Introduction to Algebra

Course Notes

Alberto Elduque

Departamento de Matemáticas
Universidad de Zaragoza
50009 Zaragoza, Spain

Contents

Syllabus

Spring Semester 2017

This is a required course for Math Majors at the University of Zaragoza (Science School). It gives 6 credits.

Lecturer: Alberto Elduque
Office: Math. Building. Second floor. Algebra Section. Office no. 2.
e-mail: elduque@unizar.es
http://www.unizar.es/matematicas/algebra/elduque
Office hours: Tuesday and Friday, from 17:00 to 20:00 h.

Course description: The goal of the course is to understand the basic properties of the integers, to consider the abstract systems (rings) satisfying these properties and to study, in particular, the rings of polynomials, and the modules over these rings. The first notions of field extensions will be given too, in order to treat some classical problems: the Fundamental Theorem of Algebra, the resolution by radicals of the equations of low degree and some ancient geometrical problems (doubling the cube, trisecting an angle and squaring the circle).

Exam, exercises: Students are required to prepare and explain to their classmates some of the exercises in these notes. There will be a final exam, which will consist of some questions of a theoretical nature and some exercises.

References:

- J.A. Beachy and W.D. Blair: *Abstract Algebra* (2nd edition), Waveland Press Inc, 1996. There is a web site for this textbook: http://www.math.niu.edu/ beachy/aaol/

- D.S. Dummit and R.M. Foote: *Abstract Algebra* (2nd edition). John Wiley and Sons, 1999.

- J.A. Gallian: *Contemporary Abstract Algebra* (5^{th} edition), Houghton Mifflin, 2000.

- J.J. Rotman: *A First Course in Abstract Algebra* (2^{nd} edition), Prentice Hall, 2000.

- A. Mihailovs and M. May: *Abstract Algebra,* `http://www.mapleapps.com/powertools/abstractalgebra/abstractalgebra.shtml`.

Chapter 0

Integers

By now, you are used to deal with the integers:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

which are endowed with two operations: addition ($+$) and multiplication, and with a total order ($\leq$). In this Chapter some of the well-known properties and definitions related to them will be recalled, mostly without proofs, which you know from the course *Números y Conjuntos*.

§ 1. Division

Here are the main features that have to be taken into account:

- $\leq$ is a well order in $\mathbb{Z}^+ (= \mathbb{N})$. That is, for any $\emptyset \neq S \subseteq \mathbb{N}$, there is an element $m \in S$ such that $m \leq n$ for any $n \in S$. Moreover, for any $a, b, c, d \in \mathbb{Z}$ with $a \leq b$ and $d \geq 0$, it follows that $a + c \leq b + c$ and $ad \leq bd$.

- For any $m, n \in \mathbb{Z}$ with $m \neq 0$, m is said to *divide* n (and written $m \,|\, n$) if there exists a $c \in \mathbb{Z}$ such that $mc = n$.

- **Division algorithm:** For any $a, b \in \mathbb{Z}$, with $b \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that

  $$a = qb + r \qquad \text{and} \qquad 0 \leq r < |b|.$$

  Here $|b|$ denotes the absolute value of b. The integers q and r are called the quotient and the remainder of the division of a by b.

- **Euclidean algorithm:** Given any pair of integers a and b, with $b \neq 0$, iterate the division algorithm until the remainder is 0:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \quad (\text{remainder}= 0) \end{aligned} \qquad 0 < r_n < r_{n-1} < \cdots < |b|$$

  Define $r_{-2} = a$, $r_{-1} = |b|$ and $r_{n+1} = 0$ (note that n can be -1) . Then

$$\begin{aligned} \{\text{common divisors of } a \text{ and } b\} &= \{\text{common divisors of } b \text{ and } r_0\}, \\ &= \cdots \\ &= \{\text{common divisors of } r_{n-1} \text{ and } r_n\}, \\ &= \{\text{divisors of } r_n\}. \end{aligned}$$

  Therefore r_n is the unique natural number that satisfies:

$$\begin{cases} r_n \,|\, a, \ r_n \,|\, b, \\ \text{for any } e \in \mathbb{Z},\ e \,|\, a \text{ and } e \,|\, b \ \Rightarrow\ e \,|\, r_n, \end{cases}$$

  that is, r_n is the *greatest common divisor* of a and b. The notation $r_n = \gcd(a, b)$ or just $r_n = (a, b)$ is used.

- **Bezout's identity:** Given any two nonzero integers a and b, there are integers x and y such that

$$ax + by = \gcd(a, b).$$

  Proof. It is enough to go backwards in the Euclidean Algorithm:

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = (1 + q_{n-1} q_n) r_{n-2} - q_n r_{n-3} \\ &= \cdots \end{aligned}$$

  □

- In the other direction, if $a, b, x, y \in \mathbb{Z}$ are nonzero integers such that $ax + by = 1$, then $\gcd(a, b) = 1$, since any common divisor of a and b is a divisor of $ax + by$. In this situation, a and b are said to be *relatively prime* or *coprime*.

- Let $a, b \in \mathbb{Z} \setminus \{0\}$, then the set of positive common multiples of a and b has a lowest element. Therefore, there exists a unique natural number l such that

$$\begin{cases} a\,|\,l,\ b\,|\,l, \\ \text{for any } e \in \mathbb{Z}, \quad a\,|\,e \text{ and } b\,|\,e \ \Rightarrow\ l\,|\,e, \end{cases}$$

  l is said to be the *lowest (or least) common multiple* of a and b and denoted $\operatorname{lcm}(a, b)$. You already know (but this a good moment to try to prove it by yourself) that for $0 \neq a, b \in \mathbb{Z}$:

$$|ab| = \gcd(a, b) \operatorname{lcm}(a, b).$$

Let us pause to give an example: take $a = 57970$ and $b = 10353$. The Euclidean algorithm gives:

$$\begin{aligned} 57970 &= 5 \times 10353 + 6205 \\ 10353 &= 6205 + 4148 \\ 6205 &= 4148 + 2057 \\ 4148 &= 2 \times 2057 + 34 \\ 2057 &= 60 \times 34 + 17 \\ 34 &= 2 \times 17 \end{aligned}$$

Thus

$$\begin{aligned} \gcd(57970, 10353) = 17 &= 2057 - 60 \times 34 \\ &= 2057 - 60 \times (4148 - 2 \times 2057) \\ &= -60 \times 4148 + 121 \times 2057 \\ &= -60 \times 4148 + 121 \times (6205 - 4148) \\ &= -181 \times 4148 + 121 \times 6205 \\ &= -181 \times (10353 - 6205) + 121 \times 6205 \\ &= -181 \times 10353 + 302 \times 6205 \\ &= -181 \times 10353 + 302 \times (57970 - 5 \times 10353) \\ &= 302 \times 57970 - 1691 \times 10353 \end{aligned}$$

and

$$\operatorname{lcm}(57970, 10353) = \frac{57970 \times 10353}{17} = 3410 \times 10353 = 35303730.$$

There is an easy way to perform the Euclidean algorithm and get the coefficients in Bezout's identity. With $r_n = x_n a + y_n b$ for any $n \geq -2$, let $R_n = (r_n, x_n, y_n)$ ($R_{-2} = (a, 1, 0)$, $R_{-1} = (b, 0, 1)$). Since $r_{n-1} = q_{n+1} r_n +$

r_{n+1}, $0 \leq r_{n+1} \leq r_n$, it turns out that, since $q_{n+1} = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ ($\lfloor x \rfloor$ denotes the largest integer $\leq x$),

$$R_{n+1} = R_{n-1} - \left\lfloor \tfrac{r_{n-1}}{r_n} \right\rfloor R_n.$$

It is helpful to represent this recurrence as the evolution:

$$\begin{pmatrix} R_{-2} \\ R_{-1} \end{pmatrix} \xrightarrow{\tau_1} \begin{pmatrix} R_0 \\ R_{-1} \end{pmatrix} \xrightarrow{\tau_2} \begin{pmatrix} R_0 \\ R_1 \end{pmatrix} \xrightarrow{\tau_1} \begin{pmatrix} R_2 \\ R_1 \end{pmatrix} \xrightarrow{\tau_2} \cdots$$

with

$$\tau_1 : \begin{pmatrix} R_{n-1} \\ R_n \end{pmatrix} \longrightarrow \begin{pmatrix} R_{n-1} - \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor R_n \\ R_n \end{pmatrix}$$

$$\tau_2 : \begin{pmatrix} R_n \\ R_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} R_n \\ R_{n-1} - \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor R_n \end{pmatrix}$$

In the previous example we get

$$\begin{aligned} \begin{pmatrix} 57970 & 1 & 0 \\ 10353 & 0 & 1 \end{pmatrix} &\longrightarrow \begin{pmatrix} 6205 & 1 & -5 \\ 10353 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 6205 & 1 & -5 \\ 4148 & -1 & 6 \end{pmatrix} \\ &\longrightarrow \begin{pmatrix} 2057 & 2 & -11 \\ 4148 & -1 & 6 \end{pmatrix} \longrightarrow \begin{pmatrix} 2057 & 2 & -11 \\ 34 & -5 & 28 \end{pmatrix} \\ &\longrightarrow \begin{pmatrix} 17 & 302 & 1791 \\ 34 & -5 & 28 \end{pmatrix} \longrightarrow \begin{pmatrix} 17 & 302 & -1691 \\ 0 & -609 & 3410 \end{pmatrix} \end{aligned}$$

so $17 = \gcd(57970, 10353) = 302 \times 57970 - 1691 \times 10353$.

- An integer $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is said to be *prime* if given any $a, b \in \mathbb{Z}$ such that $p \,|\, ab$, either $p \,|\, a$ or $p \,|\, b$. Otherwise, p is said to be *composite*.

  A word of caution is needed here. This definition is different from the one you saw in the course *Números y Conjuntos*. Let us see that both definitions are equivalent:

1.1 Theorem. *Let $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Then p is prime if and only if the only divisors of p are ± 1 and $\pm p$.*

Proof. $\Rightarrow$) Assume that p is prime and, without loss of generality, positive. If $1 < a < p$ and $a \,|\, p$, then there is a $b \in \mathbb{Z}$ such that $p = ab$, so $p \,|\, a$ or $p \,|\, b$, a contradiction since both a and b are smaller than p. Therefore, the only divisors of p are ± 1 and $\pm p$.

$\Leftarrow$) Assume that $p \mid ab$ but $p \nmid a$. Then $\gcd(p, a) = 1$ since the only divisors of p are ± 1 and $\pm p$. By Bezout's identity, there are $x, y \in \mathbb{Z}$ such that $1 = xp + ya$, so $b = xpb + yab$ is a multiple of p, because so are p and ab. $\square$

- There are infinitely many prime numbers.

To end this section, let us recall the **Fundamental Theorem of Arithmetic**:

1.2 Theorem. *Any natural number $n > 1$ can be factored in a unique way as a product of positive prime numbers:*

$$n = p_1^{a_1} \cdots p_r^{a_r}$$

($a_1, \ldots, a_r \in \mathbb{N}$).

Besides, if a and b are natural numbers, then there are positive prime numbers $p_1, \ldots, p_r$ and integers $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\}$ such that $a = p_1^{a_1} \cdots p_r^{a_r}$ and $b = p_1^{b_1} \cdots p_r^{b_r}$. Then:

$$\begin{cases} \gcd(a,b) = p_1^{\min\{a_1,b_1\}} \cdots p_r^{\min\{a_r,b_r\}} \\ \operatorname{lcm}(a,b) = p_1^{\max\{a_1,b_1\}} \cdots p_r^{\max\{a_r,b_r\}} \end{cases}$$

§ 2. Congruences

Given a natural number n, define a relation in $\mathbb{Z}$ by means of:

$$a \sim b \qquad \text{if} \qquad n \,|\, b - a.$$

The usual notation for $a \sim b$ is $a \equiv b \pmod{n}$ (read as *a is congruent to b modulo n*.

- $\sim$ is an equivalence relation.
- For any $a \in \mathbb{Z}$, its equivalence class is $\bar{a} = \{a + kn : k \in \mathbb{Z}\}$.
- There are exactly n equivalence classes: $\bar{0}, \ldots, \overline{n-1}$. The quotient set is denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$.
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ ac &\equiv bd \pmod{n} \end{aligned}$$

  so we may define an addition and a multiplication on $\mathbb{Z}/n\mathbb{Z}$ by means of:

$$\begin{aligned} \bar{a} + \bar{b} &= \overline{a+b} \\ \bar{a}\bar{b} &= \overline{ab} \end{aligned}$$

2.1 Example. What are the last two digits of 2^{1000}?

Since any natural number is congruent modulo 100 to the number formed by the last two digits, we compute the class of 2^{1000} modulo 100, taking advantage of the remarks above:

$$\begin{aligned} &2^{10} = 1024 \equiv 24 \pmod{100}, \\ &2^{12} = 2^{10}2^2 \equiv 24 \times 4 = 96 = -4 = -2^2 \pmod{100}, \\ &2^{20} = 2^{12}2^8 \equiv -2^2 2^8 = -2^{10} \pmod{100}. \end{aligned}$$

Thus, if $a = 2^{10}$, then $a^2 \equiv -a \pmod{100}$, so

$$2^{1000} = a^{100} \equiv (-1)^{99} a = -a \equiv -24 \equiv 76 \pmod{100}$$

and the answer is 76.

