is algebraic over F. □

Corollary 3.0.60. *If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*

Proof. Let u be any arbitrary element of L. Since L is algebraic over K, then there is a polynomial satisfied by u, i.e $\sigma_0 + ...\sigma_m u^m = 0$. Consider now the field extension $M = F(\sigma_0, ..., \sigma_m)$ is a finite extension of F since each σ_i is algebraic over F. But u is of course also algebraic over M since it is algebraic over F. Thus $M(u)$ is a finite extension of F. But this implies that u is algebraic over M. However, $[M(u) : F] = [M(u) : M][M : F]$, whence $M(u)$ is a finite extension of F. But this implies that u is algebraic over F. □

Theorem III.10. *If a, b in K are algebraic over F then $a \pm b$, ab and a/b (if $b \neq 0$) are all algebraic over F. In other words, the elements in $K*$ which are algebraic over F form a subfield of K.*

Proof. Suppose that a is algebraic of degree m over F while b is algebraic of degree n over F. Thus $[F(a) : K]$ is of degree m over F. Now b is algebraic of degree n over K, a fortiori it is algebraic of degree at most n over $F(a)$ which contains F. Thus the subfield $F(a, b)$ of K is of degree at most n over $F(a)$.But $[F(a, b), F(a)][F(a) : F] = [F(a, b) : F]$; therefore $[W : F] \leq mn$ and so W is a finite extension of F. However, a and b are both in $F(a, b)$, whence all of $a \pm b$, ab, a/b are in $F(a, b)$. Since $[F(a, b) : F]$ is finite, these elements must be algebraic over F. □

Remark III.11. *If a and b in K are algebraic over F of degree m and n, respectively, then $a \pm b$, ab and a/b (if $b \neq 0$) are algebraic over F of degree at most mn.*

When we work over the rationals some interesting result can be proved. We have the following definitions:

Definition 3.0.61. *A complex number is said to be an **algebraic number** if it is algebraic over the field of rational numbers. A complex number which is not algebraic is called **transcendental**. An algebraic number a is said to be an **algebraic integer** if it satisfies an equation of the form* $a^m + \alpha_1 a^{m-1} + ... + \alpha_m = 0$ *where* $\alpha_1, ..., \alpha_m$ *are integers.*

Lemma 3.0.62. *Let* $f(x)$ *to be the polynomial*

$$f(x) = \frac{1}{(p-1)!} x^{p-1}(1-x)^p ...(n-x)^p$$

where p is a prime number such that $p > n$. *Consider* $F(x) = f(x) + ... + f^{((n+1)p-1))}(x)$ *where* $f^{(i)}(x)$ *is the* i^{th} *derivative of* $f(x)$ *with respect to* x. *Then*

1. *for any* $j \in \{1, ...n\}$, $F(j) - e^j F(j-1) = -e^{(1-\theta_j)} f(\theta_j) = \epsilon_j$ *where* θ_j *is some real number between* 0 *and* 1. *Moreover,* $\epsilon_j \to 0$ *when* $p \to \infty$.

2. $f^{(i)}(x)$ *is a polynomial with coefficients which are integers all of which are multiples of* p*, for any* $i \geq p$.

3. $F(j)$ *is an integer and is a multiple of* p*, for* $j = 1, 2, ..., n$ *and* $F(0)$ *is an integer not divisible by* p.

Proof.

1. Since $f^{((n+1)p))}(x) = 0$, then $d/dx(e^{-x}F(x)) = -e^{-xf(x)}$. Then we apply to $g(x) = e^{-x}F(x)$ continuously differentiable, single-valued function on the closed interval $[x_1, x_2]$ the formula
$$\frac{g(x_1) - g(x_2)}{x_1 - x_2} = g^{(1)}(x_1 + \theta(x_2 - x_1))$$
where $0 < \theta < 1$.
We have
$$\epsilon_j = \frac{-e^{j(1-\theta_j)}(1 - j\theta_j)^p ...(n - j\theta_j)^p (j\theta_j)^{p-1} j}{(p-1)!}$$
with $0 < \theta_i < 1$. Thus
$$|\epsilon_i| \leq e^n \frac{n^p (n!)^p}{(p-1)!} \to 0$$
when $p \to \infty$. (Use induction on n).

2. Use a induction on n.

3. $f(x)$ has a root of multiplicity p at $x = 1, 2, ..., n$. Thus for $j = 1, 2..., n$, $f(j) = 0$, ... , $f^{(p-1)}(j) = 0$. Then $F(j) = 0 + \sum_{i=p+1}^{((n+1)p-1)} f^{(i)}(j)$. Thus by 2., $F(j)$ is an integer and is a multiple of p. 0 is a root of $f(x)$ of multiplicity $p - 1$. $f(0) = ... = f^{(p-1)}(0) = 0$. For $i \geq p$, $f^{(i)}(0)$ is an integer divisible by p and $f^{(p)}(0) = (n!)^p$ and since $p > n$ and is a prime number, so $p \nmid (n!)^p$ so that $f^{(p-1)}(0)$ is an integer not divisible by p. Since $F(0) = f(0) + f^{(1)}(0) + ... + f^{(p-1)}(0) + f^{(p)}(0) + ... + f^{((n+1)p-1)}(0)$, we conclude that $F(0)$ is an integer not divisible by p.

□

Theorem III.12. *The number e is transcendental.*

Proof. Suppose now that e is an algebraic number; then it satisfies some relation of the form

$$c_n e^n + c_{n-1}e^{n-1} + ... + c_1 e^1 + c_0 = 0,$$

where c_0, c_1, ..., c_n are integers and where $c_0 > 0$. Multiplying, the equalities of the previous lemma 1. by c_j and adding these up we get

$$c_1 F(1) + ... + c_n F(n) - F(0)(c_1 e + ... + c_n e^n) = c_1\epsilon_1 + ... + c_n\epsilon_n$$

But since the $\epsilon_j \to 0$ when $p \to \infty$. We can take a prime p larger than both n and c_0 and large enough to force $|c_1\epsilon_1 + ... + c_n\epsilon_n| < 1$. But $c_1\epsilon_1 + ... + c_n\epsilon_n = c_0 F(0) + ... + c_n F(n)$ must be an integer; since it is strictly smaller than 1, then $c_1\epsilon_1 + ... + c_n\epsilon_n = 0$; this however is sheer nonsense, since we have that $p \nmid (c_0 F(0) + ... + c_n F(n))$; whereas $p|0$. This contradiction, stemming from the assumption that e is algebraic, proves that e must be transcendental. □

4 Splitting field

We are able now to precise more one of a result that we obtained previously:

Theorem III.13. *if $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F, such that $[E : F] = n$, in which $p(x)$ has a root.*

Proof. Let $F[x]$ be the ring of polynomials in x over F and let $V = (p(x))$ be the ideal of $F[x]$ generated by $p(x)$. Since $p(x)$ is irreducible then V is a maximal ideal and $E = F[x]/V$ is a field. This E will be shown to satisfy the conclusions of the theorem.
As we have already seen we have an embedding $F \hookrightarrow E$, which permits to see E as an extension of F. Finally, E is a extension of degree n since $1 + V$, $x + V$, ... , $x^{n-1} + V$ form a basis of E over F. (Prove!). □

Corollary 4.0.63. *If $f(x) \in F[x]$, then there is a finite extension E of F in which $f(x)$ has a root. Moreover, $[E : F] \leq deg(f(x))$.*

More generally, we can construct a field containing all the roots:

Theorem 4.0.64. *Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then there is an extension E of F of degree at most $n!$ in which $f(x)$ has its n roots (A root of multiplicity m is counted as m roots).*

Proof. By the above corollary, there is an extension E_0 of F with $[E_0 : F] \leq n$ in which $f(x)$ has a root α. Thus in $E_0[x]$, $f(x)$ factors as $f(x) = (x - \alpha)q(x)$, where $q(x)$ is of degree $n - 1$. Using induction (or continuing the above process), there is an extension E of E_0 of degree at most $(n-1)!$ in which $q(x)$ has $n - 1$ roots. Since any root of $f(x)$ is either α or a root of $q(x)$, we obtain in E all n roots of $f(x)$. Now, $[E : F] = [E : E_0][E_0 : F] \leq (n-1)!n = n!$. □

Definition 4.0.65. *If $f(x) \in F[x]$, a finite extension E of F is said to be a* ***splitting field over*** *F* ***for*** *$f(x)$ if over E (that is, in $E[x]$), but not over any proper subfield of E, $f(x)$ can be factorized as a product of linear factors. In other words, E is a splitting field of $f(x)$ over F if E is a minimal extension of F in which $f(x)$ has n roots, where $n = deg(f(x))$.*

Remark III.14. *1. The previous theorem guarantees the existence of splitting fields.*

2. Given n, we can always construct a polynomial of degree n such that the splitting field in equal to $n!$.

In the following, we consider two isomorphic field and denote by τ an isomorphism of F to F'. For convenience, let us denote the image of any $\alpha \in F$ under τ by α'; that is $\tau(\alpha) = \alpha'$. This isomorphism induce an isomorphism that we denote τ^* between $F[x]$ and $F'[t]$ the ring of the polynomials on the indeterminate x (resp. t) over F (resp. F') sending a polynomial $f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n \in F[x]$ to $\tau^*(f(x)) = \alpha'_0 + \alpha'_1 t + ... + \alpha'_n t^n \in F'[t]$, again we will denote $\tau^*(f(x))$ by $f'(x)$. This implies immediately that the factorizations of $f(x)$ in $F[x]$ result in like factorizations of $f'(t)$ in $F'[t]$ and vice versa. In particular, $f(x)$ is irreducible in $F[x]$ if and only if $f'(t)$ is irreducible in $F'[t]$.

Lemma 4.0.66. *There is an isomorphism τ^{**} of $F[x]/(f(x))$ onto $F'[t]/(f'(t))$ with the property that for every $\alpha \in F$, $\tau^{**}(\alpha) = \alpha'$ and $\tau^{**}(x + (f(x))) = t + (f'(t))$. In other work, τ^{**} send $g(x) + (f(x))$ to $g'(t) + (f'(t))$, for every $g(x) \in F[x]$.*

The proof is left as exercise. We wish to prove the uniqueness of splitting fields. We have the following theorem.

Theorem III.15. *If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this isomorphism σ can be chosen that*

1. $\sigma(v) = w$.

2. $\sigma(\alpha) = \alpha'$, for every $\alpha \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension K of F. Let $M = \{f(x) \in F[x] | f(v) = 0\}$. Trivially M is an ideal of $F[x]$ and $M \neq F[x]$. Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$. We can then prove that there is an isomorphism ψ^* from $F[x]/(p(x))$ to $F(v)$ leaving every element of F fixed and with the property that $v = \psi^*(x + (p(x)))$. Since $p(x)$ is irreducible in $F[x]$, $p'(t)$ is irreducible in $F'[t]$, and there is an isomorphism θ^* of $F'[t]/(p'(t))$ onto $F'(w)$ where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $\theta^*(t + (p'(t))) = w$.
We know also that there is an isomorphism τ^{**} of $F[x]/(p(x))$ onto $F'[t]/(p'(t))$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$. The mapping $\sigma = (\psi^*)^{-1}\tau^{**}\theta^* : F(v) \to F[x]/(p(x)) \to F'[t]/(p'(t)) \to F'(w)$ is an isomorphism satisfying the requirement of the isomorphism in the statement of the theorem. □

Corollary 4.0.67. *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphism to $F(b)$ by an isomorphism which takes a onto b and which leaves every element of F fixed.*

Theorem III.16. *Any splitting fields E and E' of the polynomials $f(x) \in F[x]$ and $f'(t) \in F'[t]$, respectively are isomorphic by an isomorphism ϕ with the property that $\phi(\alpha) = \alpha'$ for every $\alpha \in F$. (In particular, any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.)*

Proof. We argue by induction on the degree $[E : F]$ of the splitting field.
If $[E : F] = 1$, then $E = F$, whence $f(x)$ splits into a product of linear factors over F itself but then $f'(t)$ splits over F' into a product of linear factors, hence $E' = F'$. But then $\phi = \tau$ provides us with an isomorphism of E onto E' coinciding with τ on F.
Assume the result to be true for any field F_0 and any polynomial $f(x) \in F_0[x]$ provided the degree of some splitting field E_0 of $f(x)$ has degree less than n over F_0, that is, $[E_0 : F_0] < n$. Suppose that $[E : F] = n > 1$, where E is a splitting field of $f(x)$ over F. Since $n > 1$, $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$. Let $p'(t)$ be the corresponding irreducible factor of $f'(t)$. Since E splits $f(x)$, a full complement of roots of $f(x)$, and so, a priori, of roots of $p(x)$, are in E. Thus there is a $v \in E$ such that $p(v) = 0$; thus $[F(v) : F] = r$. Similarly, there is a $w \in E'$ such that $p'(w) = 0$. By the previous theorem; there is an isomorphism σ of $F(v)$ onto $F'(w)$ with the property that $\sigma(\alpha) = \alpha'$, for every $\alpha \in F$.
Since $[F(v) : F] = r > 1$,

$$[E : F(v)] = [E : F]/[F(v) : F] = n/r < n$$

We claim that E is a splitting field for $f(x)$ considered as polynomial over $F_0 = F(v)$, for no subfield of E, containing F_0 and hence F, can split $f(x)$, since E is assumed to be a splitting field for $f(x)$ considered as a polynomial over $F_0 = F(v)$, for no subfield of E, containing F_0 and hence F, can split $f(x)$, since E is assumed to be a splitting field of $f(x)$ over F. Similarly E' is a splitting field for $f'(t)$ over $F'_0 = F'(w)$. By our induction hypothesis there is an isomorphism ϕ of E onto E' such that $\phi(a) = \sigma(a)$ for all $a \in F_0$. But for every $\alpha \in F$, $\sigma(\alpha) = \alpha'$ hence for every $\alpha \in F \subset F_0$, $\phi(\alpha) = \alpha'$. This complete the proof by induction. □

Remark III.17. *Any two splitting fields of the same polynomial over F are isomorphic and by an isomorphism leaving every element of F fixed, we are justified of speaking about "the" splitting field, rather than a splitting field, for it is essentially unique.*

Example 4.0.68.