2.2 Theorem. ***(Chinese Remainder Theorem)*** *Let $m_1, \ldots, m_r$ be natural numbers such that any two of them are coprime, and let $x_1, \ldots, x_r \in \mathbb{Z}$. Then the system of linear congruences*

$$\begin{aligned} z &\equiv x_1 \pmod{m_1} \\ &\vdots \\ z &\equiv x_r \pmod{m_r} \end{aligned}$$

has a solution. Moreover, if z_1 and z_2 are two solutions, then $z_1 \equiv z_2 \pmod{m_1 \cdots m_r}$.

Proof. Write $m = m_1 \cdots m_r$ and for any $i = 1, \ldots, r$ let $s_i = \dfrac{m}{m_i} = m_1 \cdots \hat{i} \cdots m_r$. By our assumptions, $\gcd(m_i, s_i) = 1$ for any $i = 1, \ldots, r$, so there are integers a_i, b_i such that $a_i m_i + b_i s_i = 1$ for any i. Let $u_i = b_i s_i$, then

$$\begin{cases} u_i \equiv 1 \pmod{m_i}, \\ u_i \equiv 0 \pmod{s_i}, \text{ so } u_i \equiv 0 \pmod{m_j} \quad \forall j \neq i. \end{cases}$$

Let $z = x_1 u_1 + \cdots + x_r u_r$, then for any $i = 1, \ldots, r$:

$$z = x_1 u_1 + \cdots + x_r u_r \equiv x_1 \cdot 0 + \cdots + x_i \cdot 1 + \cdots + x_r \cdot 0 = x_i \pmod{m_i},$$

so that z is a solution.

Moreover, if z_1 and z_2 are two solutions, then $z_1 - z_2 \equiv x_i - x_i = 0 \pmod{m_i}$ for any i, so that $m_i \mid z_1 - z_2$ and hence $m = m_1 \cdots m_r = \operatorname{lcm}(m_1, \ldots, m_r) \mid z_1 - z_2$. Thus $z_1 \equiv z_2 \pmod{m}$. □

An important subset of $\mathbb{Z}/n\mathbb{Z}$ is the subset of its *invertible elements*:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{b} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{a}\bar{b} = \bar{1} \right\}$$

2.3 Proposition.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}.$$

(Notice that $\gcd(0,n) = n$ for any $0 \neq n \in \mathbb{Z}$.)

Proof. First, if $\gcd(a,n) = 1$, by Bezout's identity there are integeres $x, y \in \mathbb{Z}$ such that $ax + ny = 1$ so, as $\bar{n} = \bar{0}$, $\bar{a}\bar{x} = \overline{ax} = \bar{1}$ and $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Conversely, if $\bar{a}\bar{b} = \bar{1}$, then $n \,|\, 1-ab$, so there is an $x \in \mathbb{Z}$ with $1-ab = nx$. Then $1 = ab + nx$, and this forces $\gcd(a,n)$ to be 1. □

2.4 Definition. The map

$$\begin{aligned} \phi : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\mapsto \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| \ \Big(= |\{0 \leq x < n : \gcd(x,n) = 1\}|\Big) \end{aligned}$$

is called the *Euler map.*

Properties of the Euler map:

(i) $\phi(1) = 1$, $\phi(p^k) = p^k - p^{k-1}$ for any $p, k \in \mathbb{N}$ with p prime.

This is because in the 'interval' $0 \leq x < p$ there are p^{k-1} multiples of p: $0, p, 2p, \ldots, (p^{k-1}-1)p$.

(ii) If $m_1, m_2 \in \mathbb{N}$ and $\gcd(m_1, m_2) = 1$, then $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$.

Proof. Let f be the map from $\{0 \leq z < m_1 m_2 : \gcd(z, m_1 m_2) = 1\}$ into the cartesian product $\{0 \leq x < m_1 : \gcd(x, m_1) = 1\} \times \{0 \leq y < m_2 : \gcd(y, m_2) = 1\}$, given by $f(z) = (x, y)$, where

$$\begin{cases} x \text{ is the remainder of the division of } z \text{ by } m_1, \\ y \text{ is the remainder of the division of } z \text{ by } m_2. \end{cases}$$

f is well defined because there are elements $a, b, q_1, q_2 \in \mathbb{Z}$ such that $1 = az + bm_1m_2$, $z = q_1m_1 + x$ and $z = q_2m_2 + y$. Hence $1 = ax + (bm_2 + aq_1)m_1$ and $1 = ay + (bm_1 + aq_2)m_2$, so that $\gcd(x, m_1) = 1 = \gcd(y, m_2)$. Now, the Chinese Remainder Theorem assures us that f is a bijection. □

(iii) For any $n \in \mathbb{N}$, $\phi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$.

Proof. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorization of n; then, by the two previous properties:

$$\phi(n) = \prod_{i=1}^{r} \left(p_i^{a_i} - p_i^{a_i - 1} \right) = \prod_{i=1}^{r} p_i^{a_i} \left(1 - \frac{1}{p_i} \right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right),$$

as required. □

(iv) For any $n \in \mathbb{N}$, $n = \sum_{0<d|n} \phi(d)$.

Proof. By joining together the elements in $\{1, \ldots, n\}$ with the same greatest common divisor with n, one obtains that $n = \sum_{0<d|n} n_d$, with $n_d = |\{0 < x \leq n : \gcd(x, n) = d\}|$. But if $\gcd(x, n) = d$ with $0 < x \leq n$, then $x = yd$ with $0 < y \leq \dfrac{n}{d}$ and $\gcd\left(y, \dfrac{n}{d}\right) = 1$, so that $n_d = \phi\left(\dfrac{n}{d}\right)$ and the result follows. □

We finish our review of the Integers with a classical result that has become very important for Criptography in recent times, as we will see in the computer lab.

2.5 Theorem. ***(Euler's Theorem)*** *Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ such that $\gcd(x, n) = 1$. Then*

$$\boxed{x^{\phi(n)} \equiv 1 \pmod{n}}$$

Proof. If $n = 1$ this is trivial, so we will assume that $n \geq 2$. Let $r = \phi(n)$ and let $\{z_1, \ldots, z_r\} = \{0 < y < n : \gcd(y, n) = 1\}$, so that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{z}_1, \ldots, \bar{z}_r\}$. Since $\gcd(x, n) = 1$, there is an element $y \in \mathbb{Z}$ such that $\bar{x}\bar{y} = \bar{1}$. Therefore the map

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \bar{u} &\mapsto \bar{x}\bar{u} \end{aligned}$$

is a bijection, whose inverse is 'the multiplication by $\bar{y}$'. Therefore

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{z}_1, \ldots, \bar{z}_r\} = \{\bar{x}\bar{z}_1, \ldots, \bar{x}\bar{z}_r\}$$

and in $\mathbb{Z}/n\mathbb{Z}$,

$$\bar{z}_1 \cdots \bar{z}_r = (\bar{x}\bar{z}_1) \cdots (\bar{x}\bar{z}_r) = \bar{x}^r (\bar{z}_1 \cdots \bar{z}_r).$$

Let $z = z_1 \cdots z_r$, then $\gcd(z, n) = 1$ and $\bar{z} = \bar{x}^r \bar{z}$. But since $\bar{z}$ has an 'inverse' in $\mathbb{Z}/n\mathbb{Z}$, it follows that $\bar{x}^r = \bar{1}$ or, what is the same, $x^r \equiv 1 \pmod{n}$, as required. □

2.6 Corollary. ***(Fermat's Little Theorem)*** *Let $p \in \mathbb{N}$ be a prime number and let $x \in \mathbb{Z}$. Then $x^p \equiv x \pmod{p}$.*

Moreover, if $p \nmid x$ then $x^{p-1} \equiv 1 \pmod{p}$.

Proof. If $p \mid x$, then $x \equiv 0 \pmod{p}$, so that $x^p \equiv 0 \equiv x \pmod{p}$ and we are done. Otherwise, $p \nmid x$, so $\gcd(x, p) = 1$ as p is prime. Then by Euler's Theorem $x^{p-1} \equiv 1 \pmod{p}$ and thus $x^p \equiv x^{p-1}x \equiv 1x = x \pmod{p}$. □

Exercises

1. For any of the following pairs of natural numbers a and b, compute its greatest common divisor, least common multiple and integers x and y with $ax + by = \gcd(a, b)$:

   (a) $a = 1761$, $b = 1567$.

   (b) $a = 507885$, $b = 60808$.

2. Given a positive prime number p, prove that $\sqrt{p}$ is not a rational number.

3. Let $a \in \mathbb{N}$, so that $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$, with $0 \leq a_i < 10$ for any $i = 0, \ldots, n$. Prove that $a \equiv a_0 + a_1 + \cdots + a_n \pmod{9}$. Deduce from this the *rule of 9* for checking the correctness of multiplications.

4. Let a be as in the previous exercise. Prove that $a \equiv a_0 - a_1 + \cdots \pm a_n \pmod{11}$.

5. Let $a, b \in \mathbb{Z}$:

   (a) Prove that $10a + b$ is a multiple of 7 if and only if so is $a - 2b$.

   (b) Prove that $10a + b$ is a multiple of 13 if and only if so is $a + 4b$.

6. Compute the remainder of the division of 37^{100} by 29.

7. Compute the last two digits of 9^{1500}.

8. Compute the last digit of $99999^{9999^{999^{99^9}}}$.

9. Check that there are no squares whose last digit is 2, 3, 7 or 8.

10. Check that the square of any odd number gives remainder 1 when divided by 8.

11. Is $\dfrac{7^{1968^{1978}} - 3^{68^{78}}}{1978 - 1968}$ an integer?

12. Let $a, b \in \mathbb{Z}$. Prove that the division of $a^2 + b^2$ by 4 never gives remainder 3.

13. Prove that there are no integers a, b, c, not all of them 0, such that $a^2 + b^2 = 3c^2$.

14. For any of the following pairs of integers a and n, check if they are coprime and find the 'inverse of a modulo n' (that is, $1 \leq x < n$ such that $ax \equiv 1 \pmod{n}$):

    (a) $a = 13$, $n = 20$,

    (b) $a = 69$, $n = 89$.

    (c) $a = 1891$, $n = 3797$,

    (d) $a = 6003722857$, $n = 77695236973$.

15. With stamps of 15 and 21 cents, can you prepare a postage of 2 euros and 11 cents? and of 2 euros and 13 cents?

[13] Reduce modulo 4.

Chapter 1

Rings

The purpose of this chapter is the study of those sets that, like the integers, are endowed with two operations: addition and multiplication, satisfying the usual properties. Many of the properties satisfied by these sets are obtained with the same arguments used for the integers, so some of the (easy) proofs will be omitted.

§ 1. Definitions and examples

1.1 Definition. A *ring* is a set R, endowed with two binary operations:

addition: $R \times R \to R$, $(a, b) \mapsto a + b$, and

multiplication: $R \times R \to R$, $(a, b) \mapsto ab$,

satisfying the following properties:

(i) The addition is associative, commutative, R contains a neutral element for it (this is called the *zero* element and denoted by 0) and any element has an opposite element (the opposite of a is denoted by $-a$).

(ii) The multiplication is associative and distributive relative to the addition.

1.2 Remark. If R is a ring and only the addition is taken into account, then it forms an *abelian group*.

1.3 Definition.

- A ring R is said to be *commutative* if its multiplication is commutative.
- A ring R is said to be *unital* if there is a neutral element for its multiplication, which is denoted by 1, and $1 \neq 0$. Thus, $1a = a1 = a$ for any $a \in R$.

- A ring R is said to be a *division ring* if it is unital and for any $0 \neq a \in R$, there is an inverse for a (denoted by a^{-1}), that is, $aa^{-1} = a^{-1}a = 1$.
- A commutative division ring is called a *field*.

1.4 Examples.

(i) $\mathbb{Z}$ is a unital commutative ring, but it is not a field.

(ii) $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

(iii) $\mathbb{Z}/n\mathbb{Z}$ is a unital commutative ring. Moreover, the set of nonzero elements that have an inverse is precisely $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore,

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ is a field if and only if } n \text{ is prime}}$$

(iv) **Hamilton quaternions** (1843)
$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ (real vector space with basis $\{1, i, j, k\}$). The addition in $\mathbb{H}$ is its addition as a vector space, while the multiplication of two elements is obtained by the distributive property and by applying the rules:

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

$\mathbb{H}$ is a division ring with

$$(a + bi + cj + dk)^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk),$$

but it is not a field.

(v) If F is a field, then

$$\begin{aligned} F[X] &= \{\text{polynomials with coefficients in } F\} \\ &= \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{Z}_{\geq 0},\ a_0, \ldots, a_n \in F\} \end{aligned}$$

is a unital commutative ring and, as for $\mathbb{Z}$, there is a 'division algorithm' for polynomials. For any $p(X) \in F[X]$ and $0 \neq q(X) \in F[X]$, there are unique polynomials $c(X), r(X) \in F[X]$ such that $p(X) = c(X)q(X) + r(X)$ and either $r(X) = 0$ or the degree of $r(X)$ is strictly smaller than the degree of $q(X)$. Then, as in $\mathbb{Z}$, this gives a 'Euclidean algorithm' to compute the greatest common divisor, ...