1. *Let F be any field and let $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$, be in $F[x]$. If K is any extension of F in which $p(x)$ has a root, a, then the element $b = -\alpha - a$ also in K is also a root of $p(x)$. If $b = a$ it is easy to check that $p(x)$ must then be $p(x) = (x - a)^2$, and so both roots of $p(x)$ are in K. If $b \neq a$, then be $p(x) = (x - a)^2$, and so both roots of $p(x)$ are in K. If $b \neq a$ then again both roots of $p(x)$ are in K. Consequently, $p(x)$ can be split by an extension of degree 2 of F.*

2. *Let F be the field of rational numbers and let $f(x) = x^3 - 2$. in the field of complex numbers the three roots of $f(x)$ are ${}^3\sqrt{2}$, $\omega^3\sqrt{2}$, $\omega^{23}\sqrt{2}$, where $\omega = (-1 + \sqrt{3}i)/2$ and where ${}^3\sqrt{2}$ is a real cube root of 2. Now $F({}^3\sqrt{2})$ cannot split $x^3 - 2$, for, as a subfield of the real field, it cannot contain the complex, but not real, number $\omega^3\sqrt{2}$. Without explicitly determining it, what can we say about E, the splitting field of $x^3 - 2$ over F? We know that $[E : F] \leq 3! = 6$; by the above remark, since $x^3 - 2$ is irreducible over F and since $[F({}^3\sqrt{2}) : F] = 3$. The only way out is $[E : F] = 6$. We could, of course, get this result by making two extensions $F_1 = F({}^3\sqrt{2})$ and $E = F_1(\omega)$ and showing that ω satisfies an irreducible quadratic equation over F_1.*

3. *Let F be the field of rational numbers and let*

$$f(x) = x^4 + x^2 + 1 \in F[x].$$

We claim that $E = F(\omega)$ where $\omega = (-1+\sqrt{3}i)/2$ is a splitting field of $f(x)$. Thus $[E:F] = 2$, far short of the maximum possible $4! = 24$.

5 Construction with straightedge and compass

Definition 5.0.69. *A real number α is said to be a* ***constructible number*** *if by the use of straightedge and compass alone we can construct a line segment of length α. We assume that we are given some fundamental unit length.*

Recall that from high-school geometry, we can construct with a straightedge and compass a line perpendicular to and a line parallel to a given line through a given point. From this it is easy exercise to prove that if α and β are constructible number then so are $\alpha \pm \beta$, $\alpha\beta$ and when $\beta \neq 0$, α/β (Exercise!). Therefore the set of constructible numbers form a subfield, W, of the field of real numbers. In particular, since $1 \in W$ must contain $\mathbb{Q}$, the field of rational numbers. We wish to study the relation of W to the rational field. If $w \in W$, we can reach w from the rational field by a finite number of constructions.

Definition 5.0.70. *Let F be any subfield of the field of the real numbers. Consider all the points (x, y) in the real eucliedean plane both of whose coordinates x and y are in F; we call the set of these point the* ***plane*** *of F.*

In order to see the structure of the constructible number, we consider which construction In the plane of a field, we can consider straight line and circle:

1. Any straight line joining two points in the plane of F has an equation of the form $ax + by + c = 0$ where a, b, c are all in F (Exercise!).

2. Moreover, any circle having as center a point in the plane of F and having as radius an element of F has an equation of the form $x^2 + y^2 + ax + by + c = 0$, where all of a, b, c are in F (Exercise!).

Let's see now the behavior of their intersection:

1. Given two line in F which intersect in the real plane, the their intersection point is a point in the plane of F (Exercise!).

2. The intersection of a line in F and a circle in F need not yield a point in the plane of F. But, using the fact that the equation of a line in F is of the form $ax + by + c = 0$ and that the equation of a circle in F is of the form $x^2 + y^2 + dx + ey + f = 0$, where a, b, c, d, e, f are all in F, we can show that when a line and a circle of F intersect in the real plane, they intersect either in a point in the plane of F or in the plane of $F(\sqrt{\gamma})$, for some positive γ in F (Exercise!).

3. The intersection of two circles in F can be realized as that of a line in F and a circle in F, for if these two circles are $x^2+y^2+a_1x+a_2y+c_1=0$ and $x^2+y^2+a_2x+b_2y+c_2=0$, then their intersection is the intersection of either of these with the line $(a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0$, so also yields a point either in the plane F or of $F(\sqrt{\gamma})$ for some positive γ in F.

As a consequence of all this, lines and circles of F lead us to points either in F or in quadratic extension of F. If we now are in $F(\sqrt{\gamma_1})$ for some quadratic extension of F. If we now are in $F(\sqrt{\gamma_1})$ for some quadratic extension of F, the lines and circles in $F(\sqrt{\gamma_1})$ intersect in points in the plane of $F(\sqrt{\gamma_1},\sqrt{\gamma_2})$ where γ_2 is a positive number in $F(\sqrt{\gamma_1})$. A point is constructible from F if we can find real numbers $\lambda_1,\ldots,\lambda_n$, such that $\lambda_1^2\in F$, $\lambda_2^2\in F(\lambda_1)$, $\lambda_3^2\in F(\lambda_1,\lambda_2)$, ..., $\lambda_n^2\in F(\lambda_1,...,\lambda_{n-1})$, such that the point is in the plane of $F(\lambda_1,...,\lambda_n)$.
Conversely, if $\gamma\in F$ is such that $\sqrt{\gamma}$ is real then we can realize γ as an intersection of lines and circles in F (Exercise!). Thus, a point is constructible from F if and only if we can find a finite number of real numbers λ_1, ..., λ_n such that

1. $[F(\lambda_1):F]=1$ or 2;

2. $[F(\lambda_1,...,\lambda_i):F(\lambda_1,...,\lambda_{i-1}]=1$ or 2 for $i=1,2,....,n$;

and such a point lies in the plane of $F(\lambda_1,...,\lambda_n)$.
Then we have,

Theorem III.18. *The real number α is constructible if and only if we can find a finite number of real numbers $\lambda_1,\ldots,\lambda_n$ such that*

1. $\lambda_1^2\in\mathbb{Q}$,

2. $\lambda_1^2\in\mathbb{Q}(\lambda_1,...,\lambda_{i-1})$*, for* $i=1,2,...,n$,

such that $\alpha\in\mathbb{Q}(\lambda_1,...,\lambda_n)$.

Proof. We have defined a real number α to be constructible if by use of straightedge and compass we can construct a line segment of length α. But this translates, in terms of the discussion above, into: α is constructible if starting from the plane of the rational numbers, $\mathbb{Q}$, we can imbed α in a field obtained from $\mathbb{Q}$ by a finite number of quadratic extensions. □

Corollary 5.0.71. *If α is constructible then α lies in some extension of the rationals of degree a power of* 2.

Proof. We can compute the degree of $\mathbb{Q}(\lambda_1,...,\lambda_n)$ over $\mathbb{Q}$, by the previous theorem,

$$[\mathbb{Q}(\lambda_1,...,\lambda_n),\mathbb{Q}]=[\mathbb{Q}(\lambda_1,...,\lambda_n):\mathbb{Q}(\lambda_1,...,\lambda_{n-1})]\times[\mathbb{Q}(\lambda_1,...,\lambda_{n-1}):\mathbb{Q}(\lambda_1,...,\lambda_{n-2})]\times....\times[\mathbb{Q}(\lambda_1):\mathbb{Q}]$$

Each term of the product is either 1 or 2, we get that

$$[\mathbb{Q}(\lambda_1,...,\lambda_n),\mathbb{Q}]=2^r$$

□

We get then a important criterion for non constructibility,

Corollary 5.0.72. *If the real number α satisfies an irreducible polynomial over the field of rational number of degree k, and if k is not a power of* 2*, then α is not constructible.*

Proof. If α is constructible, by the corollary above, there is a subfield K of the real field such that $\alpha \in K$ and such that $[K:\mathbb{Q}] = 2^r$. however, $\mathbb{Q}(\alpha) \subset K$, whence $[\mathbb{Q}(\alpha):\mathbb{Q}]|[K:\mathbb{Q}] = 2^r$; thereby $[\mathbb{Q}(\alpha),\mathbb{Q}]$ is also a power of 2. However, if α satisfies an irreducible polynomial of degree k over $\mathbb{Q}$, we have proved that $[\mathbb{Q}(\alpha):\mathbb{Q}] = k$. □

The last corollary enables us to settle the ancient problem of trisecting an angle by straightedge and compass alone, for we prove:

Theorem III.19. *It is impossible, by straightedge and compass alone, to trisect* 60ř.

Proof. If we could trisect 60° by straightedge and compass alone, then the length $\alpha = cos(20°)$ would be constructible. At this point, let us recall the identity $\alpha = cos(20°)$ would be constructble. At this point, let us recall the identity $cos(3\theta) = 4cos^3(\theta) - 3cos(\theta)$. Putting $\theta = 20°$ and remembering that $cos(60°) = 1/2$, we obtain $4\alpha^3 - 3\alpha = 1/2$, whence $8\alpha^3 - 6\alpha - 1 = 0$. Thus α is a root of the polynomial $8x^3 - 6x - 1$ over the rational field. However, this polynomial is irreducible over the rational field (Exercise!) and since its degree is 3, which is not a power of 2, thus not constructible. Hence, 60° cannot be trisected by straightedge and compass. □

Another ancient problem is that of duplicating the cube, that is, of constructing a cube whose volume is twice that of a given cube.

Theorem III.20. *By straightedge and compass it is impossible to duplicate the cube.*

Proof. If the original cube is the unit cube, this entails constructing a length α such that $\alpha^3 = 2$. Since the polynomial $x^3 - 2$ is irreducible over the rationals (Exercise!), again α is not constructble. □

We wish to exhibit yet another geometric figure which cannot be constructed by straightedge and compass, namely, the regular septagon.

Theorem III.21. *It is impossible to construct a regular septagon by straightedge and compass.*

Proof. To carry out such a construction would require the constructibility of $\alpha = 2cos(2\pi/7)$. However, we claim that α satisfies $x^3 + x^2 - 2x - 1$ (Exercise!) and that this polynomial is irreducible over the files of rational number (Exercise!), thus α is not constructible. □

6 Finite field

Definition 6.0.73. *We say that a field is a **finite field** if it has a finite number of elements.*

Lemma 6.0.74. *Let F be a finite field with q elements and suppose that $F \subset K$ where K is also a finite field. Then K has q^n elements where $n = [K:F]$.*

Proof. K is a vector space over F and since K is finite it is certainly finite dimensional as a vector space over F. Suppose that $[K : F] = n$; then K has a basis of n element in K has a unique representation in the form $\alpha_1 v_1 + ... + \alpha_n v_n$ where $\alpha_n v_n$ where $\alpha_1, ..., \alpha_n$ are all in F. Thus the number of elements in K is the number of $\alpha_1 v_1 + ... + \alpha_n v_n$ as the α_1, ..., α_n range over F. Since each coefficient can have q values K must clearly have q^n elements. □

Corollary 6.0.75. *Let F be a finite field; then F has p^m elements where the prime number p is the characteristic of F.*

Proof. Since F be a finite number of elements, we know that $f.1 = 0$ whee f is the number of elements in F. Thus F has characteristic p for some prime number p. Therefore F contains a field isomorphic to $F_p := \mathbb{Z}/p\mathbb{Z}$. Since F_p has p elements, F has p^m elements where $m = [F : F_p]$ by the previous lemma. □

Corollary 6.0.76. *If the finite field F has p^m elements then every $a \in F$ satisfies $a^{p^m} = a$.*

Proof. If $a = 0$ the assertion is trivial. On other hand, the nonzero elements of F form a group under the multiplication of order $p^m - 1$ thus by Lagrange's theorem $a^{p^m - 1} = 1$ for all $a \neq 0$ in F. Multiplying this relation by a we obtain that $a^{p^m} = a$. □

From this last corollary we can easily pass to

Lemma 6.0.77. *If the finite field F has p^m elements then the polynomial $x^{p^m} - x$ in $F[x]$ factor in $F[x]$ as*

$$x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$$

Proof. We have proven that the polynomial $x^{p^m} - x$ being a polynomial of degree p^m has at most p^m roots in F. However, by the previous corollary we know p^m such a roots, namely all the element of F. Thus, we can conclude that $x^{p^m} - x = \prod_{\lambda \in F}(x - \lambda)$. □

Corollary 6.0.78. *If the field F has p^m elements then F is the splitting field of the polynomial $x^{p^m} - x$.*

Proof. We already know that $x^{p^m} - x$ certainly splits in F. However, it cannot split in any smaller field for that field would have to have all the roots of this polynomial and so would have to have at least p^m elements. Thus F is the splitting field of $x^{p^m} - x$. □

We have proven that any two splitting fields over a given field of a given polynomial are isomorphic. Thus, we have the following result:

Lemma 6.0.79. *Any two finite fields having the same number of elements are isomorphic.*

Proof. If these fields have p^m elements, by the above corollary they are both splitting fields of the polynomial $x^{p^m} - x$ over $F_p = \mathbb{Z}/p\mathbb{Z}$ whence they are isomorphic. □

Thus for any integer m and any prime number p there is, up to isomorphism, at most one field having p^m elements. We want now to know if for any prime p and any integer m there is a field gavin p^m elements. When this is done we shall know that there is exactly one field having p^m elements where p is an arbitrary prime and m an arbitrary integer. For this recall that in elementary calculus the equivalence is shown between the existence of multiple root of a function and the simultaneous vanishing of the function and its derivative at a given point. Even in our setting, where F is an arbitrary field such an interrelation exists.

Corollary 6.0.80. *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$, has distinct roots.*

Proof. The derivative of $x^{p^n} - x$ is $p^n x^{p^{n-1}} - 1 = -1$, since F is of characteristic p. Therefore, $x^{p^n} - x$ and its derivative are certainly relatively prime, which, by Corollary 2.0.51, implies that $x^{p^n} - x$ has no multiple roots. □

Lemma 6.0.81. *For every prime number p and every positive integer m there exists a field having p^m elements.*

Proof. Consider the polynomial $x^{p^m} - x$ in $F_p[x]$, the ring of polynomials in x over F_p, the field of integers mop p. Let K be the splitting field of this polynomial. In K, let $F = \{a \in K | a^{p^m} = a\}$. The elements of F are thus the roots of $x^{p^n} - x$, which are distinct by the previous corollary; whence F has p^m elements. We now claim that F is a field. If a, $b \in F$ since the characteristic is p, $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m} = a \pm b$, hence $a \pm b \in F$. Consequently F is a subfield of K and so is a field. Having exhibited the field F having p^m elements we have proved the lemma. □

As a consequence,

Theorem III.22. *For every prime number p and every positive integer m there is a unique field having p^m elements.*

Lemma 6.0.82. *Let G be a finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by at most n elements of G, for every integer n. Then G is a cyclic group.*

Proof. If the order of G is a power of some prime number q then the result is very easy. For suppose that $a \in G$ is an element whose order is as large as possible; its order must be q^r for some integer r. The elements e, a, a^2, ... , $a^{q^r - 1}$ give us q^r distinct solutions of the equation $x^{q^r} = e$, which, by our hypothesis, implies that these are all the solution of this equation. Now, if $b \in G$ its order is q^s where $s \leq r$, hence $b^{q^r} = (b^{q^s})^{q^{r-s}} = e$. By the observation made above this forces $b = a^i$ for some i, and so G is cyclic.
The general finite abelian group can be realize as $G = S_{q_1} ... S_{q_k}$ where q_i are the distinct prime divisors of $o(G)$ and where the S_{q_i} are the Sylow subgroups of G. Moreover, every element $g \in G$ can be written in a unique way as $g = s_1 ... s_k$ where $s_i \in S_{q_i}$ is one of $x^n = e$ in G so that each S_{q_i} inherits the hypothesis we have imposed on G. By the remarks of the first paragraph of the proof, each S_{q_i} is a cyclic group; let a_i be a generator of S_{q_i}. We claim that $c = a_1 .... a_k$ is a cyclic generator of G. To verify this all we must do is prove that $o(G)$

divides m, the order of c. Since $c^m = e$, we have that $a_1^m a_2^m ... a_k^m = e$. By the uniqueness of representation of an element of G as a product of elements in the S_{q_i}, we conclude that each $a_i^m = e$. Thus $o(S_{q_i})|m$, for every i. Thus $o(G) = o(S_{q_1})...o(S_{q_k})|m$. However, $m|o(G)$ and so $o(G) = m$. This proves that G is cyclic. □

Lemma 6.0.83. *Let K be a field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.*

Proof. Since K is a field, any polynomial of degree n in $K[x]$ has at most n roots in K. Thus in particular, for any integer n, the polynomial $x^n - 1$ has at most n roots in K, and all the more so, at most n roots in G. The hypothesis of the lemma is satisfied, so G is cyclic. □

Theorem III.23. *The multiplicative group of nonzero elements of a finite field is cyclic.*

Proof. Let F be a finite field. We apply the previous lemma with $F = K$ and $G =$ the group of the nonzero elements of F. □

Lemma 6.0.84. *If F is a finite field and $\alpha \neq 0$, $\beta \neq 0$ are two elements of F then we can find elements a and b in F such that* $1 + \alpha a^2 + \beta b^2 = 0$.

Proof. If the characteristic of F is 2, F has 2^n elements and every element x in F satisfies $x^{2^n} = x$. Thus every element in F is a square. In particular $\alpha^{-1} = a^2$ for some $a \in F$. Using this a and $b = 0$, we have $1 + \alpha a^2 + \beta b^2 = 1\alpha\alpha^{-1} + 0 = 1 + 1 = 0$, the last equality being a consequence of the fact that the characteristic of F is 2.
If the characteristic of F is an odd prime p, F has p^n elements. Let $W_\alpha = \{1 + \alpha x^2 | x \in F\}$. We must check how often $1+\alpha x^2 = 1+\alpha y^2$. But this relation forces $\alpha x^2 = \alpha y^2$ and so, since $\alpha \neq 0$, $x^2 = y^2$. Finally, this leads to $x = \pm y$. Thus for we get $1 \in W_\alpha$. Thus W_α has $1 + (p^n - 1)/2 = (p^n + 1)/2$ elements. Similarly, $W_\beta = \{-\beta x^2 | x \in F\}$ has $(p^n + 1)/2$ elements. The intersection is thus nonempty since sum of their cardinality is $p^n + 1$. Let $c \in W_\alpha \cap W_\beta$. Since $c \in W_\alpha$, $c = 1+\alpha a^2$, for some $a \in F$; since $c \in W_\beta$, $c = -\beta b^2$ for some $b \in F$. Therefore, $1+\alpha a^2 = -\beta b^2$, which, on transposing yields the desired result $1 + \alpha a^2 + \beta b^2 = 0$. □

Chapter IV

Galois theory

(Notes of Joel Spencer) Galois Theory involves the study of arbitrary fields and fields can come in many different guises. However, throughout these notes we shall restrict ourselves to fields whose elements are complex numbers. That is, all of our fields F (even when we forget to mention it!) will have $F \subset \mathbb{C}$.

1 Galois Basics

Definition 1.0.85. *Let $F \subset K, K'$, all fields. We say $\sigma : K \to K'$ is an isomorphism* over *F if*

1. *σ is a bijection from K to K'*
2. *$\sigma(a+b) = \sigma(a) + \sigma(b)$ for all $a, b \in K$*
3. *$\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in K$*
4. *$\sigma(c) = c$ for all $c \in F$*

We say that the elements of F are fixed by σ. The most important case is when $K = K'$.

Remark IV.1. *However, that it is acceptible that other elements (not in F) are also fixed by σ.*

Now we come to the object of study.

Definition 1. *Let $F \subset K$, both fields. We define the **Galois Group of** K **over** F, denote $Gal(K,F)$ as follows. The elements are all of the automorphims of K over F. The group operation is the composition of automorphism. That is, given two automorphisms σ, τ we define their product $\sigma\tau$ by*

$$(\sigma\tau)(a) = \tau(\sigma(a)) \tag{IV.1}$$

We define the inverse σ^{-1} by

$$(\sigma^{-1})(b) \text{ is that } a \text{ such that } \sigma(a) = b \tag{IV.2}$$

It is not hard to prove that $\sigma\tau \in Gal(K,F)$ and $\sigma^{-1} \in Gal(K,F)$ for any $\sigma \in Gal(K,F)$ and $\tau \in Gal(K,F)$. The identity element of this group is the identity map $Id : K \to K$ sending an element of K to it self.

Remark IV.2. *Of course, there is at least one element in $Gal(K,F)$ which is the identity map corresponding to the identity element.*

Example 1.0.86. *Consider $Gal(\mathbb{C},\mathbb{R})$, the automorphisms of the complex numbers $\mathbb{C}$ over the real numbers $\mathbb{R}$. We claim that complex conjugation, defined by (for a, b real)*

$$\sigma(a+bi) = a - bi \tag{IV.3}$$

It is not hard to check that this define a automorphism of $\mathbb{C}$ which stabilize $\mathbb{R}$.
There is another element of $Gal(\mathbb{C}:\mathbb{R})$, of course, the identity map of $\mathbb{C}$. In fact there are the only two elements of $Gal(\mathbb{C},\mathbb{R})$

Theorem 1.0.87. *The* only *elements of $Gal(\mathbb{C}:\mathbb{R})$ are complex conjugation σ and the identity Id.*

Proof. Let $\tau \in Gal(\mathbb{R}:\mathbb{R})$ and consider $\tau(i)$. As $i^2+1=0$

$$0 = \tau(0) = \tau(i^2+1) = \tau(i)^2+1 \tag{IV.4}$$

That is, denoting $\tau(i)$ by z, z must satisfy $z^2+1=0$. There are only two possibilities for z, either $z = i$ or $z = -i$. Further, the value of $z = \tau(i)$ determines the entire map τ. This is because any complex number α can be written $\alpha = a+bi$ with a, b real and so

$$\tau(\alpha) = \tau(a) + \tau(b)\tau(i) = a + bz \tag{IV.5}$$

as τ fixes all real numbers. When $z = i$ we have $\tau(\alpha) = \alpha$ so that τ is the identity. When $z = -i$ we have $\tau(a+bi) = a-bi$ and so τ is complex conjugation σ. □

We therefore have $Gal(\mathbb{C},\mathbb{R}) = \{e,\sigma\}$. The identity acts as the identity of the group and

$$\sigma^2(a+bi) = \sigma(\sigma(a+bi)) = \sigma(a-bi) = a+bi \tag{IV.6}$$

so that $\sigma^2 = e$. We have a group on two elements. We can further write

$$Gal(\mathbb{C},\mathbb{R}) \cong (\mathbb{Z}/2\mathbb{Z},+) \tag{IV.7}$$

by mapping Id to 0 and σ to 1.

Remark IV.3. ⚠*An expression such as $\sigma^3(\alpha)$ does* not *mean the cube of $\sigma(\alpha)$ but rather the result of applying σ three times to α, in this case, $\sigma(\sigma(\sigma(\alpha)))$. To say, for example, that $\sigma^3 = e$, would be to say that $\sigma(\sigma(\sigma(\alpha))) = \alpha$ for* all *α.*

The proof ideas in Theorem 1.0.87 can be greatly generalized.

Theorem 1.0.88. *Let $F \subset K, K'$, all fields. Let $\sigma : K \to K'$ be an isomorphism over F as given by Definition 1.0.85. Let $\alpha \in K$ and let α be a root of some $p(x) \in F[x]$. That is, we may write*

$$p(x) = a_0 + a_1x + \ldots + a_nx^n \in F[x]$$

with the coefficients in F. Set $\beta = \sigma(\alpha)$ Then β is a root of $p(x)$.

Proof. As

$$0 = p(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

we apply σ to both sides and (noting, critically, that as $a_i \in F$, $\sigma(a_i\alpha^i) = \sigma(a_i)\sigma(\alpha)^i = a_i\beta^i$)

$$0 = \sigma(0) = a_0 + a_1\beta + \ldots + a_n\beta^n$$

as desired. □

Theorem 1.0.89. *Let $F \subset K, K'$, all fields. Assume $K = F(\alpha_1, \ldots, \alpha_s)$. Let $\sigma : K \to K'$ be an isomorphism over F as given by Definition 1.0.85. Then σ is determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_s)$.*

Proof. For any mononomial $\kappa = c\alpha_1^{m_1} \cdots \alpha_s^{m_s}$ with $\mathbb{C} \in F$, the value of $\sigma(\kappa)$ is determined by

$$\sigma(\kappa) = c\sigma(\alpha_1)^{m_1} \cdots \sigma(\alpha_s)^{m_s}$$

Any polynomial λ in $\alpha_1, \ldots, \alpha_s$ is the sum of monomials and hence $\sigma(\lambda)$ is determined. When K is an extension of F of finite dimension (which is pretty much all we look at) every $\lambda \in K$ is such a polynomial and so σ is determined on K. But even in the general case every $\lambda \in K$ can be written as the quotient $\lambda = \lambda_1/\lambda_2$ of polynomials and hence $\sigma(\lambda) = \sigma(\lambda_1)/\sigma(\lambda_2)$ is still determined. □

Here is a powerful consequence.

Theorem 1.0.90. *Let $F \subset K$, both fields, and assume only that $[K : F]$ is finite. Then the Galois Group $Gal(K, F)$ (as given by Definition 1) is finite.*

Proof. Suppose $n = [K : F]$. Write $K = F(\alpha_1, \ldots, \alpha_s)$ for some $\alpha_1, \ldots, \alpha_s$. Let $\sigma \in Gal(K, F)$ and set $\beta_i = \sigma(\alpha_i)$ for each i. Each α_i satisfies some polynomial $p_i(x) \in F[x]$ of degree at most n. From theorem 1.0.88, β_i satisfies the same polynomial. But we know that a polynomial of degree at most n can have at most n roots so there are at most n choices for β_i. These choices, from Theorem 1.0.89, determine σ on all of K. □

Remark IV.4. ⚠*Suppose that in Theorem 1.0.90 we have $K = F(\alpha_1, \ldots, \alpha_s)$. Each $\sigma(\alpha_i)$ must be one of a finite number of choices.* However, *not all choices necessarily give a good σ. For example, suppose we wrote $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$. For $\sigma \in Gal(K, F)$ we must have $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$, $\sigma(\sqrt{6}) = \pm\sqrt{6}$. But we don't get all eight choices. If, say, $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = +\sqrt{3}$, then we must have (as σ sends products to products) $\sigma(\sqrt{6}) = -\sqrt{6}$.*

Now we can give a wide class of examples for which the Galois Group is determined.

Theorem 1.0.91. *Let $F \subset K$, both fields, and assume that $K = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial for α. Suppose further that $\beta \in K$ is also a root of $p(x)$. Then there is an automorphism σ of K over F with $\sigma(\alpha) = \beta$.*

Proof. Set n to be the degree of $p(x)$. Then

$$K = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\}$$

As $p(x)$ is a minimal polynomial for α it must be irreducible (over F) and hence it must be a minimal polynomial for β as well. Thus $[F(\beta) : F] = n$. But as $\beta \in F(\alpha)$, $F(\beta) \subseteq F(\alpha)$. As the dimensions over F are the same we deduce that $F(\beta) = K$. Thus we can write

$$K = \{a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1} : a_0, \ldots, a_{n-1} \in F\}$$

We define σ by

$$\sigma(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}$$

The key point is that products are sent to products. Write $p(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0$. In multiplying elements of the form $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ we use the reduction $\alpha^n = -b_{n-1}\alpha^{n-1} - \ldots - b_0$. As β has the same minimal polynomial in multiplying elements of the form $a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1}$ we use the same reduction $\beta^n = -b_{n-1}\beta^{n-1} - \ldots - b_0$. □

Theorem 1.0.92. *Let $F \subset K$, both fields, and assume that $K = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial for α. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ be all the roots of $p(x)$ in K. Then the Galois Group $Gal(K,F)$ (as given by Definition 1) will have precisely s elements $\sigma_1 = e, \sigma_2, \ldots, \sigma_s$.*

Proof. As $K = F(\alpha)$, σ is determined (Theorem 1.0.89) by $\sigma(\alpha)$ which must be (Theorem 1.0.88) one of $\alpha_1, \ldots, \alpha_s$. From Theorem 1.0.91 each of these give a valid $\sigma_i \in Gal(K,F)$. □

2 Examples

In all our examples the ground field shall be $\mathbb{Q}$ and the extension field will be a subfield of the complex numbers $\mathbb{C}$.