(vi) Given any interval I on the real line, the sets of functions:

$$\begin{aligned} \mathcal{C}(I, \mathbb{R}) &= \{f : I \to \mathbb{R} : f \text{ is continuous}\} \\ \mathcal{D}(I, \mathbb{R}) &= \{f : I \to \mathbb{R} : f \text{ has a derivative at any point}\} \end{aligned}$$

are unital commutative rings with the usual addition and multiplication of functions.

(vii) If F is a field, $\mathrm{Mat}_n(F)$ (the $n \times n$ square matrices over F) is a unital ring. If $n \geq 2$, $\mathrm{Mat}_n(F)$ is not commutative.

(viii) If R_1 and R_2 are rings, so is its cartesian product $R_1 \times R_2$, where the operations are defined componentwise. This is called the *direct product* of the rings R_1 and R_2. The same happens with the cartesian product of any family of rings.

1.5 'Silly' properties of rings. You should be able to prove these without help:

(i) $0a = a0 = 0$ for any $a \in R$.

(ii) $(-a)b = a(-b) = -(ab)$ for any $a, b \in R$.

(iii) $(-a)(-b) = ab$ for any $a, b \in R$. (This is a consequence of (ii).)

(iv) If R is unital, then $-a = (-1)a$ for any $a \in R$. (This too is a consequence of (ii).)

Given any ring R, for any $a \in R$ and $n \in \mathbb{N}$, the following notation will be used:

$$na = a + \cdots + a \quad (-n)a = (-a) + \cdots + (-a) \quad (n \text{ summands}).$$

1.6 Definition. Let R be a ring.

(i) An element $0 \neq a \in R$ is said to be a *zero divisor* if there exists $0 \neq b \in R$ such that $ab = 0$ or $ba = 0$.

(ii) If R is unital and $u \in R$, u is said to be a *unit* or an *invertible element* if there exists $v \in R$ such that $uv = 1 = vu$. The subset of R formed by its units is denoted by $R^\times$.

(iii) R is said to be an *integral domain* if it is commutative, unital and contains no zero divisors.

1.7 Examples.

- $\mathbb{Z}$ is an integral domain and $\mathbb{Z}^\times = \{\pm 1\}$.
- Let $R = \{f : [0,1] \to \mathbb{R} : f \text{ is continuous}\}$ and let $f, g \in R$ defined by means of:

$$f(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \text{if } \frac{1}{2} \leq x \leq 1 \end{cases} \qquad g(x) = \begin{cases} -x + \frac{1}{2} & \text{if } 0 \leq x \leq \frac{1}{2} \\ 0 & \text{if } \frac{1}{2} \leq x \leq 1 \end{cases}$$

  Then $f \neq 0 \neq g$ but $fg = 0$, so f and g are zero divisors.

1.8 Not so 'silly' properties. Let R be a ring. Then:

(i) If R is unital and $a \in R$ is a zero divisor, then a is not a unit. In particular, any field is an integral domain.

Proof. If $ab = 0$ and $ac = ca = 1$, then $0 = c(ab) = (ca)b = 1b = b$. □

(ii) Let $0 \neq a \in R$. If a is not a zero divisor, then one may simplify by a. That is, for any $b, c \in R$, if $ab = ac$, then $b = c$ and if $ba = ca$, then $b = c$ too.

Proof. If $ab = ac$, then $a(b - c) = 0$ and, since a is not a zero divisor, $b - c = 0$, or $b = c$. □

A word of caution here: *zero divisors cannot be simplified!!* For instance, $\bar{2} \times \bar{2} = \bar{4} = \bar{2} \times \bar{8}$ in $\mathbb{Z}/12\mathbb{Z}$, but $\bar{2} \neq \bar{8}$.

(iii) Any finite integral domain is a field.

Proof. Let R be a finite integral domain and $0 \neq a \in R$. Consider the left multiplication by a:

$$\begin{aligned} L_a : R &\to R \\ x &\mapsto ax. \end{aligned}$$

Since a is not a zero divisor, this is one-to-one. But any one-to-one map between two finite sets with the same number of elements is also onto. Therefore there is a $b \in R$ such that $ab = 1 (= ba)$ (R is commutative). Thus any nonzero element has a multiplicative inverse. Hence R is a field. □

1.9 Example. Let R be a unital commutative ring. Then the polynomials in X with coefficients in R also form a unital commutative ring, denoted by $R[X]$. Besides, if R is an integral domain, then:

- $\forall p(X), q(X) \in R[X] \setminus \{0\}$, $\deg(p(X)q(X)) = \deg p(X) + \deg q(X)$,
- $R[X]^\times = R^\times$.
- $R[X]$ is an integral domain too.

1.10 Definition. A *subring* of a ring R is a nonempty subset of R that is closed for the addition, multiplication and opposites.

That is, if $\emptyset \neq S \subseteq R$, S is a *subring* of R if for any $a, b \in S$, also, $a + b \in S$, $ab \in S$ and $-a \in S$.

In particular, for any $a \in S$, $0 = a + (-a) \in S$, so S becomes a ring with the addition and multiplication inherited from R. This situation is written $S \leq R$.

1.11 Examples.

(i) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$.

(ii) For any unital commutative ring R, $R \leq R[X]$.

(iii) $\mathcal{D}(I, \mathbb{R}) \leq \mathcal{C}(I, \mathbb{R})$, for any real interval I.

(iv) $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k \leq \mathbb{H}$.

§ 2. Homomorphisms and ideals

2.1 Definition. Let R and S be two rings and let $\varphi : R \to S$ be a map. Then:

- φ is said to be a *ring homomorphism* (or just a homomorphism) if for any $a, b \in R$,

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = \varphi(a)\varphi(b).$$

- If φ is a ring homomorphism, then its *kernel* is the subset $\ker \varphi = \varphi^{-1}(0)$ of R, while its *image* is the set $\operatorname{im} \varphi = \varphi(R)$.

- A ring homomorphism is said to be a *monomorphism* if it is one-to-one, an *epimorphism* if it is surjective, and an *isomorphism* if it is a bijection. Moreover, the isomorphisms $\psi : R \to R$ are called *automorphisms*.

2.2 Examples.

(i) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, given by $\varphi(x) = \bar{x}$ is an epimorphism, with kernel
$$\ker \varphi = \bar{0} = n\mathbb{Z} = \{nx \in \mathbb{Z} : x \in \mathbb{Z}\}.$$

(ii) The map $\psi : \mathbb{Z} \to \mathbb{Z}$, given by $\psi(x) = 2x$, is NOT a homomorphism.

(iii) Given any unital commutative ring R and any element $a \in R$, the map $\varphi : R[X] \to R$, $p(X) \mapsto p(a)$ is a homomorphism, called *evaluation homomorphism*.

You should be able to prove the following:

2.3 Properties. *Let $\varphi : R \to S$ be a ring homomorphism. Then:*

(i) $\varphi(0) = 0$ *and* $\varphi(-a) = -\varphi(a)$ *for any* $a \in R$.

(ii) $\operatorname{im}\varphi$ *is a subring of* S.

(iii) $\ker\varphi$ *is a subring of* R *that satisfies that for any* $a \in R$ *and* $x \in \ker\varphi$, $ax, xa \in \ker\varphi$.

These properties satisfied by the kernel of any homomorphism deserve a recognition:

2.4 Definition. Let R be a ring and I a nonempty subset of R.

- I is said to be a *left ideal* (respectively *right ideal*) of R if it is a subring of R and for any $a \in R$ and $x \in I$, $ax \in I$ (respectively, $xa \in I$). The notation $I \trianglelefteq_{\text{left}} R$ (respectively $I \trianglelefteq_{\text{right}} R$) will be used.

- I is said to be an *ideal* of R if it is both a left and a right ideal of R. In this case, we write $I \trianglelefteq R$.

Notice that for commutative rings, left ideals, right ideals or ideals are the same thing.

2.5 Examples.

1. Let us compute the ideals of $\mathbb{Z}$. First of all, $\{0\}$ is clearly an ideal (which, by abuse of notation, is denoted simply by 0), something that is valid for any ring. Now, let $0 \neq I \trianglelefteq \mathbb{Z}$ and let n be the least natural number in I (notice that if $-n \in I$, then also $n = -(-n) \in I$). Then for any $x \in I$, there are integers c and r such that $x = cn + r$ and $0 \leq r < n$. But $x, n \in I$, so $r = x - cn \in I$. From our hypotheses on n, we must have $r = 0$. Therefore I consists of multiples of n and hence $I = n\mathbb{Z}$.

   Thus
   $$\boxed{\{\text{Ideals of } \mathbb{Z}\} = \{n\mathbb{Z} : n \in \mathbb{N} \cup \{0\}\}}$$

2. Let F be a field, $n > 1$ an integer and $R = \operatorname{Mat}_n(F)$. For any $j = 1, \ldots, n$, let R_j be the set of those matrices in R whose entries not in the j^{th} row are all 0 and, in the same vein, let C_j be the set of those matrices in R whose entries not in the j^{th} column are all 0. Then
   $$R_j \trianglelefteq_{\text{right}} R, \quad C_j \trianglelefteq_{\text{left}} R,$$
   but
   $$R_j \not\trianglelefteq_{\text{left}} R, \quad C_j \not\trianglelefteq_{\text{right}} R.$$

Now we arrive at one of the most important concepts in Ring Theory.

Let R be a ring and I an ideal of R. Consider the binary relation on R defined by

$$a \sim b \quad \text{if} \quad a - b \in I, \tag{2.6}$$

for any $a, b \in R$. Then $\sim$ is an equivalence relation. The equivalence class of any $a \in R$ is the set

$$a + I = \{a + r : r \in I\}.$$

The quotient set (that is, the set of equivalence classes) is denoted by R/I.

Moreover, if $a, b, c, d \in R$ and $a \sim c$, $b \sim d$, then also $a + b \sim c + d$ and $ab \sim cd$, so an addition and a multiplication can be defined on R/I by means of:

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I,\\ (a + I)(b + I) &= ab + I.\end{aligned}$$

With these two operations, the quotient set R/I is a ring, which is called the *quotient ring* of R by I.

The ring $\mathbb{Z}/n\mathbb{Z}$ developed in Chapter 0 is just an instance of quotient ring.

2.7 Properties. *Let R and S be two rings.*

- ***First Isomorphism Theorem:*** *Let $\varphi : R \to S$ be a homomorphism, then the quotient ring $R/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$ through the isomorphism*

$$\begin{aligned}\bar{\varphi} : R/\ker\varphi &\to \operatorname{im}\varphi\\ a + \ker\varphi &\mapsto \varphi(a).\end{aligned}$$

- *Let I be an ideal of R, then the map $\pi : R \to R/I$, $a \mapsto a + I$, is an epimorphism, called the* natural projection *of R over R/I. Besides, $\ker\pi = I$. In particular, this shows that any ideal is the kernel of some homomorphism.*

- *Let $\varphi : R \to S$ be a homomorphism, then*

$$\boxed{\begin{aligned}\varphi \text{ is a monomorphism} &\iff \ker\varphi = 0,\\ \varphi \text{ is an epimorphism} &\iff \operatorname{im}\varphi = S.\end{aligned}}$$

- ***Second Isomorphism Theorem:*** *Let A be a subring and I an ideal of R, then $A + I = \{a + x : a \in A, x \in I\}$ is a subring of R, $A \cap I$ is an ideal of A and the map*

$$\begin{aligned}A/A \cap I &\to A + I/I\\ a + A \cap I &\mapsto a + I,\end{aligned}$$

is an isomorphism.

Proof. The map $A \to A + I/I$, $a \mapsto a + I$ is clearly an epimorphism with kernel $A \cap I$. Now the First Isomorphism Theorem applies. □

- ***Third isomorphism theorem:*** *Let I and J be two ideals of R with $I \subseteq J$, then J/I is an ideal of R/I and the quotient rings $(R/I)/(J/I)$ and R/J are isomorphic.*

  Proof. The map $R/I \to R/J$, $a + I \mapsto a + J$ is an epimorphism with kernel J/I and again the First Isomorphism Theorem applies. □

- *Let I be an ideal of R, then the map*

$$\begin{aligned} \{\textit{subrings of } R \textit{ containing } I\} &\to \{\textit{subrings of } R/I\} \\ S &\mapsto S/I, \end{aligned}$$

  is a bijection. The inverse map is given by $\tilde{S} \leq R/I \mapsto S = \{a \in R : a + I \in \tilde{S}\}$. The same result is valid changing subrings for ideals.

Some more properties of ideals and homomorphisms are given in the next result:

2.8 Proposition. *Let R be a unital ring. Then:*

(i) *If I is an ideal of R, then $I = R$ if and only if I has a unit.*

(ii) *If R is commutative, then R is a field if and only if R has no proper ideals. (An ideal I is said to be* proper *if $I \neq 0, R$.)*

(iii) *Let R be a field and let $\varphi : R \to S$ be a nonzero homomorphism. Then φ is a monomorphism.*

Let R be a ring and let A be a subset of R, consider the following subsets of R:

$$\begin{aligned} RA &= \{r_1a_1 + \cdots + r_na_n : n \in \mathbb{N}, r_i \in R, a_i \in A\, \forall i\}, \\ AR &= \{a_1r_1 + \cdots + a_nr_n : n \in \mathbb{N}, r_i \in R, a_i \in A\, \forall i\}, \\ RAR &= \{r_1a_1r_1' + \cdots + r_na_nr_n' : n \in \mathbb{N}, r_i, r_i' \in R, a_i \in A\, \forall i\}. \end{aligned}$$

where, by convention, $R\emptyset = \emptyset R = R\emptyset R = 0$.