We take as basic that the *only* nonzero rational numbers $\mathbb{C}$ for which $\sqrt{c} \in \mathbb{Q}$ are those positive $\mathbb{C}$ for which each prime factor p appears an even number of times. In particular, $\sqrt{2}, \sqrt{3}, \sqrt{3/2}$ are all irrational.

2.1 $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

As $\sqrt{2}$ has minimal polynomial $x^2 - 2$, $\mathbb{Q}(\sqrt{2})$ has basis $1, \sqrt{2}$ over $\mathbb{Q}$. Now we need a simple result:

Theorem 2.1.1. $\sqrt{3} \not\in \mathbb{Q}(\sqrt{2})$

Proof. If it were we would have

$$\sqrt{3} = a + b\sqrt{2}$$

with $a, b \in \mathbb{Q}$. Squaring both sides

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}$$

As $1, \sqrt{2}$ is a basis the coefficient of $\sqrt{2}$ would need be zero. That is, $2ab = 0$. So either $a = 0$ or $b = 0$.

1. $b = 0$: Then $\sqrt{3} = a \in \mathbb{Q}$, contradiction.

2. $a = 0$. Then $\sqrt{3} = b\sqrt{2}$ so $\sqrt{3/2} = b \in \mathbb{Q}$, contradiction.

□

From Theorem 2.1.1 and that $\sqrt{3}$ satisfies a quadratic (namely, $x^2 - 3$) over $\mathbb{Q}(\sqrt{2})$, $1, \sqrt{3}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ and so $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis for K over $\mathbb{Q}$. That is, we may write

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in Q\} \tag{IV.8}$$

and every $\alpha \in K$ has a *unique* expression in this form.

Now we turn to the Galois Group $Gal(K, \mathbb{Q})$. Any $\sigma \in K$ has $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$ which gives four (⚠this is 2 × 2) possibilities. The value of σ on $\sqrt{2}, \sqrt{3}$ determines the value on all of K. The four elements of the Galois Group are $Id, \sigma_1, \sigma_2, \sigma_3$ where

$$Id(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

$$\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

Check that these really are automorphisms, that they are bijections that send sums to sums and products to products. This will actually come out of more general stuff later. (Exercise!)

What does the group $Gal(K, \mathbb{Q})$ look like. The identity is the identity, no problem. Any σ when squared gives the identity. For example

$$\sigma_1^2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = \sigma_1(a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

We can also see this by noticing that either $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$ but in either case $\sigma^2(\sqrt{2}) = \sqrt{2}$ and similarly $\sigma^2(\sqrt{3}) = \sqrt{3}$ so that $\sigma^2 = Id$. We also calculate that if you multiply any two of $\sigma_1, \sigma_2, \sigma_3$ in either directtion you get the other third one. For example

$$\sigma_2(\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})) = \sigma_2(a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

We have the Klein Vierergruppe, aka the Fourgroup, which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Actually, there are only two groups with four elements (up to isomorphism, of course), the cyclic group $\mathbb{Z}/4\mathbb{Z}$ and the Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ so once it isn't the first it *must* be the second!

2.2 $K = \mathbb{Q}(\epsilon)$ with $\epsilon = e^{2\pi i/5}$

ϵ satisfies $x^5 - 1 = 0$ and, as $\epsilon \neq 1$, it satisfies $p(x) = 0$ with

$$p(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1 \tag{IV.9}$$

This is irreducible (one can show this by replacing x by $x+1$ giving $x^4 + 5x^3 + 10x^2 + 5x + 5$ and using Eisenstein's criterion) so $[K : \mathbb{Q}] = 4$ and we write

$$K = \{a + b\epsilon + c\epsilon^2 + d\epsilon^3 : a, b, c, d \in \mathbb{Q}\} \tag{IV.10}$$

The minimal polynomial (IV.9) has roots $\epsilon, \epsilon^2, \epsilon^3, \epsilon^4$. From Theorem 1.0.92 the Galois Group $Gal(K, \mathbb{Q})$ consists of four automorphism which we shall label $\sigma_1, \sigma_2, \sigma_3, \sigma_4$. They are determined by their values on ϵ and we shall let σ_j be that automorphism with $\sigma_j(\epsilon) = \epsilon^j$. Note that σ_1 is the identity and σ_4 is the complex conjugation.

What is the product $\sigma_j\sigma_k$. Lets see what it does to ϵ.

$$(\sigma_j\sigma_k)(\epsilon) = \sigma_j(\sigma_k(\epsilon)) = \sigma_j(\epsilon^k) = \sigma_j(\epsilon)^k = (\epsilon^j)^k = \epsilon^{jk} \tag{IV.11}$$

Then, $\sigma_j\sigma_k = \sigma_{jk}$. But we only have four automorphisms. What does it mean to say $\sigma_3\sigma_3 = \sigma_9$. The key is that $\epsilon^5 = 1$ so that we can reduce ϵ^{jk} by reducing jk modulo 5. As $\epsilon^9 = \epsilon^4$ we have $\sigma_3\sigma_3 = \sigma_4$. So we *can* and *do* say $\sigma_j\sigma_k = \sigma_{jk}$ with the understanding that jk is computed modulo 5. With this we have

$$Gal(K, \mathbb{Q}) \cong \left(\mathbb{Z}/5\mathbb{Z}\right)^* \tag{IV.12}$$

where we associate σ_j with j. Finally $(\mathbb{Z}/5\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z}, +)$ (the cyclic group, not the Vierergruppe) by associating $1, 2, 3, 4$ with $0, 1, 3, 2$ respectively.

2.3 $K = \mathbb{Q}(2^{1/3}, \omega)$ with $\omega = e^{2\pi i/3}$

The polynomial

$$p(x) = x^3 - 2 \tag{IV.13}$$

is irreducible (by Eisenstein's criterion, or simply that, as a cubic, it has no rational roots) and its roots are α, β, γ where for convenience we write

$$\alpha = 2^{1/3}, \beta = 2^{1/3}\omega, \gamma = 2^{1/3}\omega^2 \tag{IV.14}$$

Any field that contains $2^{1/3}, \omega$ contains α, β, γ and any field that contains α, β, γ contains $2^{1/3}, \omega$ so we may also write $K = \mathbb{Q}(\alpha, \beta, \gamma)$, so K is the *splitting field* of $p(x)$ over $\mathbb{Q}$. A basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is $1, \alpha, \alpha^2$. As all elements of $\mathbb{Q}(\alpha)$ are real, $\omega \not\in \mathbb{Q}(\alpha)$. As ω satisfies the quadratic $1 + x + x^2 = 0$ over $\mathbb{Q}(\alpha)$, a basis for $K = \mathbb{Q}(\alpha, \omega)$ over $\mathbb{Q}(\alpha)$ is $1, \omega$. Hence a basic for K over $\mathbb{Q}$ is $1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$ and we can write

$$K = \{a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2 : a, b, c, d, e, f \in Q\} \tag{IV.15}$$

and each $\zeta \in K$ has a unique such representation.

What are the automorphisms $\sigma \in Gal(K,\mathbb{Q})$? As $K = \mathbb{Q}(\alpha,\beta,\gamma)$, σ is determined by its values on α,β,γ. Further, as α,β,γ satisfy the same irreducible (IV.13), σ of any of them must be one of them. Further, as σ must be a *bijection*, σ cannot send two of α,β,γ to the same value and hence σ must be a permutation on α,β,γ. This gives that there are *at most* six automorphisms and that $Gal(K,\mathbb{Q})$ is isomorphic to a subgroup of S_3, the full symmetric group on three elements, here α,β,γ.

Actually, *all* permutations of α,β,γ yield automorphisms of K and so

$$Gal(K,\mathbb{Q}) \cong S_3 \tag{IV.16}$$

This actually will follow from some general stuff but we can give an idea here. Two automorphisms are easy, the identity (we *always* have the identity) and complex conjugation σ. We do have to check that complex conjugation is a bijection from K to itself. As $\sigma(\alpha) = \alpha$ and $\sigma(\omega) = \omega^2 \in K$ it sends K to K and since $\sigma^2 = Id$ it must be a bijection. (That is, $\sigma^{-1}(\zeta) = \sigma(\zeta)$.) This σ corresponds to the permutation that keeps α fixed and transposes β,γ.

Here is another $\tau \in Gal(K,\mathbb{Q})$. Generate it by setting $\tau(\alpha) = \beta$ and $\tau(\omega) = \omega$. Then

$$\tau(\beta) = \tau(\alpha\omega) = \tau(\alpha)\tau(\omega) = \beta\omega = \gamma \tag{IV.17}$$

and

$$\tau(\gamma) = \tau(\beta\omega) = \tau(\beta)\tau(\omega) = \gamma\omega = \alpha \tag{IV.18}$$

so it cycles α to β to γ back to α. With the representation of (IV.15)

$$\tau(a + b\alpha + c\alpha^2 + d\omega + e\omega\alpha + f\omega\alpha^2) = a + b\omega\alpha + c\omega^2\alpha^2 + d\omega + e\omega^2\alpha + f\alpha^2 \tag{IV.19}$$

In this form one need show τ is bijective (pretty easy), that $\tau(\zeta_1+\zeta_2) = \tau(\zeta_1)+\tau(\zeta_2)$ (quite easy), and that $\tau(\zeta_1\zeta_2) = \tau(\zeta_1)\tau(\zeta_2)$ (lengthy, unless you use some tricks).

Indeed, here is another approach to show that τ is indeed an automorphism from K to K. Consider the intermediate field $L = \mathbb{Q}(\omega)$. We first claim that $p(x)$ given by (IV.13) is irreducible over L. As it is a cubic, if it reduced it would have a root in L. So either $\alpha, \beta = \alpha\omega, \gamma = \alpha\omega^2$ would be in L. As $\omega \in L$ if any of α,β,γ were in L then all three would be in L, in particular $\alpha \in L$. But then L would have ω and α and so would be $\mathbb{Q}(\alpha,\omega) = K$. As $[L : Q] = 2 \neq 6 = [K : Q]$ that cannot happen. Now α,β have the same minimal polynomial in $L[x]$ and $K = L(\alpha) = L(\beta)$, so, there does exist an automorphism τ of K that preserves L and has $\tau(\alpha) = \beta$. As it preserves L we also have $\tau(\omega) = \omega$. Since τ preserves L it certainly preserves the smaller $\mathbb{Q}$ and so $\tau \in Gal(K,\mathbb{Q})$.

Once we have $\sigma,\tau \in Gal(K,\mathbb{Q})$ we have that $Gal(K,\mathbb{Q})$ is a subgroup of S_3 that contains an element τ of order three and an element σ of order two. From τ it must have at least three elements, from σ it can't have exactly three elements, so it has more than three elements, so it has all six elements, it is all of S_3.

3 Normal Extensions

Here we are usually dealing with a “ground field" F and an extension field K. Throughout we will only consider finite extensions K/F. In most examples F is the field of rational numbers $\mathbb{Q}$. While other examples will be considered, one may well think about F as $\mathbb{Q}$ in the first reading.

Recall the following facts:

Definition 2. *Let $\sigma : K_1 \to K_2$ be an isomorphism preserving F. Let $h(x) = h_0 + h_1x + \ldots + h_wx^w \in K_1[x]$. Then σh is that polynomial achieved by applying σ to all of the coefficients. That is,*

$$(\sigma h)(x) = \sigma(h_0) + \sigma(h_1)x + \ldots + (\sigma h_w)x^w$$

We note $(\sigma h)(x) \in K_2[x]$.

Theorem 3.0.1. *If $c(x) = a(x)b(x)$ in $K_1[x]$ then $(\sigma c)(x) = (\sigma a)(x)(\sigma b)(x)$ in $K_2[x]$*

Proof. Immediate. □

Theorem 3.0.2. *$p(x) \in K_1[x]$ is irreducible in K_1 if and only if $(\sigma p(x)) \in K_2[x]$ is irreducible in K_2.*

Proof. If $p(x) = a(x)b(x)$ in $K_1[x]$ then $(\sigma p) = (\sigma a)(\sigma b)$ in $K_2[x]$. Conversely we may apply the isomorphism σ^{-1} so if $(\sigma p)(x) = a(x)b(x)$ in $K_2[x]$, $p(x) = (\sigma^{-1}a)(x)(\sigma^{-1}b(x))$ in $K_1[x]$. □

Theorem 3.0.3. *Let $f(x) \in F[x]$ be irreducible over F. Let $\sigma : K_1 \to K_2$ be an isomorphism preserving F. Let $f(x) = p_1(x)\cdots p_l(x)$ be the factorization of $f(x)$ into irreducible factors in $K_1[x]$. Then $f(x) = (\sigma p_1)(x)\cdots(\sigma p_l)(x)$ is the factorization of $f(x)$ into irreducible factors in $K_2[x]$.*

Proof. As $f(x) \in F[x]$, $(\sigma f)(x)$ is $f(x)$. From Theorem 3.0.1, $f(x) = (\sigma p_1)(x)\cdots(\sigma p_l)(x)$ is a factorization and from Theorem 3.0.2 the factors are irreducible in $K_2[x]$. □

Theorem 3.0.4. *Suppose K is the splitting field of $f(x) \in F[x]$ over F. Suppose $g(x) \in F[x]$ is irreducible (over F) and suppose further that there is an $\beta \in K$ with $g(\beta) = 0$. Then $g(x)$ completely splits into linear factors in $K[x]$.*

Proof. Let $\alpha_1, \ldots, \alpha_r$ denote the roots of $f(x)$ and let $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ denote the complex roots of $g(x)$. If the theorem fails we can assume, without loss of generality, that $\beta_1 \in K$ and $\beta_2 \notin K$. Set $K_1 = F(\beta_1)$, $K_2 = F(\beta_2)$. As β_1, β_2 have the same minimal polynomial $g(x)$ over F we find an isomorphism $\sigma : K_1 \to K_2$ which preserves F and has $\sigma(\beta_1) = \beta_2$.