2.9 Proposition. *Let R be a unital ring and let A be a subset of R, then:*

- *RA is the smallest left ideal of R containing A.*
- *AR is the smallest right ideal of R containing A.*

- *RAR is the smallest ideal of R containing A.*

Under the conditions of 2.9, RA (respectively AR, RAR) is said to be the left ideal (respectively right ideal, ideal) *generated* by A.

If $A = \{a\}$ or $A = \{a_1, \ldots, a_n\}$ then one writes $RAR = (a)$ or $(a_1, \ldots, a_n)$.

2.10 Definition. Let R be a unital ring and let I be an ideal of R such that there exists $a \in R$ (respectively $a_1, \ldots, a_n \in R$) with $I = (a)$ (respectively $I = (a_1, \ldots, a_n)$), then I is said to be *principal* (respectively *finitely generated*).

2.11 Examples.

- In $\mathbb{Z}$ every ideal is principal.
- Let us see that the ideal $(2, X)$ of $\mathbb{Z}[X]$ is not principal. First notice that

$$\begin{aligned}(2, X) &= \{2p(X) + Xq(X) : p(X), q(X) \in \mathbb{Z}[X]\} \\ &= \{p(X) \in \mathbb{Z}[X] : p(0) \text{ is even}\}.\end{aligned}$$

  If there would exist a polynomial $a(X) \in \mathbb{Z}[X]$ such that $(2, X) = \big(a(X)\big)$, then $2 \in \big(a(X)\big)$, so there would exist $p(X) \in \mathbb{Z}[X]$ with $2 = a(X)p(X)$, but then the degree of $a(X)$ would be 0 and $a(X) = \pm 1$ or $a(X) = \pm 2$. In the first case $\big(a(X)\big) = \mathbb{Z}[X]$, while in the second case $X \notin \big(a(X)\big)$, a contradiction.

2.12 Definition. Let R be a ring and let M be an ideal of R with $M \neq R$. Then M is said to be *maximal* if the only ideal of R containing strictly M is the whole R.

2.13 Example. In $\mathbb{Z}$, $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m \mid n$, so the maximal ideals of $\mathbb{Z}$ are precisely the $p\mathbb{Z}$ with p a prime number.

For many other unital rings, like $\mathbb{Z}$, it can be easily proved that they contain maximal ideals, but a 'general proof' requires the use of Zorn's Lemma (which is equivalent to the Axiom of Choice). Let us pause to recall some relevant facts about it.

* * * * *

The Axiom of Choice. *Let I be a nonempty set and let $\{A_i\}_{i \in I}$ be a family of nonempty sets, then $\prod_{i \in I} A_i$ is not empty.*

This assertion is quite intuitive, but it is not a consequence of the basic axioms of Set Theory. By the way, recall that $\prod_{i \in I} A_i$ is defined as the set of *choice functions* $f : I \to \cup_{i \in I} A_i$, where $f(i) \in A_i$ for any $i \in I$. The Axiom of Choice asserts that there is always a choice function, even if the family is infinite, which means that one may take an infinite choice of elements.

Definition. A *partial order* on a nonempty set is a binary relation $\leq$ that is reflexive, antisymmetric and transitive.

If A is a nonempty set endowed with a partial order $\leq$, B is a subset of A and $u \in A$, then:

- u is an *upper bound* (respectively *lower bound*) of B if for any $b \in B$, $b \leq u$ (respectively $u \leq b$). Besides, if $u \in B$, then u is the *maximum* (respectively *minimum*) of B.
- u is a *maximal element* (respectively *minimal element*) of B if $u \in B$ and for any $x \in B$, $u \leq x \iff u = x$ (respectively $x \leq u \iff u = x$).
- B is a *chain* if $B \neq \emptyset$ and the restriction of $\leq$ to B is a total order (that is, for any $a, b \in B$, either $a \leq b$ or $b \leq a$)
- $\leq$ is a *well order* if any nonempty subset of A has a minimum.

Zorn's Lemma. *Let A be a partially ordered nonempty set such that there is an upper bound for any of its chains. Then there are maximal elements of A.*

Well Ordering Principle. *Any nonempty set admits a well order.*

Even though Zorn's Lemma and the Well Ordering Principle do not seem as intuitive as the Axiom of Choice, it can be proved that the three assertions are equivalent:

$$\boxed{\text{Axiom of Choice} \iff \text{Zorn's Lemma} \iff \text{Well Ordering Principle}}$$

This is proved in the appendix to this chapter.

* * * * *

2.14 Proposition. *Let R be a unital ring and let I be an ideal of R, $I \neq R$. Then I is contained in some maximal ideal of R.*

Proof. Consider the set $\mathcal{S} = \{J \trianglelefteq R : J \neq R \text{ and } I \subseteq J\}$. Then $\mathcal{S} \neq \emptyset$ since $I \in \mathcal{S}$. The relation $\subseteq$ is a partial order in $\mathcal{S}$. Let $\mathcal{C}$ be a chain in $\mathcal{S}$ and let $J = \cup_{A \in \mathcal{C}} A$. Then:

- J is an ideal of R. To see this, note that for any $x, y \in J$ and $r \in R$, there are $A, B \in \mathcal{C}$ such that $x \in A$ and $y \in B$. Since $\mathcal{C}$ is a chain, either $A \subseteq B$ or $B \subseteq A$, so $C = A \cup B$ is equal either to A or to B and hence $C \in \mathcal{C}$ with $x, y \in C$. Since C is an ideal, $x + y, -x, xy, rx, xr \in C\,(\subseteq J)$, so $x + y, -x, xy, rx, xr \in J$. Therefore J is an ideal.
- $1 \notin J$, since $1 \notin A$ for any $A \in \mathcal{C}$. In particular, $J \neq R$.

- J is an upper bound of $\mathcal{C}$ (obvious).

It has been proved that there is an upper bound for any chain in $\mathcal{S}$. Then Zorn's Lemma implies that $\mathcal{S}$ has maximal elements. But the maximal elements of $\mathcal{S}$ are precisely the maximal ideals of R containing I. □

2.15 Proposition. *Let R be a unital commutative ring and let I be an ideal of R, $I \neq R$. Then I is a maximal ideal of R if and only if R/I is a field.*

Proof. Recall that

$$\{\text{ideals of } R/I\} = \{J/I : J \trianglelefteq R,\, I \subseteq J\},$$

so that both assertions in the Proposition are equivalent to

$$\{\text{ideals of } R/I\} = \{0, R/I\}. \qquad \square$$

2.16 Examples.

- $(2, X)$ is a maximal ideal of $\mathbb{Z}[X]$ (we write $(2, X) \trianglelefteq_{\max} \mathbb{Z}[X]$).

  Proof. Since $(X) \subseteq (2, X)$, $\mathbb{Z}[X]/(2, X) \cong (\mathbb{Z}[X]/(X)) \,/\, ((2, X)/(X))$. Consider the homomorphism $\varphi : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ obtained as the composition of $\mathbb{Z}[X] \to \mathbb{Z}$, $p(X) \mapsto p(0)$, and $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $n \mapsto n + 2\mathbb{Z}$. φ is an epimorphism with $\ker \varphi = \{p(X) \in \mathbb{Z}[X] : p(0) = 2\mathbb{Z}\} = (2, X)$, so by the First Isomorphism Theorem, φ induces an isomorphism $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, we get $(2, X) \trianglelefteq_{\max} \mathbb{Z}[X]$. □

- Let $R = \{f : [0, 1] \to \mathbb{R} : f \text{ is continuous}\}$ and let $\alpha \in [0, 1]$ be fixed. Consider $M_\alpha = \{f \in R : f(\alpha) = 0\}$. Then $M_\alpha = \ker \varphi_\alpha$, where φ_α is the epimorphism $R \to \mathbb{R}$, $f \mapsto f(\alpha)$. Therefore $R/M_\alpha \cong \mathbb{R}$, which is a field, and thus $M_\alpha \trianglelefteq_{\max} R$.

2.17 Definition. Let R be a unital commutative ring and let $P \trianglelefteq R$ with $P \neq R$. Then P is said to be *prime* if for any $a, b \in R$ with $ab \in P$, either $a \in P$ or $b \in P$.

The prime ideals of $\mathbb{Z}$ are precisely 0 and the ideals $p\mathbb{Z}$, with p a prime number.

2.18 Properties. *Let R be a unital commutative ring.*

- *Let $P \neq R$ be an ideal, then P is prime if and only if R/P is an integral domain.*

- *Any maximal ideal of R is prime. However the converse is not valid (0 is a prime ideal of $\mathbb{Z}$ but it is not maximal since $0 \subsetneqq 2\mathbb{Z} \subsetneqq \mathbb{Z}$).*

2.19 Definition. Let R be a ring and let $I, J \trianglelefteq R$. Then I and J are said to be *comaximal* in case $I + J = R$.

2.20 Example. $n\mathbb{Z}$ and $m\mathbb{Z}$ are comaximal in $\mathbb{Z}$ if and only if $1 \in n\mathbb{Z}+m\mathbb{Z}$, if and only if there are $x, y \in \mathbb{Z}$ with $1 = nx+my$, if and only if $\gcd(n, m) = 1$, if and only if n and m are relatively prime.

Given any ring R and ideals $I_1, \ldots, I_m \trianglelefteq R$, the product $I_1 \cdots I_m$ denotes the ideal

$$I_1 \cdots I_m = \left\{ \sum_{\text{finite}} a_1 \cdots a_m : a_i \in I_i \ \forall i = 1, \ldots, m \right\}.$$

If R is unital and commutative and if $I_i = (a_i)$ for any $i = 1, \ldots, m$, then $I_1 \cdots I_m = (a_1 \cdots a_m)$ is principal too.

Recall that given any rings $R_1, \ldots, R_m$, its direct product $R_1 \times \cdots \times R_m$ is a ring too.

2.21 Chinese Remainder Theorem. *Let R be a unital commutative ring and let $I_1, \ldots, I_m \subsetneqq R$ be ideals of R ($m \geq 2$). Then the map*

$$\begin{aligned} \varphi : R &\longrightarrow R/I_1 \times \cdots \times R/I_m \\ x &\mapsto (x + I_1, \ldots, x + I_m), \end{aligned}$$

is a ring homomorphism with kernel $\ker \varphi = I_1 \cap \ldots \cap I_m$.

Moreover, if for any $i \neq j$, I_i and I_j are comaximal, then φ is an epimorphism and $I_1 \cap \ldots \cap I_m = I_1 \cdots I_m$, so

$$\begin{aligned} \bar{\varphi} : R/I_1 \cdots I_m &\longrightarrow R/I_1 \times \cdots \times R/I_m \\ x + I_1 \cdots I_m &\mapsto (x + I_1, \ldots, x + I_m) \end{aligned}$$

is an isomorphism.

Proof. The first part of the Theorem is easy. Suppose then that I_i and I_j are comaximal for any $i \neq j$, then $R = I_1 + I_2 = I_1 + I_3 = \cdots = I_1 + I_m$, so there are elements $a_i \in I_1$ and $b_i \in I_i$ for any $i = 2, \ldots, m$ such that $1 = a_i + b_i$. Therefore

$$1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_m + b_m) = b_2 \cdots b_m + \text{terms contained in } I_1.$$

Hence $1 \in I_1 + I_2 \cdots I_m$. Interchanging the index 1 by i for any i, this argument shows that for any $i = 1, \ldots, m$ there are elements $x_i \in I_i$ and $y_i \in I_1 \overset{\hat{i}}{\cdots} I_m$ such that $1 = x_i + y_i$. But $y_i \in I_1 \overset{\hat{i}}{\cdots} I_m \subseteq I_j$ for any $j \neq i$, so that $y_i + I_j = 0$ for any $j \neq i$. Besides, $y_i + I_i = (1 - x_i) + I_i = 1 + I_i$ since $x_i \in I_i$. Thus,

$$\varphi(y_i) = (0 + I_1, \ldots, 1 + I_i, \ldots, 0 + I_m)$$

for any $i = 1, \ldots, m$. Also, for any $a_i \in R$,

$$\begin{aligned}\varphi(a_i y_i) &= (a_i + I_1, \ldots, a_i + I_m)(0 + I_1, \ldots, 1 + I_i, \ldots, 0 + I_m) \\ &= (0 + I_1, \ldots, a_i + I_i, \ldots, 0 + I_m),\end{aligned}$$

so that for any $a_1, \ldots, a_m \in R$

$$\begin{aligned}\varphi(a_1 y_1 + \cdots + a_m y_m) &= \varphi(a_1 y_1) + \cdots + \varphi(a_m y_m) \\ &= (a_1 + I_1, \ldots, a_m + I_m),\end{aligned}$$

and this shows that φ is onto.

Finally, $I_1 \cdots I_m \subseteq I_1 \cap \cdots \cap I_m$, but for any $a \in I_1 \cap \cdots \cap I_m$,

$$\begin{aligned}a &= a1 \cdots 1 = a(x_1 + y_1) \cdots (x_m + y_m) \\ &= a x_1 \cdots x_m + \sum \text{terms } (a y_i) u.\end{aligned}$$

Since $a x_1 \cdots x_m \in I_1 \cdots I_m$ and $a \in I_i$, $y_i \in I_1 \cdots \hat{i} \cdots I_m$, also $(a y_i) u \in I_1 \cdots I_m$. Thus $a \in I_1 \cdots I_m$ and $I_1 \cdots I_m = I_1 \cap \cdots \cap I_m$, as required. □

As a particular case, take $R = \mathbb{Z}$ and $I_i = n_i \mathbb{Z}$, with $n_1, \ldots, n_m$ relatively prime. Then the above Theorem shows that the map

$$\begin{aligned}\mathbb{Z}/n_1 \cdots n_m \mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z} \\ x + n_1 \cdots n_m \mathbb{Z} &\mapsto (x_1 + n_1\mathbb{Z}, \ldots, x_m + n_m\mathbb{Z}),\end{aligned}$$

is an isomorphism. This assertion is equivalent to the 'classical version' of the Chinese Remainder Theorem (see Chapter 0, Theorem 2.2).

§ 3. Field of fractions

The usual construction of the rational field $\mathbb{Q}$ from the integers will be generalized in this section.

Recall that

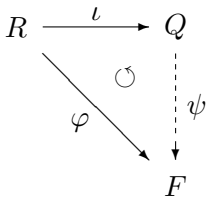
$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z},\, b \in \mathbb{Z} \setminus \{0\} \right\},$$

with the convention that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. Also, $\mathbb{Z}$ is embedded in $\mathbb{Q}$ by means of the map $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $a \mapsto \frac{a}{1}$, and this allows us to identify $\mathbb{Z}$ with a subring of the field $\mathbb{Q}$.

3.1 Theorem. *Let R be an integral domain. Then there exists a field Q and a ring monomorphism $\iota : R \hookrightarrow Q$ (which allows us to identify R with a subring of Q) satisfying:*

1. *Any element of Q is of the form $\iota(a)\iota(b)^{-1}$ with $a \in R$ and $b \in R \setminus \{0\}$.*

2. *(Uniqueness of Q) If $\varphi : R \to F$ is a ring monomorphism into a field F, then there is a unique monomorphism $\psi : Q \to F$ such that $\psi \circ \iota = \varphi$:*



That is, in a sense, Q is the smallest field containing R.

Proof. This is done by mimicking the arguments for $\mathbb{Z}$ and $\mathbb{Q}$. Let

$$\mathcal{F} = R \times (R \setminus \{0\}) = \{(a, b) \in R \times R : b \neq 0\},$$

and consider in $\mathcal{F}$ the relation

$$(a, b) \sim (c, d) \iff ad = bc.$$

Then $\sim$ is an equivalence relation. Let Q be the quotient set and denote by $\frac{a}{b}$ the equivalence class of the pair $(a, b) \in \mathcal{F}$. That is,

$$\frac{a}{b} = \{(c, d) \in \mathcal{F} : (a, b) \sim (c, d)\},$$

so that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

Now define the binary operation on Q by means of:

$$\begin{aligned} &\text{addition:} && \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \\ &\text{multiplication:} && \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}. \end{aligned}$$

It is an easy exercise to show that these are well defined and that Q is a field. The neutral element of the addition is $\frac{0}{1}$ $(= \frac{0}{b}$ for any $0 \neq b \in R)$ and of the multiplication is $\frac{1}{1}$ $(= \frac{b}{b}$ for any $0 \neq b \in R)$.

Moreover,

$$\begin{aligned} \iota : R &\longrightarrow Q \\ r &\mapsto \frac{r}{1}, \end{aligned}$$

is a ring monomorphism and any element of Q is of the form

$$\frac{a}{b} = \frac{a}{1}\frac{1}{b} = \iota(a)\iota(b)^{-1},$$

so the first condition is satisfied.

Now, assume that $\varphi : R \to F$ is a ring monomorphism into a field F. Define

$$\begin{aligned} \psi : Q &\longrightarrow F \\ \frac{a}{b} &\mapsto \varphi(a)\varphi(b)^{-1}. \end{aligned}$$

ψ is well defined, it is a ring monomorphism (check all this!) and $\psi \circ \iota = \varphi$. Besides, if $\tilde{\psi} : Q \to F$ is another ring monomorphism satisfying $\tilde{\psi} \circ \iota = \varphi$, then

$$\tilde{\psi}\left(\frac{a}{b}\right) = \tilde{\psi}\big(\iota(a)\big)\tilde{\psi}\big(\iota(b)^{-1}\big) = \tilde{\psi}\big(\iota(a)\big)\tilde{\psi}\big(\iota(b)\big)^{-1} = \varphi(a)\varphi(b)^{-1} = \psi\left(\frac{a}{b}\right),$$

so $\psi = \tilde{\psi}$, proving the uniqueness. □

3.2 Definition. Let R be an integral domain. The field Q constructed in the previous Theorem is said to be the *field of fractions* of R.

3.3 Examples.

- The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.
- If F is a field, the field of fractions of F is F itself (up to isomorphism), since ι is an isomorphism in this case.
- Let $R = F[X]$ be the ring of polynomials over a field F. Its field of fractions is the *field of rational functions*

$$F(X) = \left\{ \frac{p(X)}{q(X)} : p(X), q(X) \in F[X], q(X) \neq 0 \right\}.$$

§ 4. Divisibility

In this section we will consider classes of integral domains verifying some of the properties satisfied by the integers. Namely, the existence of a division algorithm, the fact that any nonzero ideal can be generated by just one element, and the unique factorization into prime numbers. Each one of these properties will lead to a different and interesting class of rings: *euclidean domains*, *principal ideal domains* and *unique factorization domains*.

4.1 Definition. Let R be an integral domain.

(i) A map $N : R \to \mathbb{N} \cup \{0\}$ with $N(0) = 0$ is called a *norm* of R.

(ii) R is said to be a *euclidean domain* if it has a norm N such that for any $a \in R$ and $b \in R \setminus \{0\}$, there are elements $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. (q is said to be the *quotient* and r the *remainder* of the *division* of a by b –although they may be not unique–.)

In this way, if R is a euclidean domain and $a, b \in R$ with $b \neq 0$, one may apply a *euclidean algorithm*, exactly as in $\mathbb{Z}$, which consists in iterating the division until a remainder 0 is found, so that:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \quad \text{(remainder= 0)} \end{aligned} \tag{4.2}$$

with $0 \leq N(r_n) < N(r_{n-1}) < \cdots < N(b)$.

4.3 Examples.

- Every field is a euclidean domain with $N(a) = 0$ for any a.
- $\mathbb{Z}$ is a euclidean domain with $N(a) = |a|$ for any $a \in \mathbb{Z}$.
- Let F be a field, then $F[X]$ is a euclidean domain with $N(0) = 0$ and $N\big(p(X)\big) = \deg p(X)$ for any $0 \neq p(X) \in F[X]$.
- The ring of *Gaussian integers* is the subring

  $$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

  of the complex field $\mathbb{C}$. It is a euclidean domain with

  $$N(a + bi) = (a + bi)\overline{(a + bi)} = a^2 + b^2.$$

  Proof. Let $\alpha = a + bi, \beta = c + di \in \mathbb{Z}[i]$ with $\beta \neq 0$. By dividing in $\mathbb{C}$ we get:

  $$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = q_0 + q_1 i,$$

  where $q_0, q_1 \in \mathbb{Q}$. Let $u, v \in \mathbb{Z}$ with $|u - q_0| \leq \frac{1}{2}$ and $|v - q_1| \leq \frac{1}{2}$ and let $\gamma = u + vi \in \mathbb{Z}[i]$ and $\rho = \alpha - \beta\gamma \in \mathbb{Z}[i]$. Then, in $\mathbb{C}$,

  $$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \gamma = (q_0 - u) + (q_1 - v)i,$$

so that

$$\frac{N(\rho)}{N(\beta)} = \left|\frac{\rho}{\beta}\right|^2 = (q_0 - u)^2 + (q_1 - v)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

Hence $N(\rho) < N(\beta)$, as required. □

4.4 Definition. Let R be a commutative ring and $a, b \in R$ with $b \neq 0$. Then:

(i) a is said to be a *multiple* of b (or b a *divisor* of a) if there exists $x \in R$ such that $a = bx$. (Notation: $b \mid a$.)

(ii) A *greatest common divisor* of a and b is an element $0 \neq d \in R$ such that

(a) $d \mid a$, $d \mid b$, and

(b) for any $0 \neq d' \in R$ such that $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

(Notation: $d = \gcd(a, b)$, although d may be not unique.)

Divisibility is related to ideals.

4.5 Properties. *Let R be a unital commutative ring, and $0 \neq a, b \in R$. Then*

1. *For any $d \in R$, $d \mid a$ and $d \mid b$ if and only if $(a, b) \subseteq (d)$.*

   Proof. It is enough to realize that $d \mid a$ if and only if $a \in (d)$ if and only if $(a) \subseteq (d)$. □

2. *If $(a, b) = (d)$, then $d = \gcd(a, b)$. (Check this!)*

3. *Assume that R is an integral domain and $d, d' \in R$. Then $(d) = (d')$ if and only if there exists $u \in R^\times$ such that $d' = du$. In particular, if d and d' are greatest common divisors of two elements $a, b \in R$, then there is a unit $u \in R^\times$ such that $d' = du$.*

   Proof. Assume first that $(d) = (d')$. Then $d \in (d')$ so there is a $x \in R$ with $d = d'x$. Also $d' \in (d)$ so there is a $y \in R$ with $d' = dy$. Then $d' = dy = d'xy$, so $d'(1 - xy) = 0$. Since R is an integral domain, either $d' = 0$, and hence $d = d' = 0$ and we may take $u = 1$, or $xy = 1$ so $u = y \in R^\times$.

   Now, if $d' = du$ for some unit u, then $d' = du \in (d)$, so $(d') \subseteq (d)$, but also $d = d'u^{-1} \in (d')$, so $(d) \subseteq (d')$. Hence $(d) = (d')$. □

4.6 Theorem. *Let R be a euclidean domain with norm N.*

(i) *Let* $0 \neq I \trianglelefteq R$ *and let* $0 \neq a \in I$ *such that* $N(a) = \min\{N(x) : 0 \neq x \in I\}$. *Then* $I = (a)$. *In particular,* any ideal of R is principal.

(ii) *For any* $0 \neq a, b \in R$, *let* r_n *be the last nonzero remainder in the 'euclidean algorithm'* (4.2). *Then* $r_n = \gcd(a, b)$, *there are elements* $x, y \in R$ *with* $r_n = xa + yb$, *and* $(a, b) = (r_n)$.

Proof. Exactly as for $\mathbb{Z}$! □

4.7 Definition. An integral domain is said to be a *principal ideal domain* (PID for short) if any of its ideals is principal.

4.8 Properties.

- *Any euclidean domain is a principal ideal domain.*
- *If* R *is a PID and* $0 \neq a, b \in R$, *then there exists a* $0 \neq d \in R$ *such that* $(a, b) = (d)$. *Therefore* $d = \gcd(a, b)$ *and any other greatest common divisor of* a *and* b *is of the form* du *for some unit* $u \in R^\times$.
- *If* R *is a PID and* $0 \neq I \trianglelefteq R$, *then* I *is prime if and only if it is maximal.*

  Proof. We already know that any maximal ideal is prime (see 2.18). Conversely, let I be a prime ideal of R and let $I \subsetneq J \trianglelefteq R$. Since R is a PID, there are elements $p, q \in R$ such that $I = (p)$ and $J = (q)$. Now, $p \in I \subseteq J = (q)$, so there is an $x \in R$ with $p = xq$. Since I is prime and $xq \in I$, either $x \in I$ or $q \in I$. In the latter case $(q) = J \subseteq I$, so $I = J$, a contradiction, while in the former case $x \in I$, so there is a $y \in R$ with $x = yp$. But then $p = xq = ypq$ and $(1 - yq)p = 0$. Since R is an integral domain and $p \neq 0$, $yq = 1$, so q is a unit, $1 = yq \in (q) = J$ and $J = R$. Thus, I is maximal. □

4.9 Example. In $\mathbb{Z}[X]$, the ideal $(2, X)$ is not principal (see 2.11), so that $\mathbb{Z}[X]$ is not a PID

In fact, the following result holds:

4.10 Proposition. *Let* R *be a unital commutative ring. Then* $R[X]$ *is a PID if and only if* R *is a field.*

Proof. If R is a field, $R[X]$ is a euclidean domain (by 4.3), so it is a PID (see 4.8). Conversely, if $R[X]$ is a PID, in particular $R[X]$ is an integral domain, and so is R. Then since $R[X]/(X) \cong R$, it follows that $(X) \trianglelefteq_{\text{prime}} R[X]$ by 2.18. But then $(X) \trianglelefteq_{\max} R[X]$ by 4.8, so $R \cong R[X]/(X)$ is a field because of 2.15. □

Let us deal now with the concepts that generalize prime numbers in $\mathbb{N}$.