Now we extend the isomorphism σ by adding the roots of f to K_1. We do the first step in some detail.

Let $f(x) = p_1(x)^{e_1}\cdots p_l(x)^{e_n}$ and $f(x) = (\sigma p_1)(x)^{e_1}\cdots(\sigma p_l)(x)^{e_n}$ be the factorizations of f into irreducible factors over K_1 and K_2 respectively.

Pick any of the roots of f, say α_1 for definiteness. Considering the factorization in $K_1[x]$ it must be a root of precisely one of the irreducible factors. Say, for definiteness. $p_1(\alpha_1) = 0$.

Now look at $(\sigma p_1)(x)$. As it is a factor of $f(x)$ its roots all are roots of $f(x)$ and so are from $\alpha_1,\ldots,\alpha_r$. Let $\alpha_{\gamma 1}$ denote a root of $(\sigma p_1)(x)$. (It may be that the root is α_1 itself, this isn't a problem.) Now we extend σ to an isomorphism $\sigma^+ : K_1(\alpha_1) \to K_2(\alpha_{\gamma 1})$ with $\sigma^+(\alpha_1) = \alpha_{\gamma 1}$.

We continue this process. (Formally, the proof can be done by induction.) At any stage we have an isomorphism $\sigma^* : K_1^* \to K_2^*$ where K_1^*, K_2^* are extensions of K_1, K_2 be various roots of $f(x)$. If some root α of $f(x)$ is not in K_1^* we look at its minimal polynomial $p(x)$ over K_1^*, find a root α' of $(\sigma^* p)(x)$ and extend σ^* be setting $\sigma^{*+}(\alpha) = \alpha'$. This process terminates with an isomorphism $\sigma^{final} : K_1^{final} \to K_2^{final}$. Here $K_1^{final} = K_1(\alpha_1,\ldots,\alpha_r)$ as we have extended by all the roots of f. The isomorphism σ^{final} from K_1^{final} must send each root α_i of $f(x) \in F[x]$ to another root (possibly itself) and as σ^{final} is a bijection it must permute the roots and hence $K_2^{final} = K_2(\alpha_1,\ldots,\alpha_r)$.

Whats wrong with this? Well, remember that $K_1 = F(\beta_1)$ with $\beta_1 \in F(\alpha_1,\ldots,\alpha_r)$ and so $K_1^{final} = F(\alpha_1,\ldots,\alpha_r)$. But $K_2 = F(\beta_2)$ with $\beta_2 \not\in F(\alpha_1,\ldots,\alpha_r)$ and so $K_2^{final} = F(\alpha_1,\ldots,\alpha_r,\beta_2)$ is a nontrivial extension of K_1^{final}. This would mean that $[K_2^{final} : F] > [K_1^{final} : F]$ which is impossible as isomorphisms preserve dimension. That is, our original assumption that $\beta_1 \in F(\alpha_1,\ldots,\alpha_r)$ but $\beta_2 \not\in F(\alpha_1,\ldots,\alpha_r)$ is not possible. And this is what we wanted to prove. □

Now that we have proven Theorem 3.0.4 we give an important definition that distinguishes certain kind of field extensions.

Definition 3.0.5. *(Proposition) Suppose $F \subset K$ are subfields of $\mathbb{C}$ with K a finite extension of F. We say that the extension K/F is* **normal** *if one of the following equivalent assertions holds:*

1. *There is an $f(x) \in F[x]$ with K the splitting field of $f(x)$ over F.*

2. *Every $g(x) \in F[x]$ which is irreducible (over F) and has a root in K completely splits into linear factors in $K[x]$.*

When this occurs we often say that K is a normal extension of F.

Proof. We've already done the hard part. Theorem 3.0.4 gives that condition 1. implies condition 2.. Now assume condition 2.. As $[K : F]$ is finite write $K = F(\alpha_1,\ldots,\alpha_s)$ for some finite number of $\alpha_1,\ldots,\alpha_s$. For each α_i let $p_i(x) \in F[x]$ be its irreducible polynomial over F.

We claim K is the splitting field of $f(x)$ where we set $f(x)$ to be the product $p_1(x)\cdots p_s(x)$. By Condition 2. *all* of the roots of each $p_i(x)$ are in F and so the extension of F by all of the roots of $f(x)$ (that is, all of the roots of each $p_i(x)$) is still inside of F. But the roots include $\alpha_1,\ldots,\alpha_s$ so the extension must include $F(\alpha_1,\ldots,\alpha_s)$ which is all of K. That is, the extension of F by all of the roots of $f(x)$ is precisely K, giving the claim. □

Example 3.0.6.

1. *$K = \mathbb{Q}(2^{1/3})$ is* not *a normal extension of $\mathbb{Q}$ as the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ (irreducible by Eisenstein's criterion) has one root in K but its other roots are not in K.*

2. *$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a normal extension of $\mathbb{Q}$ as the polynomial $(x^2-2)(x^2-3)$ has roots $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ and extending $\mathbb{Q}$ by these four roots gives precisely K.*

3. *$K = \mathbb{Q}(2^{1/3}, \omega)$ (with $\omega = e^{2\pi i/3}$) is a normal extension of $\mathbb{Q}$ as the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has roots $2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2$ and extending $\mathbb{Q}$ by these three roots gives precisely K.*

4. *Let $\epsilon = e^{2\pi i/5}$. Then $K = \mathbb{Q}(\epsilon)$ is a normal extension of $\mathbb{Q}$ as the polynomial $(x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$ has roots $\epsilon, \epsilon^2, \epsilon^3, \epsilon^4$ and extending $\mathbb{Q}$ by these four roots gives precisely K.*

5. *Let $K = \mathbb{Q}(2^{1/4})$ and $F = \mathbb{Q}(2^{1/2})$. Then K is a normal extension of F as the polynomial $x^2 - 2^{1/2} \in F[x]$ has roots $2^{1/4}, -2^{1/4}$ and extending F by these two roots gives precisely K.*

6. *Let $K = \mathbb{Q}(2^{1/4})$. Then K is* not *a normal extension of $\mathbb{Q}$ as the polynomial $x^4 - 2 \in \mathbb{Q}[x]$ (irreducible by Eisenstein's criterion) has two roots $2^{1/4}, -2^{1/4}$ in K but the other two roots $2^{1/4}i, -2^{1/4}i$ are not in K. (One reason why $2^{1/4}i \notin K$ is that all elements of K are real.)*

Remark IV.5. ⚠*The last two examples emphasize that when we talk about a normal extension we are talking about* two *fields, that K is normal over F. Further, consider the tower $\mathbb{Q} \subset F \subset K$, with $F = \mathbb{Q}(2^{1/2})$ and $K = \mathbb{Q}(2^{1/4})$. Then F is a normal extension of $\mathbb{Q}$ as it is an extension of $\mathbb{Q}$ by the two roots of $x^2 - 2$. We've seen that K is a normal extension of F. But it is* not *true (as we just saw) that K is a normal extension of $\mathbb{Q}$. That is, we do* not *have a transitive property for normality.*

While we have to be careful about towers of fields, the following is useful and easy.

Theorem 3.0.7. *(*`The Middle Normal Theorem`*) Let $K \subset L \subset F$ be fields and* assume *K/F is a normal field extension. Then F/L is a normal field extension.*

Proof. From Definition 3.0.5, condition 1., there is an $f(x) \in F[x]$ with K the splitting field of $f(x)$ over F. That is, f splits entirely in $K[x]$ with roots $\alpha_1, \ldots, \alpha_r \in F$ and $K = F(\alpha_1, \ldots, \alpha_r)$. But now we can simply consider $f(x)$ as a polynomial in $L[x]$. It still splits entirely in $K[x]$ with roots $\alpha_1, \ldots, \alpha_r$. As $F \subset L$ we have $F(\alpha_1, \ldots, \alpha_r) \subset L(\alpha_1, \ldots, \alpha_r)$ and since $\alpha_1, \ldots, \alpha_r \in F$ and $L \subset F$, $L(\alpha_1, \ldots, \alpha_r) \subset K$ so that $L(\alpha_1, \ldots, \alpha_r) = F$ and so the F is a normal extension over L by the same Definition 3.0.5, condition 1. and the same $f(x)$. □

Remark IV.6. ⚠*Under the assumptions of Theorem 3.0.7 we do* not *necessarily have L/K a normal extension.*

Here is a nice property of normal field extensions that say, somehow, that they are nailed down.

Theorem 3.0.8. *Let K/F be a normal field extension. Let K' be a field and $\sigma : K \to K'$ an isomorphism over F. (Recall, this means $\sigma(c) = c$ for all $c \in F$.) Then $K' = K$.*

Proof. We can write $K = F(\alpha_1, \ldots, \alpha_s)$. Then $K' = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_s))$. For each i, α_i and $\sigma(\alpha_i)$ satisfy the same irreducible polynomial $p_i(x) \in F[x]$. As K/F is normal this means $\sigma(\alpha_i) \in K$. Thus $K' \subset K$. Similarly, going backward with σ^{-1}, $K \subset K'$ and so $K = K'$. □

Remark IV.7. ⚠*Theorem 3.0.8 does not say that each element of K is fixed by σ. Indeed, σ can move around the elements of K but the set of elements remains the same.*

Theorem 3.0.9. *Let K/F be a finite field extension. Then there is an extension $K \subset K^{nr}$ so that K^{nr} is a normal field extension of F.*

Proof. As $[K:F]$ is finite we can write $K = F(\alpha_1, \dots, \alpha_r)$ for some finite number of α's. Let $p_i(x)$ be the minimal polynomial for α_i in $F[x]$. Set K^{nr} to be the splitting field for the product $f(x) = p_1(x) \cdots p_r(x)$. As a splitting field it is a normal extension of F and it contains $\alpha_1, \dots, \alpha_r$ and therefore K. □

4 Fields to Groups and back again

Let us fix some finite extension $F \subset K$ of subfields of $\mathbb{C}$ and set G to be the Galois Group $Gal(K,F)$. We will be interested in intermediate fields L, that is, $F \subset L \subset K$, and in subgroups H of G. We will describe first a mapping from fields L to groups H

Definition 4.0.10. *Let $F \subset L \subset K$ be an intermediate field. We define G_L, a subgroup of G, by*

$$G_L = \{\sigma \in G : \sigma(\alpha) = \alpha \textit{ for all } \alpha \in L\} \tag{IV.20}$$

That is, G_L is those automorphisms of L which fix all elements of L.

G_L is a subgroup of G, indeed suppose σ, τ were two automorphims of K over F. Then, as we have discussed before, so is $\sigma\tau$. But further, if $\sigma(\alpha) = \alpha$ and $\tau(\alpha) = \alpha$ for all $\alpha \in L$ then

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$$

for all $\alpha \in L$ and so $\sigma\tau \in G_L$. Similarly $\sigma^{-1} \in G_L$. Finally the identity $Id \in G_L$ as Id fixes all elements.

We now will describe first a mapping from groups H to fields L.

Definition 4.0.11. *Let $H \subset G$ be a subroup of the Galois Group. We define K^H, an intermediate field, by*

$$K^H = \{\alpha \in K : \sigma(\alpha) = \alpha \textit{ for all } \sigma \in H\} \tag{IV.21}$$

That is, K^H is those elements of K which are fixed by all automorphisms $\sigma \in H$.

Set $L = K^H$. L an intermediate field. Indeed, first of all, as all automorphisms $\sigma \in G$ fix all elements $c \in F$, any element $c \in F$ will be fixed by all $\sigma \in H$, so that $F \subset L$. Now suppose $\alpha, \beta \in L$ and take any $\sigma \in H$. As $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$, we must have $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$. Thus $\alpha + \beta \in L$ and similarly $\alpha\beta, -\alpha, \alpha^{-1} \in L$.

Example 4.0.12. *Take ground field $F = \mathbb{Q}$ and extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The four elements of the Galois Group G are $Id, \sigma_1, \sigma_2, \sigma_3$ where (as done earlier)*

$$Id(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\sigma_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$
$$\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$
$$\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

G is the Vierergruppe. There are five subgroups (we count the trivial ones here) of G:

$$\{Id\}, H_1 = \{Id,\sigma_1\}, H_2 = \{Id,\sigma_2\}, H_3 = \{Id,\sigma_3\},\ \textit{and G itself.}$$

Of course, $K^{\{Id\}} = K$. We want to describe the elements of K^{H_1}. That is, which $\alpha = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ are fixed by all Id,σ_1. Since, Id is the identity so it fixes everything so we can ignore it. If we think of $\sigma_1(\alpha) = \alpha$ as an (easy) equation it is true precisely when $b = d = 0$. So $\alpha \in K^{H_1}$ if and only if we can write $\alpha = a + c\sqrt{3}$. That is, $K^{H_1} = \mathbb{Q}(\sqrt{3})$. Similarly, for $\alpha \in K^{H_2}$ the necessary and sufficient condition is that $c = d = 0$ so $\alpha = a+b\sqrt{2}$ and $K^{H_2} = \mathbb{Q}(\sqrt{2})$. Similarly, for $\alpha \in K^{H_3}$ the necessary and sufficient condition is that $b = c = 0$ so $\alpha = a + d\sqrt{6}$ and $K^{H_3} = \mathbb{Q}(\sqrt{6})$. Finally, $\alpha \in K^G$ is such that $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ fixed by all $Id,\sigma_1,\sigma_2,\sigma_3$. To be fixed by σ_1 forces $b = d = 0$, to be fixed by σ_2 forces $\mathbb{C} = d = 0$, to be fixed by σ_3 is now redundant as it forces $b = c = 0$. So all of b, c, d must be zero but a can be an arbitrary rational and so $K^G = \mathbb{Q}$.