4.11 Definition. Let R be an integral domain.

(i) Let $0 \neq r \in R$ be a nonunit, then r is said to be *irreducible* in R if for any $a, b \in R$ such that $r = ab$, either a or b is a unit. Otherwise, r is said to be *reducible*

(ii) Let $0 \neq p \in R$ be a nonunit, then p is said to be *prime* in R if $(p) \trianglelefteq_{\text{prime}} R$. That is, p is prime in R if for any $a, b \in R$ with $p \mid ab$, either $p \mid a$ or $p \mid b$.

(iii) Two elements $a, b \in R$ are said to be *associate elements* (or *associates*) if there is a unit $u \in R^\times$ such that $a = bu$ or, what is the same, if $(a) = (b)$.

4.12 Proposition. *Let R be an integral domain.*

1. *Any prime element is irreducible.*

2. *If R is a PID, the converse is true (so prime $\Leftrightarrow$ irreducible).*

Proof. Let p be a prime element and assume that $p = ab$ for $a, b \in R$. Since p is prime either $p \mid a$ or $p \mid b$. In the first case $p \mid a$ and $a \mid p = ab$, so p and a are associates and, hence, b is a unit. In the second case a is a unit with the same argument. Hence p is irreducible.

Now assume that R is a PID and let p be an irreducible element. Let $I \trianglelefteq R$ such that $(p) \subseteq I$. Since R is a PID, $I = (m)$ for some $m \in R$. Hence, $p \in (m)$, so there is an $x \in R$ with $p = xm$ and, since p is irreducible, either x is a unit, in which case p and m are associates and $(p) = (m) = I$, or m is a unit and $I = R$. Thus, $(p) \trianglelefteq_{\max} R$, so $(p) \trianglelefteq_{\text{prime}} R$ (by 2.18) and p is prime. □

4.13 Corollary (of the proof). *Let R be a PID but not a field, then*

$$\{\textit{maximal ideals of } R\} = \{\,(p) : p \textit{ is prime}\}\,.$$

4.14 Remark. In general, an irreducible element need not be prime. For instance, let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}\,(\leq \mathbb{C})$ and let $N : R \to \mathbb{N} \cup \{0\}$ be the norm given by $N(\alpha) = \alpha\bar{\alpha}$ (the square of the usual norm in $\mathbb{C}$), so that N is multiplicative ($N(\mu\nu) = N(\mu)N(\nu)$ for any $\mu, \nu \in R$). Let $\alpha = 2 + \sqrt{-5} \in R$, let us check that α is irreducible but not prime.

To begin with, $N(\alpha) = 9$, so if $\beta, \gamma \in R$ are such that $\alpha = \beta\gamma$, then $9 = N(\alpha) = N(\beta)N(\gamma)$, so that either $N(\beta) = 1$ or $N(\gamma) = 1$, or $N(\beta) = N(\gamma) = 3$. But $N(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 3$ for any $a, b \in \mathbb{Z}$, and $N(a + b\sqrt{-5}) = 1$

if and only if $a = \pm 1$ and $b = 0$. Hence either $\beta = \pm 1$ or $\gamma = \pm 1$, so either β or γ is a unit, and α is irreducible.

However, $3^2 = 9 = \alpha\bar{\alpha} \in (\alpha)$ and $3 \notin (\alpha)$ (otherwise $3 = \alpha\delta$ for some δ, and hence $N(\delta) = 1$, so $\delta = \pm 1$, a contradiction). Therefore $(\alpha) \not\trianglelefteq_{\text{prime}} R$ and α is not prime.

As a consequence, $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

4.15 Definition. An integral domain R is said to be a *unique factorization domain* (UFD for short) if for any nonunit $0 \neq r \in R$ the following conditions are satisfied:

(i) There are $n \in \mathbb{N}$ and irreducible elements $p_1, \ldots, p_n \in R$ (not necessarily different) such that $r = p_1 \cdots p_n$.

(ii) The factorization in (i) is unique up to associates. That is, if $r = q_1 \cdots q_m$ with $m \in \mathbb{N}$ and irreducible elements $q_1, \ldots, q_m \in R$, then $m = n$ and there is a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that p_i and $q_{\sigma(i)}$ are associates for all $i = 1, \ldots, n$.

4.16 Proposition. *Let R be a UFD.*

1. *The irreducible elements in R coincide with the prime elements. (This implies, in particular, that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.)*

2. *Let $0 \neq a, b \in R$ and let $p_1, \ldots, p_n$ be primes in R so that p_i and p_j are not associates for any $i \neq j$, and such that $a = up_1^{e_1} \cdots p_n^{e_n}$ and $b = vp_1^{f_1} \cdots p_n^{f_n}$ (factorization into irreducibles), where $u, v \in R^\times$, and $e_1, f_1, \ldots, e_n, f_n \in \mathbb{N} \cup \{0\}$. Then $d = p_1^{\min\{e_1, f_1\}} \cdots p_n^{\min\{e_n, f_n\}}$ is a greatest common divisor of a and b, and any other greatest common divisor of a and b is an associate of d.*

Proof. For the first part assume that p is irreducible and $a, b \in R$ with $p \mid ab$. Then there is a $c \in R$ such that $pc = ab$. Taking factorizations of a, b, c into irreducibles and using the uniqueness of factorization, it follows that p is associate of an irreducible factor of either a and b. In particular, either $p \mid a$ or $p \mid b$.

For the second part, it is clear that d is a common divisor of a and b. By the uniqueness of factorization, any other common divisor of a and b is of the form $c = wp_1^{g_1} \cdots p_n^{g_n}$, where w is a unit and $g_i \leq \min\{e_i, f_i\}$ for any $i = 1, \ldots, n$, and the result follows easily. □

4.17 Theorem. *Any principal ideal domain is a unique factorization domain.*

Proof. Let R be a PID. Given any $0 \neq r \in R \setminus R^\times$, we want to factor r into a product of irreducible elements. Assume that this cannot be done. In particular, r is not irreducible, so that $r = r_1 r_1'$ for some $r_1, r_1' \in R \setminus R^\times$, and this implies that $(r) \subsetneqq (r_1)$ and $(r) \subsetneqq (r_1')$.

Now, if both r_1 and r_1' could be factored into a product of irreducibles, so could be r. Hence we may assume that r_1 cannot be factored into a product of irreducible elements. In particular r_1 is not irreducible, so that $r_1 = r_2 r_2'$ for some $r_2, r_2' \in R \setminus R^\times$, and this implies that $(r_1) \subsetneqq (r_2)$ and $(r_1) \subsetneqq (r_2')$. Again, we may assume that r_2 cannot be factored into a product of irreducible elements.

Continuing in this way, we find nonzero elements $r_i \in R \setminus R^\times$ such that

$$(r) \subsetneqq (r_1) \subsetneqq (r_2) \subsetneqq \cdots \subsetneqq R.$$

Let $I = \cup_{n=0}^{\infty}(r_n)$ (where $r_0 = r$). Then I is clearly an ideal of R and, since R is a PID, there is an element $a \in R$ such that $I = (a)$. Hence $a \in I = \cup_{n=0}^{\infty}(r_n)$, so there is an $n \in \mathbb{N}$ such that $a \in (r_n)$. But this shows that $(a) \subseteq (r_n) \subsetneqq (r_{n+1}) \subseteq I = (a)$, a contradiction.

Therefore any $0 \neq r \in R \setminus R^\times$ can be factored into a product of irreducibles. It remains to be shown that these factorizations are unique, up to associates. So let $0 \neq r \in R \setminus R^\times$ and let $r = p_1 \cdots p_n$ be a factorization of r with irreducible p_i's. Let $r = q_1 \cdots q_m$ be any other factorization of r as a product of irreducible elements. We shall show the uniqueness by induction on n:

- If $n = 1$, since R is a PID, r is prime, and there exists an $i = 1, \ldots, m$ such that $r \mid q_i \mid r$, that is, r and q_i are associates. We may assume that $i = 1$, so that $q_1 = ru$ for some $u \in R^\times$. Thus $r = (ru)q_2 \cdots q_m = r(uq_2 \cdots q_m)$ and, as R is an integral domain, $uq_2 \cdots q_m = 1$. Since the q_i's are not units, the only possibility is $m = 1$ and $r = p_1 = q_1$.

- Assume now that $n > 1$ and that the result is true for $n - 1$. Since $p_1 \mid r = q_1 \cdots q_m$ and p_1 is prime, there is an $i = 1, \ldots, m$ such that $p_1 \mid q_i$. We may assume that $i = 1$ and that $q_1 = p_1 u$ for some $u \in R$. But q_1 is irreducible, so u is a unit. Hence $r = p_1 \cdots p_n = q_1 \cdots q_m = p_1(uq_2)q_3 \cdots q_m$ and $p_2 \cdots p_n = (uq_2)q_3 \cdots q_m$. Since $u \in R^\times$ and q_2 is irreducible, uq_2 is irreducible too. Therefore we have two factorizations of $r' = p_2 \cdots p_n$. The induction hypothesis shows that $n - 1 = m - 1$, so $n = m$, and that after renumbering, p_i and q_i are associates for each $i = 2, \ldots, m$ (being associate of uq_2 is the same as being associate of q_2, because $u \in R^\times$).

□

4.18 Remark. The following chain of implications has already been proven:

Field ⇒ Euclidean domain ⇒ PID ⇒ UFD ⇒ Integral domain.

None of the reverse implications hold:

- $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, but not a UFD (see 4.14 and 4.16).
- In Chapter 3 (1.6) it will be proven that $\mathbb{Z}[X]$ is a UFD, but it is not a PID (see 2.11).
- In the exercises you will be asked to prove that $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID, but not a euclidean domain.
- Finally, $\mathbb{Z}$ is a euclidean domain, but not a field.

§ 5. Matrices over a principal ideal domain

Let R be a PID with field of fractions F. The following matrices in $\mathrm{Mat}_n(R)$ (which is a subring of $\mathrm{Mat}_n(F)$) are called *elementary matrices* of order n over R:

$$P_{ij} = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & i & & j & \end{array} \\ \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \cdots & 1 & & \\ & & \vdots & & \vdots & & \\ & & 1 & \cdots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array} = I_n - (E_{ii} + E_{jj}) + (E_{ij} + E_{ji}),$$

$$P_{ij}(r) = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & i & & j & \end{array} \\ \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \cdots & r & & \\ & & & \ddots & \vdots & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array} = I_n + rE_{ij}, \quad r \in R,$$

$$P_i(r) = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} & & & i & & & \end{array} \\ \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & r & & & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \end{array} = I_n + (r-1)E_{ii}, \quad r \in R^\times,$$

$$P_{ij}(a,b,c,d) = \begin{pmatrix} & & & i & & j & & \\ 1 & & & & & & & \\ & \ddots & & & & & & \\ & & & a & \cdots & b & & \\ & & & \vdots & & \vdots & & \\ & & & c & \cdots & d & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix} = \begin{array}{l} I_n - (E_{ii} + E_{jj}) \\ \quad + aE_{ii} + bE_{ij} + cE_{ji} + dE_{jj}, \\ a,b,c,d \in R \text{ with } ad - bc = 1. \end{array}$$

(Here I_n denotes the identity matrix and E_{ij} the matrix with 1 in the (i,j) position and 0's elsewhere. Note that $P_{ij}(r) = P_{ij}(1,r,0,1)$.)

The elementary matrices are invertible in $\mathrm{Mat}_n(R)$ with

$$P_{ij}^{-1} = P_{ij}, \qquad P_{ij}(r)^{-1} = P_{ij}(-r), \qquad P_i(r)^{-1} = P_i(r^{-1}),$$
$$P_{ij}(a,b,c,d)^{-1} = P_{ij}(d,-b,-c,a).$$

The set of invertible matrices in $\mathrm{Mat}_n(R)$ is denoted by $\mathrm{GL}_n(R)$.

Note that for a matrix $A \in \mathrm{Mat}_{n\times m}(R)$,

- $P_{ij}A$ is the matrix obtained by switching the rows i and j of A,
- $P_{ij}(r)A$ is the matrix obtained by adding the jth row of A multiplied by r to its ith row,
- $P_i(r)A$ is the matrix obtained by multiplying the ith row of A by r,

and for a matrix $B \in \mathrm{Mat}_{m\times n}(R)$,

- BP_{ij} is the matrix obtained by switching the columns i and j of B,
- $BP_{ij}(r)$ is the matrix obtained by adding the ith column of B multiplied by r to its jth column,
- $BP_i(r)$ is the matrix obtained by multiplying the ith column of B by r.

5.1 Theorem. *Let A be an $n \times m$ matrix over a PID R, then there exist $r \in \mathbb{N} \cup \{0\}$ and matrices $P \in \mathrm{GL}_n(R)$ and $Q \in \mathrm{GL}_m(R)$ such that*

$$PAQ = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix} = \sum_{i=1}^{r} d_i E_{ii},$$

for some elements $d_1, \ldots, d_r \in R \setminus \{0\}$ and $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$.

Moreover, r and the ideals $(d_1), \ldots, (d_r)$ are uniquely determined by A.