Now set

$$L_1 = \mathbb{Q}(\sqrt{2}), L_2 = \mathbb{Q}(\sqrt{3}), L_3 = \mathbb{Q}(\sqrt{6})$$

and consider the groups associated with the fields $\mathbb{Q}, L_1, L_2, L_3, K$. The easiest is $G_{\mathbb{Q}} = G$, which is to say that all $\sigma \in G$ fix all $\alpha \in \mathbb{Q}$ which is true as G was defined *as all automorphisms σ of K which fix all $\alpha \in \mathbb{Q}$.*

How about G_{L_1}? Clearly $Id \in G_{L_1}$ as Id fixes everything. Also $\sigma_2 \in G_{L_1}$ as $\sigma_2(a+b\sqrt{2}) = a+b\sqrt{2}$. But $\sigma_1,\sigma_3 \not\in G_{L_1}$ as they send $\sqrt{2}$ to $-\sqrt{2}$. So $G_{L_1} = \{Id,\sigma_2\}$

How about G_{L_2}? Clearly $Id \in G_{L_2}$ as Id fixes everything. Also $\sigma_1 \in G_{L_2}$ as $\sigma_1(a+c\sqrt{3}) = a+c\sqrt{3}$. But $\sigma_2,\sigma_3 \not\in G_{L_2}$ as they send $\sqrt{3}$ to $-\sqrt{3}$. So $G_{L_2} = \{Id,\sigma_1\}$

How about G_{L_3}? Clearly $e \in G_{L_2}$ as Id fixes everything. Also $\sigma_3 \in G_{L_3}$ as $\sigma_3(a+d\sqrt{6}) = a+d\sqrt{6}$. But $\sigma_1,\sigma_2 \not\in G_{L_3}$ as they send $\sqrt{6}$ to $-\sqrt{6}$. So $G_{L_3} = \{Id,\sigma_3\}$

Finally, how about G_K. Clearly $Id \in G_K$ as Id fixes everything. But the other $\sigma_1,\sigma_2,\sigma_3$ do not fix everything and so are not in G_K. Thus $G_K = G$.

We can put this all in tabular form.

Field	*Group*
$K = \mathbb{Q}(\sqrt{2},\sqrt{3})$	$\{e\}$
$L_1 = \mathbb{Q}(\sqrt{2})$	$H_2 = \{e,\sigma_2\}$
$L_2 = \mathbb{Q}(\sqrt{3})$	$H_1 = \{e,\sigma_1\}$
$L_3 = \mathbb{Q}(\sqrt{6})$	$H_3 = \{e,\sigma_3\}$
$\mathbb{Q}$	$G = \{e,\sigma_1,\sigma_2,\sigma_3\}$

We see we have a one-to-one correspondence. We can go from fields to groups by applying G_{-}. And we can go from groups to fields by applying K^{-}. And K^{-} and G_{-} are inverses as maps, if we apply one and then the other we get back where we started.

Does this always work? No. But it works *in important cases* and that will be the substance of the major theorem of Galois Theory. Indeed, not to keep you in suspence, here is that theorem. The normal extensions are precisely those extensions for which the correspondence works.

Theorem 4.0.13. `The Galois Correspondence Theorem` *Let $F \subset K$ be subfields of $\mathbb{C}$ with K/F a* normal *extension. Set $G = Gal(K,F)$. Then there is a bijection between the intermediate fields L, meaning that $F \subset L \subset K$ and the subgroups H of G. (We include $L = F$, $L = K$ as intermediate fields and we include $\{e\}$ and G itself as subgroups.) The bijection is given by G_- and K^- as previously defined. That is, $H = G_L$ if and only if $L = K^H$. Thus*

$$K^{G_L} = L \text{ and } G_{K^H} = H \tag{IV.22}$$

Furthermore, the correspondence reverses *containment, making L bigger makes $H = G_L$ smaller and making H bigger makes $L = K^H$ smaller. The field F is associated with all of G while the field K is associated with $\{e\}$. Setting $n = [K : F]$ we have $n = |G|$. Further the sizes are connected, when $H = G_L$*

$$[K : L] = |H| \tag{IV.23}$$

or, equivalently,

$$[L : F] = |G/H| \tag{IV.24}$$

Remark IV.8.

1. *In the listing for $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ above as G has only four elements it doesn't take too much work (try it!) to show that $\{Id\}, H_1, H_2, H_3, G$ are the* only *subgroups. It is not at all clear that we have listed* all *of the subfields of K. How do we know there isn't some other weird intermediate field between $\mathbb{Q}$ and K? After all, these are infinite sets so we can't try everything. It will turn out that from Galois Theory we will be able to show that the above list gives all of the intermediate fields.*

2. *Let the ground field $F = \mathbb{Q}$ and the extension field $K = \mathbb{Q}(2^{1/3})$. Any automorphism $\sigma : K \to K$ must send $2^{1/3}$ to a root of $x^3 - 2$ but $2^{1/3}$ is the* only *root of $x^3 - 2$ in K, as the other roots are not real. Thus we must have $\sigma(2^{1/3}) = 2^{1/3}$ and so σ must be the identity. That is, $G = Gal(K,\mathbb{Q}) = \{Id\}$. As $[K : Q] = 3$ there are no intermediate fields except for $\mathbb{Q}$ and K themselves. So $G_{\mathbb{Q}} = \{Id\}$ and $G_K = \{Id\}$. As every element is fixed by Id, $K^{\{Id\}} = K$. So in this case we do* not *get a bijection between subgroups of the Galois Group and intermediate fields.*

For *any* extension K/F the following “easy" result is one part of (IV.22), the main part of the Galois Correspondence Theorem, Theorem 4.0.13.

Theorem 4.0.14. *Let $F \subset K$ be subfields of $\mathbb{C}$. Then for any intermediate field L*

$$L \subset K^{G_L} \tag{IV.25}$$

and for any subgroup H

$$H \subset G_{K^H} \tag{IV.26}$$

Proof. G_L is those automorphisms σ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in L$. That is, all $\sigma \in G_L$ fix all $\alpha \in L$. That is, all $\alpha \in L$ are fixed by all $\sigma \in G_L$ and hence all $\alpha \in L$ belong to K^{G_L}. Similarly, K^H is those $\alpha \in K$ such that $\sigma(\alpha) = \alpha$ for all $\sigma \in H$. That is, all $\sigma \in H$ fix all $\alpha \in K^H$. That is, all $\sigma \in H$ are in G_{K^H}. □

Theorem 4.0.15. *Let $F \subset K$ be subfields of $\mathbb{C}$ with K a Normal extension of F and set G to be the Galois Group $Gal(K,F)$. Then for any intermediate field L*

$$K^{G_L} = L \tag{IV.27}$$

Proof. We already know $L \subset K^{G_L}$. Now suppose $\beta \in K$ and $\beta \notin L$. Our goal is to show $\beta \notin K^{G_L}$. Recall that as K is a normal extension of F, K is a normal extension of L.

Let $p(x)$ be the minimal polynomial for $\beta \in L[x]$ and let β_1 be another root of $p(x)$. As K is a normal extension of L, $\beta_1 \in K$. Thus there is an isomorphism $\sigma : L(\beta) \to L(\beta_1)$ which fixed L and has $\sigma(\beta) = \beta_1$. Applying the Isomorphism Extension Theorem we extend σ to an isomorphism σ^+ with domain K. But as σ^+ fixes L and K is normal over L, the range of σ^+ must be K. That is, σ^+ is an automorphism of K which fixes all $\alpha \in L$ but does not fix β. So $\beta \notin K^{G_L}$. □

This has a perhaps surprising followup.

Theorem 4.0.16. *Let $F \subset K$ be subfields of $\mathbb{C}$ with K a normal extension of F. Then there are only* finitely many *intermediate fields L.*

Proof. From Theorem 4.0.16, L is determined by G_L but as $G = Gal(K,F)$ is finite there can be only finitely many subgroups H, only finitely many possible G_L. □

Theorem 4.0.17. *Let K be a finite extension of F, both subfields of $\mathbb{C}$. Then there are only* finitely many *intermediate fields L.*

Proof. Extend K to K^+ so that K^+ is a normal extension of F. From Theorem 4.0.16 there are only finitely many intermediate fields between F and K^+ and thus only finitely many intermediate fields between F and the smaller K. □

Theorem 4.0.18. *Let F be a subfield of $\mathbb{C}$ and $\alpha, \beta \in \mathbb{C}$, both algebraic over F. Then there exists $\gamma \in \mathbb{C}$ with*

$$F(\gamma) = F(\alpha,\beta) \tag{IV.28}$$

Proof. As α,β are algebraic over F, $F(\alpha,\beta)$ is a finite extension of F. Now for each integer i set $F_i = F(\alpha + i\beta)$. Each of these are subfields of $F(\alpha,\beta)$ but by Theorem 4.0.17 there are only finitely many such subfields so there must be $i \neq j$ with $F_i = F_j$. Thus F_i contains $\alpha + i\beta$ *and* $\alpha + j\beta$. But then it contains $\alpha = \frac{1}{j-i}[j(\alpha+i\beta) - i(\alpha+j\beta)]$ and $\beta = \frac{1}{j-i}[(\alpha+j\beta)-(\alpha+i\beta)]$. Thus F_i must be all of $F(\alpha,\beta)$ and so we can take $\gamma = \alpha + i\beta$. □

Theorem 4.0.19. `Single Generator Theorem.` *Let K be a finite extension of F, both subfields of $\mathbb{C}$. Then there is an element $\gamma \in K$ such that $K = F(\gamma)$.*

Proof. We claim that for any $\alpha_1,\ldots,\alpha_r \in \mathbb{C}$, all algebraic over F, there exists a $\gamma \in \mathbb{C}$ with $F(\gamma) = F(\alpha_1,\ldots,\alpha_r)$. This comes from repeatedly applying Theorem 4.0.18 to replace two of the generators by one. (Formally we apply induction on r.) Now as K is a finite extension of F we can write $K = F(\alpha_1,\ldots,\alpha_r)$ for some finite set of α's and then replace them by a single γ. □

Theorem 4.0.20. *Let K be a normal extension of F and let L be an intermediate field. Set $r = [K:L]$ Then G_L consists of precisely r automorphisms.*

Proof. We know from the Middle Normal Theorem that K is a normal extension of L, which will allow us basically to ignore F. From the Single Generator Theorem 4.0.19 write $K = L(\alpha)$. Let $p(x)$ be the minimal polynomial in $L[x]$ with α as a root so that $p(x)$ has degree r. In $\mathbb{C}$ let $\alpha = \alpha_1,\alpha_2,\ldots,\alpha_r$ denote the roots of $p(x)$. As K/L is normal, $\alpha_1,\ldots,\alpha_r \in K$. As $[L(\alpha_i):L] = r$ we must have all $L(\alpha_i) = K$. For each $1 \le i \le r$ as α,α_i have the same minimal polynomial in $L[x]$ there is an isomorphism $\sigma_i : L(\alpha) \to L(\alpha_i)$ given by setting $\sigma_i(\alpha) = \alpha_i$. These are automorphisms of K fixing L, so elements of G_L. Conversely $\sigma \in G_L$ is determined by $\sigma(\alpha)$ and $\sigma(\alpha)$ must also satisfy $p(x)$ and so must be one of $\alpha_1,\ldots,\alpha_r$ and so $\sigma_1,\ldots,\sigma_r$ are *all* of the automorphisms in G_L. □

Example 4.0.21. *Take $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$. The Single Generator Theorem 4.0.19 works and we can set $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. This is not certain a priori, one must check that $\sqrt{2}+\sqrt{3}$ does indeed generate K. Setting $\gamma = \sqrt{2}+\sqrt{3}$ we check that $1,\gamma,\gamma^2 = 5+2\sqrt{6},\gamma^3 = 11\sqrt{2}+9\sqrt{3}$ are indeed linearly independent. You need to show that the vectors $(1,0,0,0)$, $(0,1,1,0)$, $(5,0,0,2)$, $(0,11,9,0)$, representing $1,\gamma,\gamma^2,\gamma^3$ are linearly independent. Now set, for example, $\overline{\gamma} = \sqrt{2}-\sqrt{3}$ and we want a $\sigma \in Gal(K,\mathbb{Q})$ with $\sigma(\gamma) = \overline{\gamma}$. Then $\sigma(\gamma^2) = \sigma(5+2\sqrt{6}) = \overline{\gamma}^2 = 5-2\sqrt{6}$ and $\sigma(\gamma^3) = \sigma(9+11\sqrt{6}) = \overline{\gamma}^3 = 11\sqrt{2}-9\sqrt{3}$. σ is a linear transformation from K to itself. From $\sigma(\gamma^2) = \overline{\gamma}^2$ we deduce $\sigma(\sqrt{6}) = -\sqrt{6}$. Further $\gamma^3 - 9\gamma = 2\sqrt{2}$ and so $\sigma(2\sqrt{2}) = \overline{\gamma}^3 - 9\overline{\gamma} = 2\sqrt{2}$. Thus we must have $\sigma(\sqrt{2}) = \sqrt{2}$ and, finally, $\sigma(\sqrt{3}) = \sigma(\sqrt{6})/\sigma(\sqrt{2}) = -\sqrt{3}$. That is, σ is one of the four automorphisms we knew we had.*

Now we have shown the size relationship in the Galois Correspondence Theorem 4.0.13. The only item left is to show that the correspondence between L and G_L gives us *all* of the subgroups H. This will take an interesting side detour.

5 Symmetric Functions

Now for a change of pace which has applications to what we are doing and is interesting by itself. Lets look at polynomials in n variables $x_1,\ldots,x_n$. In our examples we'll take $n = 3$ and call the variables simply x, y, z.

We'll call a polynomial symmetric if no matter how you permute the variables you get the same thing. For example: $x^{20}+y^{20}+z^{20}$ or $x^5y^5+x^5z^5+y^5z^5$. One class is of particular interest to us. For $1 \le i \le n$ define the i-th *elementary symmetric polynomial* as the sum of all of the products of i distinct variables. That is, $s_1 = x+y+z$, $s_2 = xy+xz+yz$, $s_3 = xyz$.

Suppose

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \tag{IV.29}$$

is a monic polynomial of degree n with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. (When α is a root of multiplicity m just write it m times here.) Then

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x-\alpha_1)\cdots(x-\alpha_n) \tag{IV.30}$$

Multiplying out the product, x^{n-1} has coefficient $-(\alpha_1 + \ldots + \alpha_n)$, the constant coefficient is $(-1)^n \alpha_1 \cdots \alpha_n$ and, in general, the coefficient of x^{n-i} is $(-1)^i$ times the value of the i-th symmetric polynomial s_i on the values $\alpha_1, \ldots, \alpha_n$. For $n = 3$, calling the roots α, β, γ, we have

$$a_1 = -(\alpha + \beta + \gamma) \tag{IV.31}$$

$$a_2 = (\alpha\beta + \beta\gamma + \alpha\gamma) \tag{IV.32}$$

$$a_3 = -(\alpha\beta\gamma) \tag{IV.33}$$

Theorem 5.0.22. *Any symmetric polynomial in $x_1, \ldots, x_n$ can be expressed in terms of the elementary symmetric polynomials.*

This can get pretty bogged down in notation so we will first only show the argument for $n = 3$ with variable x, y, z. We say two monic momomials (i.e., with constant coefficient one) have the same *form* if they have the same exponents with the same multiplicities. For any monic monomial $g(x)$ we let $\overline{g(x)}$ denote the sum of all monomials with that form. Thus for a, b, c distinct nonnegative integers

$$\overline{x^a y^b z^c} := x^a y^b z^c + x^a z^b y^c + y^a x^b z^c + y^a z^b x^c + z^a x^b y^c + z^a y^b x^c \tag{IV.34}$$

We do not double count so, for example,

$$\overline{x^2 y^2 z} = x^2 y^2 z + x^2 z^2 y + y^2 z^2 x \tag{IV.35}$$

(That is, we don't count, say, $y^2 x^2 z$ separately. This is only a technical point.) A monoic monomial is determined by the exponents written in decreasing order, that is, $(a_1, \ldots, a_n)$ with $a_1 \geq \ldots \geq a_n \geq 0$) or, for $n = 3$, simply (a, b, c) with $a \geq b \geq c \geq 0$.

Any symmetric polynomial can be expressed as a linear combination of these so it suffices (we are now doing only the case $n = 3$) to write $\overline{x^a y^b z^c}$ in terms of s_1, s_2, s_3. We actually get the expression by reducing to simpler (more on that later) terms.

If a, b, c are positive, simply take out a common factor of $s_3 = xyz$.

If $a = b > 0 = c$ express

$$\overline{x^a y^a} = (xy + xz + xy)^a - \Delta \tag{IV.36}$$

As the other two parts are symmetric their difference Δ is also symmetric. But all the terms in Δ have all three variables and so they can be reduced.

Example 5.0.23. *With $a = b = 2, c = 0$:*

$$(x^2 y^2 + x^2 z^2 + y^2 z^2) = (xy + xz + yz)^2 - 2xyz(x + y + z) \tag{IV.37}$$

If $a > b > 0 = c$ express

$$\overline{x^a y^b} = \overline{x^b y^b} \cdot \overline{x^{a-b}} + \Delta \tag{IV.38}$$

The polynomials $\overline{x^b y^b}$ and $\overline{x^{a-b}}$, being smaller, have already been done. Again, Δ, as the difference of symmetric polynomials, is symmetric and again all terms in Δ have all three variables and so they can be reduced.

Example 5.0.24. *With $a = 5$, $b = 2$, $c = 0$:*

$$\overline{x^5 y^2} = (x^2y^2 + x^2z^2 + y^2z^2)(x^3 + y^3 + z^3) - x^2y^2z^2(x + y + z) \tag{IV.39}$$

Finally when $a > 0 = b = c = 0$ we express

$$x^a + y^a + z^a = (x + y + z)^a + \Delta \tag{IV.40}$$

Again Δ is symmetric, and consists only of terms on two or three variables, which we have already done.

Example 5.0.25. *With $a = 4$, $b = 0$, $c = 0$:*

$$x^4 + y^4 + z^4 = (x + y + z)^4 - 4\overline{x^3 y} - 6\overline{x^2 y^2} - 12xyz(x + y + z) \tag{IV.41}$$

There is a powerful consequence.

Theorem 5.0.26. *Let L be any subfield of $\mathbb{C}$. Let $f(x) \in L[x]$ be a polynomial of degree n with complex roots $\alpha_1, \ldots, \alpha_n$. (For multiple roots we repeat the root.) Then any symmetric polynomial of $\alpha_1, \ldots, \alpha_n$ is in L.*

Proof. From Theorem 5.0.22 we write any symmetric polynomial in terms of the elementary symmetric polynomials and their values are ± the coefficients of $f(x)$, which are in L. □

Example 5.0.27. *Take $L = \mathbb{Q}$ (the main case we shall use) and let α, β, γ be the roots of $f(x) = x^3 + x^2 + 2x + 1$. Consider $\kappa = \alpha^3 + \beta^3 + \gamma^3$. We express*

$$\kappa = (\alpha + \beta + \gamma)^3 - 3(\alpha^2\beta + \cdots + \gamma^2\beta) - 6\alpha\beta\gamma \tag{IV.42}$$

and further reduce

$$\alpha^2\beta + \cdots + \gamma^2\beta) = (\alpha\beta + \alpha\gamma + \beta\gamma)(\alpha + \beta + \gamma) - 3\alpha\beta\gamma \tag{IV.43}$$

We know $\alpha + \beta + \gamma = -1$ and $\alpha\beta + \alpha\gamma + \beta\gamma = 2$ and $\alpha\beta\gamma = -1$ so $\alpha^2\beta + \ldots + \gamma^2\beta = 2(-1) - 3(-1) = 1$ and so $\kappa = (-1)^3 - 3(1) - 6(-1) = 2$.

Lets return to Theorem 5.0.22. How do we turn our arguments into a rigorous proof for a general number of variables n. For each $\vec{a} = (a_1, \ldots, a_n)$ with $a_1 \geq \ldots a_n \geq 0$ let $MM(\vec{a})$ denote the monic polynomial

$$MM(\vec{a}) = \overline{x_1^{a_1} \cdots x_n^{a_n}} \tag{IV.44}$$

We set $D = D(\vec{a}) = a_1 + \ldots a_n$ and call $D(\vec{a})$ the degree of $\vec{a}$. (Note it is the degree of the associated monic polynomial. The idea is to subtract off from $MM(\vec{a})$ some combination of elementary symmetric polynomials so as to be left with simpler forms. We define an ordering on the possible $\vec{a}$. Let $\vec{a} = (a_1, \ldots, a_n)$ and $\vec{b} = (b_1, \ldots, b_n)$ with $a_1 \geq \ldots a_n \geq 0$ and $b_1 \geq \ldots b_n \geq 0$.

1. If $D(\vec{a}) \neq D(\vec{b})$ then the one with the smaller degree is called simpler.

2. Now suppose $b_1 + \ldots + b_n = a_1 + \ldots + a_n$. Let i be the smallest index (it may be that $i = 1$) with $a_i \neq b_i$. If $a_i < b_i$ we then say $\vec{a}$ is simpler than $\vec{b}$, else $\vec{b}$ is simpler.

Among the $\vec{a}$ with the same sum of coordinates, simpler can be thought of as a lexicographical ordering of the possible vectors, thought of as words.

We want to show that, for any $\vec{a}$, $MM(\vec{a})$ can be expressed in terms of the elementary symmetric functions. We do this by a double induction, first on the degree D and then, amongst those of a given degree D, in order of simplicity as given by (2) above. To start the induction, for $D = 1$ the only vector is $\vec{a} = (1, 0, \ldots, 0)$ and $MM(\vec{a}) = s_1$. Now suppose the result is true for all $\vec{b}$ of degree less than D and for all $\vec{b}$ simpler than $\vec{a}$. If $a_n \neq 0$ we reduce by writing

$$MM(\vec{a}) = s_n \cdot MM((a_1 - 1, \ldots, a_n - 1)) \tag{IV.45}$$

That is, we take out the common factor of $s_n = x_1 \cdots x_n$ and are left with something of smaller degree. Now we come to the main case. We write (we assume $a_n = 0$)

$$MM(\vec{a}) = s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_{n-1}^{a_{n-1} - a_n} + \Delta \tag{IV.46}$$

Observe that the product on the RHS is a symmetric polynomial of degree D and so Δ is a symmetric polynomial of degree D and so we only have to check that all of the forms in Δ are simpler than $\vec{a}$.

We pause for an example. Consider $n = 5$ and $\vec{a} = (10, 7, 4, 0, 0)$. Call the variables v, w, x, y, z for convenience. Then (IV.46) becomes

$$\overline{v^{10} w^7 x^4} = (v + w + x + y + z)^3 (vw + \ldots + yz)^3 (vwx + \ldots + xyz)^4 + \Delta \tag{IV.47}$$

Looking at the leftmost terms in the products on the right we get $v^3 (vw)^3 (vwx)^4$ which is precisely the $v^{10} w^7 x^4$ that we want. The general term consists of three from $v, \ldots, z$, three from $vw, \ldots, yz$ and four from $vwx, \ldots, xyz$. One such term would be taking

$$v, v, w; vw, vw, wx, vwx, vwx, vwy, vwy$$

That gives $v^8 w^8 x^3 y^2$ and, indeed, $(8, 8, 3, 2, 0)$ is simpler than $(10, 7, 4, 0, 0)$.

It may be helpful to think of the forms of these monomials in terms of balls in bins. Imagine n bins labelled with the n variables $x_1, \ldots, x_n$. The monomial polynomial $MM(\vec{a})$ corresponds to placing a_i balls in the bin marked x_i Here is a picture corrsponding to the $\vec{a}$ of the example.:

```
x
x
x
x  x
x  x
x  x
```

```
x  x  x
x  x  x
x  x  x
x  x  x
-  -  -  -  -
v  w  x  y  z
```

Now each term from s_i consists of i balls in i different bins. A term in the product consists of placing i balls in i different bins $a_i - a_{i+1}$ times for $1 \le i \le n$. In the example above we have $v^8 w^8 x^3 y^2$ as follows:

```
x
x
   x
x  x
x  x
   x  x
x  x  x
x  x  x
x  x     x
x  x     x
-  -  -  -  -
v  w  x  y  z
```

The claim is that no matter how we place i balls in i different bins $a_i - a_{i+1}$ times for $1 \le i \le n$ we end up with a $\vec{b} = (b_1, \ldots, b_n)$ which is simpler than $\vec{a}$. First look at b_1. We can have at most one ball in a bin from each placement and so

$$b_1 \le (a_1 - a_2) + (a_2 - a_3) + \ldots + (a_{n-1} - a_n) = a_1 \tag{IV.48}$$

Now consider the total number of balls in two bins. We get at most two balls in the two bins from each placement except that the placement of one ball (corresponding to the $a_1 - a_2$ factors of s_1) gives only one ball in the two bins so

$$b_1 + b_2 \le (a_1 - a_2) + 2(a_2 - a_3) + \ldots + 2(a_{n-1} - a_n) = a_1 + a_2 \tag{IV.49}$$

In general, for $1 \le j \le n-1$ consider the total number of balls in any j bins. When $i \le j$ and i balls are placed in i different bins there are at most i balls in those j bins while when $i > j$ there are at most j balls in thos j bins. Thus

$$\sum_{k=1}^{j} b_k \le \sum_{i=1}^{j} i(a_i - a_{i+1}) + j \sum_{i=j+1}^{n-1} (a_i - a_{i+1}) = \sum_{k=1}^{j} a_k \tag{IV.50}$$

But (IV.50), for $1 \le j \le n-1$, implies $\vec{b}$ is simpler than (or equal to) $\vec{a}$. If $\vec{b} \ne \vec{a}$ let j denote the first coordinate for which $b_j \ne a_j$. As $b_k = a_k$ for $k < j$, (IV.50) for j gives $b_j \le a_j$.

6 The Final Piece

Theorem 6.0.28. *Let $F \subset K$ be subfields of $\mathbb{C}$ with K a normal extension of F and $G = Gal(K,F)$. Let H be a subgroup of G and set $L = K^H$. Then $H = G_L$.*

Proof. We already know $H \subset G_L$. Set $[K:L] = r$, express $K = L(\alpha)$. Let $p(x) \in L[x]$ be the minimal polynomial of α. Set $\Lambda = \{\alpha = \alpha_1, \dots, \alpha_r\}$, the set of roots of $p(x)$. Then we can write $H = \{\sigma_1, \dots, \sigma_r\}$ where each $\sigma_i(\alpha) = \alpha_i$ and σ_i permutes $\alpha_1, \dots, \alpha_r$. If H is a proper subset of G_L write $H = \{Id = \sigma_1, \dots, \sigma_s\}$ with $s|r$. Let $t > 1$ be such that $st = r$.

Set $\Lambda_H = \{\sigma_1(\alpha), \dots, \sigma_s(\alpha)\}$. These s elements are distinct as if $\sigma_i(\alpha) = \sigma_j(\alpha)$ then $\sigma_i^{-1}\sigma_j(\alpha) = \alpha$ which, as $K = L(\alpha)$, would imply $\sigma_i^{-1}\sigma_j = e$, or $\sigma_i = \sigma_j$. Further, each of the $\sigma \in H$ permutes Λ_H as for any $\sigma \in H$, $\sigma\sigma_1, \dots, \sigma\sigma_s$ ranges over $\sigma_1, \dots, \sigma_s$. Therefore all symmetric polynomials in Λ_H are fixed by all $\sigma \in H$. But we are assuming that $L = K^H$ so any element fixed by all $\sigma \in H$ must be in L. Let $u_1, \dots, u_s$ denote the values of the i-th symmetric polynomials on $\alpha_1, \dots, \alpha_s$. So these $u_1, \dots, u_s \in L$. But then $\alpha = \alpha_1$ would satisfy the polynomial $x^s - u_1x^{s-1} + \dots + (-1)^s u_s$ which would be a polynomial in $L[x]$ of degree s. This contradicts that, as $K = L(\alpha)$, the minimal polynomial of α in $L[x]$ has degree r. □

This complete the Galois Correspondence Theorem 4.0.13. Theorem 6.0.28 can be restated that for any subgroup H of G applying $K^{(-)}$ and then $G_{(-)}$ gets one back to H. Thus $K^{(-)}$ and $G_{(-)}$ are inverses of each other and give a bijection as desired.