Proof. For the uniqueness, denote by $I_s(A)$ the ideal generated by the minors of order $s \leq \min(n,m)$ of A, that is, the determinants of the $s \times s$ square submatrices $A^{j_1,\dots,j_s}_{i_1,\dots,i_s}$ obtained as the intersection of the rows $i_1,\dots,i_s$ and columns $j_1,\dots,j_s$ ($1 \leq i_1 < \cdots < i_s \leq n$, $1 \leq j_1 < \cdots < j_s \leq m$) of A. Note that $I_s(A) \supseteq I_{s+1}(A)$ for any $s < \min(n,m)$. If B is any $n \times n$ matrix over R, then $I_s(BA)$ is contained in $I_s(A)$, as any $s \times s$ submatrix $(BA)^{j_1,\dots,j_s}_{i_1,\dots,i_s}$ of BA is the product of the matrix $B_{i_1,\dots,i_s}$, consisting of the rows $i_1,\dots,i_s$ of B, and the matrix $A^{j_1,\dots,j_s}$ consisting of the columns $j_1,\dots,j_s$ of A. Therefore the rows of $(BA)^{j_1,\dots,j_s}_{i_1,\dots,i_s}$ are then linear combinations, with coefficients in R, of the rows in $A^{j_1,\dots,j_s}$, and hence the determinant of $(BA)^{j_1,\dots,j_s}_{i_1,\dots,i_s}$ is a linear combination of $s \times s$ of minors of A. Hence, if $P \in \mathrm{GL}_n(R)$, then $I_s(PA) \subseteq I_s(A)$, but also $I_s(A) = I_s(P^{-1}PA) \subseteq I_s(PA)$. The same argument works for $I_s(AQ)$. We conclude that with $D = \sum_{i=1}^{r} d_i E_{ii} \in \mathrm{Mat}_{n\times m}(R)$, $I_s(A) = I_s(PAQ) = I_s(D) = (d_1 \cdot \ldots \cdot d_s) \neq 0$, for $s \leq r$, and $I_s(A) = I_s(D) = 0$ for $s > r$. The uniqueness follows.

For the existence, this is clear if $A = 0$. For any $0 \neq a \in R \setminus R^\times$, $a = q_1 \cdots q_n$ for some irreducible elements, and we define the *length* of a as $l(a) = n$. Define $l(a) = 0$ if $a \in R^\times$ and $l(0) = \infty$. If $A \neq 0$, by multiplying it by matrices P_{1i} and P_{j1} we may assume that $a_{11} \neq 0$. Note that if we take two elements $x, y \in R$ with x not dividing y, and $d = \gcd(x,y)$, then $(x,y) = (d)$ and there are elements $u, v \in R$ with $d = ux + vy$. Moreover, $x = dx'$, $y = dy'$, so $ux' + vy' = 1$ and

$$\begin{pmatrix} u & v \\ -y' & x' \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Besides, d is a proper divisor of x, so that $l(d) < l(x)$. Thus, if the element in the $(1,1)$-slot does not divide an element in the first column (respectively row), multiplying A on the left (resp. right) by elementary matrices of type $P_{1i}(a,b,c,d)$ we may get in the $(1,1)$-slot elements with lower length. Eventually, we may get in the $(1,1)$-slot an element which divides any other element in the first row and column. Now, multiplying by elementary matrices $P_{i1}(r)$ on the left and $P_{1j}(r)$ on the right, we may get 0's in the entries of the first row and column other than the $(1,1)$ entry. Thus, multiplying A by elementary matrices, we may transform it into a matrix of the form

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \hat{A} & \\ 0 & & & \end{pmatrix}.$$

If there is an element $\hat{a}_{ij}$ not divisible by a, by multiplying on the left by $P_{1i}(1)$, we add the ith row to the first one, and we may apply the previous arguments to change the element a by a divisor of it. Eventually we get a

matrix as above with a dividing any entry of $\hat{A}$. Now a recursive argument works. □

The elements $d_1, \ldots, d_r$ are determined uniquely by A only up to associates. By abuse of notation, they are called the *invariant factors* of the matrix A.

5.2 Remark. The matrices P and Q in the previous theorem are obtained as products of elementary matrices.

If R is a euclidean domain, only the elementary matrices P_{ij}, $P_{ij}(r)$ and $P_i(r)$ are needed.

5.3 Example. We may 'diagonalize' any matrix over a PID and compute at the same time the invertible matrices P and Q, because the matrix P (respectively Q) is obtained by multiplying the identity matrix on the left (respectively right) by the same elementary matrices used to multiply A on the left (respectively right).

Consider, for instance, the matrix $\begin{pmatrix} 2 & 4 & 2 \\ 6 & 4 & 5 \end{pmatrix} \in \mathrm{Mat}_{2\times 3}(\mathbb{Z})$. We may proceed as follows:

$$\left[\begin{array}{ccc|cc} 2 & 4 & 2 & 1 & 0 \\ 6 & 4 & 5 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right] \to \left[\begin{array}{ccc|cc} 0 & 4 & 2 & 1 & 0 \\ 1 & 4 & 5 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ -1 & 0 & 1 & & \end{array}\right] \to \left[\begin{array}{ccc|cc} 1 & 4 & 5 & 0 & 1 \\ 0 & 4 & 2 & 1 & 0 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ -1 & 0 & 1 & & \end{array}\right]$$

$$\to \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 4 & 2 & 1 & 0 \\ \hline 1 & -4 & -5 & & \\ 0 & 1 & 0 & & \\ -1 & 4 & 6 & & \end{array}\right] \to \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 4 & 1 & 0 \\ \hline 1 & -5 & -4 & & \\ 0 & 0 & 1 & & \\ -1 & 6 & 4 & & \end{array}\right] \to \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ \hline 1 & -5 & 6 & & \\ 0 & 0 & 1 & & \\ -1 & 6 & -8 & & \end{array}\right]$$

so we get:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 4 & 2 \\ 6 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & -5 & 6 \\ 0 & 0 & 1 \\ -1 & 6 & -8 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

5.4 Corollary. *Any invertible square matrix over a PID R is a product of elementary matrices.*

Proof. If $A, B \in \mathrm{Mat}_n(R)$ satisfy $AB = I_n$, then $\det(A)\det(B) = 1$, so $\det(A) \in R^\times$. Hence $I_n(A) = R = (1)$. It follows that $I_s(A) = R$ for any s, and hence there are matrices $P, Q \in \mathrm{GL}_n(R)$, which are products of elementary matrices, such that $PAQ = I_n$. Hence $A = P^{-1}Q^{-1}$ is a product too of elementary matrices. □

Exercises

1. Show which of the following sets are subrings of the ring of functions from the interval $[0,1]$ to $\mathbb{R}$:

   (a) The set of those functions f such that $f(q) = 0$ for any $q \in \mathbb{Q} \cap [0,1]$.

   (b) The set of polynomial functions.

   (c) The set consisting of the trivial function ($f(x) = 0 \, \forall x$), together with those functions with only a finite number of zeroes.

   (d) The set of functions with an infinite number of zeroes.

   (e) The linear combinations with rational coefficients of $\cos(nx)$ and $\sin(mx)$ with $n, m \in \{0, 1, 2, \dots\}$.

2. Take $\overline{0} \neq \overline{n} \in \mathbb{Z}/m\mathbb{Z}$. Prove that $\overline{n}$ is a zero divisor if and only if $\gcd(n, m) \neq 1$.

3. Given a ring R, its *center* is the set

   $$Z(R) = \{z \in R \mid zx = xz \ \ \forall x \in R\}.$$

   Prove that $Z(R)$ is a subring of R and that, if R is a division ring, then $Z(R)$ is a field.

4. Given an element a of a ring R, consider its *centralizer* $C(a) = \{x \in R \mid xa = ax\}$. Prove that $C(a)$ is a subring and that $Z(R) = \bigcap_{a \in R} C(a)$.

5. Compute the center of the ring of Hamilton quaternions.

6. Given two rings R and S, its cartesian product $R \times S$ is a ring with the binary operations of addition and multiplication defined by $(r, s) + (r', s') = (r + r', s + s')$ and $(r, s) \cdot (r', s') = (rr', ss')$. Show that $R \times S$ is commutative (respectively unital) if and only if so are R and S.

7. A ring R is said to be *boolean* if $a^2 = a$ for any $a \in R$. Prove that any boolean ring is commutative.

8. Let X be a nonempty set and let $\mathcal{P}(X)$ be the set of all subsets of X. Define an addition and a multiplication on $\mathcal{P}(X)$ by means of

   $$A + B = (A \setminus B) \cup (B \setminus A) \quad \text{and} \quad A \cdot B = A \cap B$$

   where $A \setminus B = A \cap B^c$ and B^c denotes the complement of B. Prove that $\mathcal{P}(X)$, with these operations, is a unital boolean ring.

9. Let $d \in \mathbb{Z}$ an integer that is not a perfect square. Consider the subset of $\mathbb{C}$ given by
$$\mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$
   (a) Prove that $\mathbb{Z}[\sqrt{d}\,]$ is a subring of $\mathbb{C}$.
   (b) Consider the map, that will be called the *norm*, $N : \mathbb{Z}[\sqrt{d}\,] \to \mathbb{Z}$ defined by $N(a+b\sqrt{d}) = a^2 - db^2$. Prove that $N(xy) = N(x)N(y)$ for any $x, y \in \mathbb{Z}[\sqrt{d}\,]$.
   (c) Prove that the inverse in $\mathbb{C}$ of $a + b\sqrt{d} \neq 0$ is $\dfrac{a - b\sqrt{d}}{a^2 - db^2}$.
   (d) Prove that u is a unit in $\mathbb{Z}[\sqrt{d}\,]$ if and only if $N(u) = \pm 1$. As a consequence, if $d < -1$, then $\mathbb{Z}[\sqrt{d}\,]^\times = \{\pm 1\}$.

10. Prove that the following tables define a field:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

    How many fields of 4 elements do exist, up to isomorphism?

11. Consider the set
$$\mathcal{Q}_1 = \left\{ \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$
    with the usual addition and multiplication in $\mathrm{Mat}_2(\mathbb{C})$, as well as the set
$$\mathcal{Q}_2 = \left\{ \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma & \delta & \alpha & -\beta \\ -\delta & -\gamma & \beta & \alpha \end{pmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{R} \right\}$$
    with the usual addition and multiplication in $\mathrm{Mat}_4(\mathbb{R})$.
    Prove that both $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are rings isomorphic to $\mathbb{H}$.

12. Let A and B be two unital rings, with respective unities 1_A and 1_B, and let $f : A \longrightarrow B$ a homomorphism such that $f(a)$ is a unit of B for some $a \in A$. Prove that $f(1_A) = 1_B$ and that $f(u^{-1}) = [f(u)]^{-1}$ for any $u \in A^\times$.

13. Check which of the following maps are ring homomorphisms. Which of them are isomorphisms?

    (a) $\mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}) : x + y\sqrt{2} \mapsto x - y\sqrt{2}$,

    (b) $2\mathbb{Z} \longrightarrow 3\mathbb{Z} : 2n \mapsto 3n$,

    (c) $\mathbb{C} \longrightarrow \mathbb{C} : x + yi \mapsto x - yi$,

    (d) $\mathbb{Z}_{60} \longrightarrow \mathbb{Z}_6 \times \mathbb{Z}_{10} : m + 60\mathbb{Z} \mapsto (m + 6\mathbb{Z}, m + 10\mathbb{Z})$ $(0 \leq m < 60)$.

14. Let $d \in \mathbb{Z}$ an integer that is not a perfect square and let

$$S = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

    Prove that:

    (a) S is a subring of $\mathrm{Mat}_2(\mathbb{Z})$.

    (b) The map $\varphi\colon \mathbb{Z}[\sqrt{d}\,] \to S$ defined by $\varphi(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$ is a ring isomorphism.

15. Let X be a nonempty set and let $\mathcal{P}(X)$ be the boolean ring of the subsets of X. Let R be the ring of the maps from X to $\mathbb{Z}_2$. For any $A \in \mathcal{P}(X)$ consider the map

$$\chi_A\colon X \to \mathbb{Z}_2 \quad \text{given by} \quad \chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

    (χ_A is called the *characteristic function* of A with values in $\mathbb{Z}_2$.) Prove that the map $\mathcal{P}(X) \to R$ defined by $A \mapsto \chi_A$ is a ring isomorphism.

16. Determine which of the following sets are ideals of $\mathbb{Z}[X]$:

    (a) The set of polynomials whose constant term is a multiple of 3.

    (b) The set of polynomials whose coefficient of X^2 is multiple of 3.

    (c) The set of polynomials whose constant term and the coefficients of X and X^2 are 0.

    (d) The set of polynomials whose coefficients add up to 0.

    (e) The set of polynomials $p(X)$ such that $p'(0) = 0$. (Here $p'(X)$ denotes the usual derivative of $p(X)$.)

---

[13] $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ $(\subseteq \mathbb{R})$ is a field, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

[15] R is a ring with the operations $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$.

17. Let a be an element of a ring R.

    (a) Prove that the set $\{x \in R \mid xa = 0\}$ is a left ideal of R, called the *left annihilator* of a. In the same vein, prove that the set $\{x \in R \mid ax = 0\}$ (*right annihilator*) is a right ideal.

    (b) Prove that if $L \trianglelefteq_{\text{left}} R$, then the set $\{x \in R \mid xa = 0 \ \forall a \in L\}$ is an ideal of R (the *annihilator* of L in R).

18. Let A be a unital commutative ring. An element $a \in A$ is said to be *nilpotent* if $a^n = 0$ for some $n \in \mathbb{N}$. Prove the following assertions:

    (a) A does not contain nonzero nilpotent elements if and only if 0 is the unique element in A whose square is 0.