7 Cyclotomic Fields

Lets return to one of our original examples: $K = \mathbb{Q}(\epsilon)$ with $\epsilon = e^{2\pi i/5}$.

The minimal polynomial for ϵ in $\mathbb{Q}[x]$ is $(x^5-1)/(x-1)$ which has roots $\epsilon, \epsilon^2, \epsilon^3, \epsilon^4$ which all all in K. Thus K is the splitting field of that polynomial (over $\mathbb{Q}$) and hence K is normal over $\mathbb{Q}$.

The Galois Group is $(\mathbb{Z}/5\mathbb{Z})^\times$ which is cyclic. Let $\sigma \in Gal(K,F)$ be determined by $\sigma(\epsilon) = \epsilon^2$. Then $\sigma^2(\epsilon) = \epsilon^4$ and $\sigma^3(\epsilon) = \epsilon^8 = \epsilon^3$ and $\sigma^4(\epsilon) = \epsilon^{16} = \epsilon$ so $\sigma^4 = Id$. There is one nontrivial subgroup: $H = \{Id, \sigma^2\}$. From the Galois Correspondence theorem 4.0.13 this means there is one nontrivial intermediate field $\mathbb{Q} \subset L \subset \mathbb{Q}(\epsilon)$ and $L = K^H$. As $2 = |H| = [\mathbb{Q}(\epsilon) : L]$ we have $[L : \mathbb{Q}] = 2$, so L is a quadratic extension of $\mathbb{Q}$.

To find L we look for which $\alpha \in \mathbb{Q}(\epsilon)$ are in K^H. As Id fixes all elements, $\alpha \in \mathbb{Q}(\epsilon)$ if and only if $\sigma^2(\alpha) = \alpha$. Writing $\alpha = a + b\epsilon + c\epsilon^2 + d\epsilon^3$ we must have

$$\alpha = \sigma^2(\alpha) = a + b\epsilon^4 + c\epsilon^8 + d\epsilon^{12} = a + b(-1-\epsilon-\epsilon^2-\epsilon^3) + c\epsilon^3 + d\epsilon^2 \qquad \text{(IV.51)}$$

Equating the coefficients using the basis $1, \epsilon, \epsilon^2, \epsilon^3$ yields the equation system: $a = a - b$, $b = -b$, $c = d - b$, $d = c - b$ which reduces to $b = 0$, $c = d$. Thus the elements of L may be uniquely written as $a + c(\epsilon^2 + \epsilon^3)$. Set $\kappa = \epsilon^2 + \epsilon^3$. As $L = \mathbb{Q}(\kappa)$, κ must satisfy a quadratic. We find it by calculating $\kappa^2 = \epsilon^4 + 2 + \epsilon = 1 - \epsilon^2 - \epsilon^3$. Then $1, \kappa, \kappa^2$ are dependent, more precisely

$\kappa^2 = 1 - \kappa$. Solving the quadratic gives

$$\kappa = \frac{-1 \pm \sqrt{5}}{2} \tag{IV.52}$$

(The actual sign is minus, but this method doesn't tell us that.) Thus we find $L = \mathbb{Q}(\kappa) = \mathbb{Q}(\sqrt{5})$.

When p is an odd prime we can define $K = \mathbb{Q}(\epsilon)$ with $\epsilon = e^{2\pi i/p}$. The minimal polynomial for ϵ is $p(x) = (x^p - 1)/(x-1)$ which has roots $\epsilon, \epsilon^2, \ldots, \epsilon^{p-1}$. Again, K is normal over $\mathbb{Q}$. The Galois Groups $Gal(K, F)$ has automorphisms σ_i given by $\sigma_i(\epsilon) = \epsilon^i$ for each $i \in Z_p^*$ and $\sigma_i \sigma_j = \sigma_{ij}$ where multiplication is done modulo p. Thus $Gal(K, F) \cong (\mathbb{Z}/p\mathbb{Z})^*$. It is known that this is a cyclic group of order $p-1$, so $Gal(K, F) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$. This group has a unique subgroup with half the elements, namely the multiples of 2 (thinking of it as $\mathbb{Z}/(p-1)\mathbb{Z}$). Hence, by the Galois Correspondence Theorem 4.0.13 there is a unique quadratic extension of $\mathbb{Q}$ lying inside of $\mathbb{Q}(\epsilon)$.

Here is a way of finding the square root in $\mathbb{Q}(\epsilon)$ for general odd prime p. Rather than the usual basis $1, \epsilon, \ldots, \epsilon^{p-1}$ we use the basis (`Exercise`: Show this is a basis.) $\epsilon, \epsilon^2, \ldots, \epsilon^{p-1}$. The Galois Group $Gal(\mathbb{Q}(\epsilon), \mathbb{Q})$ consists of σ_i for $1 \le i \le p-1$ where $\sigma_i(\epsilon) = \epsilon^i$. Associating σ_i with $i \in (\mathbb{Z}/p\mathbb{Z})^*$, the group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. The unique subgroup H of $(\mathbb{Z}/p\mathbb{Z})^*$ of index 2 (that is, size $(p-1)/2$) consists of the squares (modulo p). That is H has the automorphisms σ_{k^2} for $1 \le k \le p-1$. (Each square appears twice so there are $(p-1)/2$ elements of H. Now write an arbitrary element $\alpha \in \mathbb{Q}(\epsilon)$ with the new basis as

$$\alpha = \sum_{i=1}^{p-1} a_i \epsilon^i \tag{IV.53}$$

For $\alpha \in K^H$ we need that for each k we have $\sigma_{k^2}(\alpha) = \alpha$. That is,

$$\alpha = \sigma_{k^2}(\alpha) = \sum_{i=1}^{p-1} a_i \epsilon^{k^2 i} \tag{IV.54}$$

Here as $\epsilon^p = 1$ we can consider the exponent $k^2 i$ as calculated in $\mathbb{Z}/p\mathbb{Z}$. Thus the condition becomes

$$a_i = a_{k^2 i} \text{ for all } i, k \in (\mathbb{Z}/p\mathbb{Z})^* \tag{IV.55}$$

But (IV.55) just says that a_i is constant over the quadratic residues and constant (maybe a different constant) over the quadratic nonresidues. (0 is special and is counted neither as a quadratic residue nor as a quadratic nonresidue.) Let $R, N \subset (\mathbb{Z}/p\mathbb{Z})^*$ denote the sets of quadratic residues and quadratic nonresidues respectively. Set

$$\kappa = \sum_{r \in R} \epsilon^r = \frac{1}{2} \sum_{k=1}^{p-1} \epsilon^{k^2} \tag{IV.56}$$

$$\lambda = \sum_{r \in N} \epsilon^r \tag{IV.57}$$

Then κ, λ form a basis for K^H. It is convenient to note that

$$\kappa + \lambda = \sum_{r=1}^{p-1} \epsilon^r = -1 \tag{IV.58}$$

so

$$\lambda = -1 - \kappa \tag{IV.59}$$

and we can replace the basis κ, λ with the basis $1, \kappa$. Thus

$$K^H = \{a + b\kappa : a, b \in Q\} \tag{IV.60}$$

is the unique quadratic extension of $\mathbb{Q}$ inside $\mathbb{Q}(\epsilon)$. Thus κ satisfies a quadratic equation (and is not itself rational) and one can write $\kappa = a_1 + a_2\sqrt{d}$ so that the unique quardatic extension of $\mathbb{Q}$ inside $\mathbb{Q}(\epsilon)$ can be written $\mathbb{Q}(\sqrt{d})$.

One can also find κ explicitly. From (IV.56) we find

$$\kappa^2 = \frac{1}{4} \sum_{x,y=1}^{p-1} \epsilon^{x^2+y^2} \tag{IV.61}$$

This gets into some interesting number theory. For each $r \in \mathbb{Z}/p\mathbb{Z}$ one examines the number of solutions to the equation $x^2 + y^2 = r$ over $\mathbb{Z}/p\mathbb{Z}$ with $x, y \neq 0$. Let r, s both be quadratic residues. Then we can write $s = rt^2$. Each solution $x^2 + y^2 = r$ corresponds to a solution of $x_1^2 + y_1^2 = s$ by setting $x_1 = xt, y_1 = yt$. We can go in the other direction, dividing a solution by t. Thus there is a value, call it R. so that $x^2 + y^2 = r$ has precisely R solutions for every quadratic residue r. Now let r, s both be quadratic nonresidues. Again we can write $r = st^2$ and again the number solutions is the same. Thus there is value value, call it N. so that $x^2 + y^2 = r$ has precisely N solutions for every quadratic nonresidue r. Also, let Z be the number of solutions to $x^2 + y^2 = 0$. We apply (IV.61) to find

$$\kappa^2 = \frac{1}{4}[Z + R\kappa + N\lambda] = \frac{1}{4}[Z + R\kappa + L(-1-\kappa)] = \frac{1}{4}[(Z - L) + (R - L)\kappa] \tag{IV.62}$$

which we can solve by the quadratic formula. Actually, we won't know the choice of ± in the quadratic formula, but in either case we get $\mathbb{Q}(\kappa) = \mathbb{Q}(\sqrt{d})$ for the same explicit d.

Example 7.0.29. *Take $p = 11$ and $\epsilon = e^{2\pi i/11}$. The residues are $1, 4, 9, 16 = 5, 25 = 3$ so the nonresidues are $2, 6, 7, 8, 10$. Then*

$$\kappa = \epsilon + \epsilon^3 + \epsilon^4 + \epsilon^5 + \epsilon^9 \tag{IV.63}$$

Now consider the terms in κ^2, always reducing the exponent modulo 11. We get (this is not always the case!) no terms of ϵ^0. We get $2\epsilon^3\epsilon^9 = 2\epsilon^1$ as well as $2\epsilon^3, 2\epsilon^4, 2\epsilon^5, 2\epsilon^9$. For the nonresidues we get $\epsilon^1\epsilon^1 + 2\epsilon^4\epsilon^9 = 3\epsilon^2$ as well as $3\epsilon^6, 3\epsilon^7, 3\epsilon^8, 3\epsilon^{10}$. Thus

$$\kappa^2 = 2\kappa + 3\lambda = 2\kappa + 3(-1-\kappa) = -3 - \kappa \tag{IV.64}$$

so that

$$\kappa = \frac{-1 \pm \sqrt{-11}}{2} \tag{IV.65}$$

The unique quadratic field inside $\mathbb{Q}(\epsilon)$ *is therefore* $\mathbb{Q}(\sqrt{-11})$.

When $p = 5$ *the quadratic field was* $\mathbb{Q}(\sqrt{5})$ *and when* $p = 11$ *the quadratic field was* $\mathbb{Q}(\sqrt{-11})$. *Coincidence? No! The quadratic field will be* $\mathbb{Q}(\sqrt{p})$ *when* p *is a prime of the form* $4k+1$ *and will be* $\mathbb{Q}(\sqrt{-p})$ *when* p *is a prime of the form* $4k+3$. *But we'll leave this nice fact unproven.*

8 Assorted Consequences

Suppose that an irreducible $p(x) \in \mathbb{Q}[x]$ of degree n has complex roots $\alpha_1, \ldots, \alpha_n$ and we set $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Each $\sigma \in Gal(K,F)$ permutes the roots though not every permutation of the roots yields an automorphism σ.

Suppose ρ is a polynomial function of $\alpha_1, \ldots, \alpha_n$ which is symmetric. Then every $\sigma \in Gal(K,F)$ has $\sigma(\rho) = \rho$. Hence $\rho \in \mathbb{Q}$. As an example suppose a cubic $p(x) \in \mathbb{Q}[x]$ has roots α, β, γ and let

$$\rho = (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2 \tag{IV.66}$$

Any permutation of α, β, γ fixes ρ and hence ρ is a rational number. (FYI: this is called the *discriminant* and generalizes the famous $b^2 - 4a\mathbb{C}$ term with quadratics.)

When ρ is not fully symmetric in $\alpha_1, \ldots, \alpha_n$ there is still some information to be gleaned. Suppose κ is fixed by the alternating group, the even permutations of $\alpha_1, \ldots, \alpha_n$. If $Gal(K,F)$ is contained in the alternating group then $\kappa \in \mathbb{Q}$ as before. Otherwise, $Gal(K,F)$ would have more than $n!/2$ elements and so would be the full symmetric group of $\alpha_1, \ldots, \alpha_n$. In that case κ would not be in $\mathbb{Q}$ since it isn't fixed by all $\sigma \in Gal(K,F)$. Letting H be the alternating group, as $|H| = |G|/2$, $[K^H : Q] = 2$. Then κ would be in a quadratic extension of $\mathbb{Q}$. Continuing the cubic example above, now set

$$\kappa = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \tag{IV.67}$$

Assume $Gal(K,F) \cong S_3$. Of the six permutations of α, β, γ, three send κ to itself and the other three send κ to $-\kappa$ (which is not κ as $\kappa \neq 0$ as α, β, γ are distinct). (For example, if α, β are flipped and γ stays where it is then κ goes to $-\kappa$ but if α goes to β which goes to γ which goes to α then κ goes to κ.) Then $[\mathbb{Q}(\kappa) : Q] = 2$ so κ can be expressed in terms of a square root. Since, further, $\kappa^2 = \rho \in \mathbb{Q}$, κ will be the square root of a rational number.