    (b) The set $\mathcal{N}(A)$ of all the nilpotent elements of A is an ideal of A, called the *nilradical* of A, and $\mathcal{N}\big(A/\mathcal{N}(A)\big) = 0$.

    (c) $\mathcal{N}(A)$ coincides with the intersection of all the prime ideals of A.

19. Let A be a unital commutative ring. Prove that the sum of a unit and a nilpotent element is a unit.

20. Let A be a unital commutative ring. Its *Jacobson radical* $\mathcal{J}(A)$ is defined as the intersection of all the maximal ideals of A. Prove that for any element $a \in A$, $a \in \mathcal{J}(A)$ if and only if $1 - ab$ is a unit for any $b \in A$. Prove also that $\mathcal{J}\big(A/\mathcal{J}(A)\big) = 0$ and that $\mathcal{N}(A) \subseteq \mathcal{J}(A)$.

21. Let A be a unital commutative ring and let P be a proper ideal of A. Prove that P is prime if and only for any ideals I and J of A such that $IJ \subseteq P$, either $I \subseteq P$ or $J \subseteq P$.

22. Let A be a unital commutative ring and let $\mathcal{Z} = \mathcal{Z}(A)$ be the set formed by the zero divisors of A and 0. Prove that $\mathcal{Z}$ is a union of prime ideals.

23. Prove that any finitely generated ideal of a boolean ring is principal.

---

[18] It is easy to see that $\mathcal{N}(A)$ is contained in any prime ideal of A. For the converse, if a is not nilpotent, consider the set of ideals I of A such that $a^n \notin I$ for any $n \in \mathbb{N}$. Use Zorn's Lemma to show that there is a maximal element in this set, and check that this is a prime ideal of A.

[19] If $a^m = 0$ for an odd m, then $1 = 1 + a^m = (1 + a)(1 - a + a^2 - \cdots + a^{m-1})$.

[20] If $M \trianglelefteq_{\max} A$ and $a \notin M$, then $M + (a) = A$.

[22] Given $x \in \mathcal{Z}$, use Zorn's Lemma with the set of those ideals of A that contain x and are contained in $\mathcal{Z}$. Prove that its maximal elements are prime ideals of A and that $\mathcal{Z}$ is the union of all of them.

[23] Check that $(x, y) = (x + y + xy)$.

24. Let R be a unital ring. An element $e \in R$ is said to be *idempotent* if $e^2 = e$. Assume that e is an idempotent in R, that is contained in $Z(R)$ (that is, $er = re$ for any $r \in R$). Prove that (e) and $(1-e)$ are ideals of R such that R is isomorphic to $(e) \times (1-e)$. Moreover, e (respectively $1-e$) is the unity of the ring (e) (respectively $(1-e)$).

25. Let R be a finite unital boolean ring. Prove that R is isomorphic to $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$.

26. Solve the following systems of congruences:

    (a) In $\mathbb{Z}$, $\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 3 \pmod 7 \\ x \equiv 9 \pmod{11} \end{cases}$

    (b) In $\mathbb{Z}_3[X]$, $\begin{cases} f(X) \equiv 1 \pmod{X-1} \\ f(X) \equiv X \pmod{X^2+1} \\ f(X) \equiv X^3 \pmod{X+1} \end{cases}$

27. (a) Are the rings $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ isomorphic?

    (b) Are the fields of fractions of $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ isomorphic?

28. Let A be an integral domain, $Q(A)$ its field of fractions, B a ring such that $A \leq B \leq Q(A)$. Prove that $Q(A)$ is the field of fractions of B too. In particular, check that $\mathbb{Q}$ is the field of fractions of $\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$.

29. Let F be a field. Prove that:

    (a) The map $\Gamma\colon \mathbb{Z} \to F$ given by $\Gamma(0) = 0$, $\Gamma(n) = 1 + \cdots + 1$ (n summands) and $\Gamma(-n) = -\Gamma(n)$ ($n \in \mathbb{N}$) is a ring homomorphism.

    (b) $\ker \Gamma \trianglelefteq_{\text{prime}} \mathbb{Z}$.

    (c) If $\ker \Gamma = 0$, then F contains an isomorphic copy of $\mathbb{Q}$. In particular, any subfield of $\mathbb{R}$ contains $\mathbb{Q}$.

    (d) If $\ker \Gamma \neq 0$, then $\ker \Gamma \trianglelefteq_{\max} \mathbb{Z}$ and thus F contains an isomorphic copy of $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

30. Let R be a euclidean domain with norm N that satisfies $N(a) \leq N(ab)$ for any $0 \neq a, b \in R$. Prove that:

    (a) $N(a) = N(au)$ for any $a \in R$ and $u \in R^\times$.

[25] Use the previous exercise.
[27] For the first part, find the units in both rings.

(b) For any $0 \neq a, b \in R$, $(a) = (b)$ if and only if $b \in (a)$ and $N(a) = N(b)$.

31. Prove that $\mathbb{Z}[\sqrt{-2}]$, with the norm given by $N(a + b\sqrt{-2}) = a^2 + 2b^2$, is a euclidean domain.

32. In the following euclidean domains, find $d = \gcd(a, b)$ and compute elements r, s such that $d = ra + sb$, where:

    (a) $A = \mathbb{Z}_3[X], \quad a = 2X^2 + 2, \quad b = X^5 + 2.$

    (b) $A = \mathbb{Z}[i], \quad a = 7 - 3i, \quad b = 5 + 3i.$

33. Let A be a UFD, prove that:

    (a) Any nonzero prime ideal of A contains a prime element.

    (b) If $0 \neq a \in A$, then there are only a finite number of principal ideals of A that contain a.

34. Recall that $\mathbb{Z}[i]$ is a euclidean domain, so it is a UFD too.

    (a) Prove that the integral solutions to the equation $x^2 + y^2 = z^2$ are, up to permutation of x and y, $x = d(u^2 - v^2)$, $y = 2duv$ and $z = d(u^2 + v^2)$, where d, u, v are integers with u and v relatively prime.

    (b) Prove that the equation $x^4 + y^4 = z^2$ has no integral nontrivial solutions.

    (c) Prove that Fermat's equation $x^n + y^n = z^n$ has no nontrivial integral solutions if n is a multiple of 4.

Through the next exercises, you will be asked to prove that the ring $R = \{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\} (\subseteq \mathbb{C})$ is a PID, but not a euclidean domain.

35. Let $F = \{a + b\sqrt{-19} : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ and $R = \{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\} \subseteq F$.

    (a) Prove that F is the field of fractions of R.

[34] (a) It is enough to deal with solutions $x, y, z \geq 1$, where x, y, z are pairwise relatively prime, with odd x, z and even y. Then factor the equation as $(x + iy)(x - iy) = z^2$, check that $x + iy$ and $x - iy$ are relatively prime and deduce that they are perfect squares in $\mathbb{Z}[i]$.

(b) Take a nontrivial solution $x, y, z \geq 1$ with minimal z and use part (a) suitably to get a contradiction.

(b) Given any $x = a + b\sqrt{-19} \in F$, let $\bar{x}$ be its complex conjugate and define $N(x) = x\bar{x}$. Prove that N is multiplicative (that is, $N(xy) = N(x)N(y)$ for any $x, y \in F$). Check also that if $0 \neq x \in R$, then $0 < N(x) \in \mathbb{Z}$.

(c) Prove that the only units in R are ± 1.

36. **Dedekind-Hasse criterion:** Let S be an integral domain and let $N\colon S \to \mathbb{Z}$ be a map such that $N(0) = 0$, $N(x) > 0$ for any $0 \neq x \in S$ and that satisfies that for any $0 \neq f, g \in S$, either g divides f in S, or there exist elements $s, t \in S$ such that $0 < N(sf - tg) < N(g)$. Prove that S is then a PID.

37. Let us check that R, with the norm N defined above, satisfies the Dedekind-Hasse criterion. In this way, it is shown that R is a PID. To do so, let f, g be nonzero elements of R such that $\dfrac{f}{g} \notin R$. Write $\dfrac{f}{g} = \dfrac{a + b\sqrt{-19}}{c} \in F$, with $a, b, c \in \mathbb{Z}$ without proper common divisors and $c > 1$ (since g does not divide f in R).

(a) Observe that, since N is multiplicative, the condition $0 < N(sf - tg) < N(g)$ is equivalent to

$$0 < N\left(\frac{f}{g}s - t\right) < 1 \qquad (*)$$

(b) Since a, b, c have no common divisors, there are elements $x, y, z \in \mathbb{Z}$ with $ax + by + cz = 1$. Take elements $q, r \in \mathbb{Z}$ such that $ay - 19bx = cq + r$ and $|r| \leq \frac{c}{2}$. Then check that the elements $s = y + x\sqrt{-19}$ and $t = q - z\sqrt{-19}$ satisfy equation $(*)$ if $c \geq 5$.

(c) If $c = 2$, since $\frac{f}{g} \notin R$ then a, b have different parity and then you may check that $s = 1$ and $t = \frac{(a-1)+b\sqrt{-19}}{2}$ are elements in R that satisfy $(*)$.

(d) If $c = 3$, show that $a^2 + 19b^2$ is not a multiple of 3, so you can find elements $q, r \in \mathbb{Z}$ such that $a^2 + 19b^2 = 3q + r$ with $r = 1$ or $r = 2$. Then the elements $s = a - b\sqrt{-19}$ and $t = q$ satisfy $(*)$.

(e) Finally, if $c = 4$, a and b cannot be both even. If only one of them is odd you can find elements $q, r \in \mathbb{Z}$ such that $a^2 + 19b^2 = 4q + r$ and $0 < r < 4$. In this case $s = a - b\sqrt{-19}$ and $t = q$ satisfy $(*)$. Also, if both a and b are odd, then show that there is an integer $q \in \mathbb{Z}$ such that $a^2 + 19b^2 = 8q + 4$, so that $s = \frac{a-b\sqrt{-19}}{2}$ and $t = q$ are elements in R that satisfy $(*)$.

[36] If I is a nonzero ideal of S and $0 \neq b \in I$ with minimal $N(b)$, then you may check that $I = (b)$.

38. In this exercise, it will be shown that R is not a euclidean domain. Let D be an integral domain and let $\tilde{D} = D^\times \cup \{0\}$. An element $u \in D \setminus \tilde{D}$ is said to be a *universal divisor* if for any $x \in D$ there exists $z \in \tilde{D}$ such that u divides $x - z$ in D.

    (a) Prove that if D is not a field and D does not contain universal divisors, then D is not a euclidean domain.

    (b) Prove that our ring R does not contain universal divisors and, therefore, it is not a euclidean domain.

39. Prove that $S = \{a + b\frac{1+\sqrt{-m}}{2} : a, b \in \mathbb{Z}\}$ is a euclidean domain for $m = 3, 7, 11$.

40. Compute the invariant factors $d_1, \ldots, d_r$ of the matrix A, and invertible matrices P, Q such that $PAQ = \sum_{i=1}^{r} d_i E_{ii}$, where,

    (a) $A = \begin{pmatrix} 1 & -4 & -2 & 1 \\ 2 & 7 & 2 & -4 \\ -4 & 1 & 2 & 2 \end{pmatrix} \in \mathrm{Mat}_{3\times 4}(\mathbb{Z})$.

    (b) $A = \begin{pmatrix} X-16 & 2 & -14 \\ 7 & X-3 & 7 \\ X-2 & 0 & X-2 \end{pmatrix} \in \mathrm{Mat}_3(F[X])$, F a field.

---

[38] (a) If D were a euclidean domain, then any element of $D \setminus \tilde{D}$ of minimal norm would be a universal divisor.
(b) Prove that the only divisors in R of 2 are $\{\pm 1, \pm 2\}$ and, in the same vein, the only divisors of 3 are $\{\pm 1, \pm 3\}$. Take $x = 2$ and prove that if u were a universal divisor, u would be a nonunit divisor of 2 or 3. Thus, either $u = \pm 2$ or $u = \pm 3$. However, with $y = \frac{1+\sqrt{-19}}{2}$, it can be easily checked that neither ± 2 nor ± 3 are universal divisors.

[39] To get the quotient of two elements, compute the quotient in $\mathbb{C}$, which will be of the form $u + v\sqrt{-m}$ with $u, v \in \mathbb{Q}$, and choose now integers $c, d \in \mathbb{Z}$ with $|c - 2u| \leq 1$, $|d - 2v| \leq \frac{1}{2}$ and of the same parity. Now take the element $\frac{c+d\sqrt{-m}}{2}$ as the quotient in S.

Appendix: The Axiom of Choice and Zorn's Lemma

The *power set* of a set A is the set consisting of all the subsets of A (including the empty set). It will be denoted by 2^A.

Let us prove that the Axiom of Choice, Zorn's Lemma and the Well Ordering Principle are equivalent.

Theorem. *The following assertions are equivalent:*

(i) ***The Axiom of Choice:*** *Let I be a nonempty set and let $\{A_i\}_{i\in I}$ be a family of nonempty sets, then $\prod_{i\in I} A_i$ is not empty.*

(ii) *Let A be a nonempty set, then there is a map $f : 2^A \setminus \{\emptyset\} \to A$, such that $f(B) \in B$ for any $\emptyset \neq B \subseteq A$. (We say that f is a* choice function *on A.)*

(iii) ***Hausdorff maximal principle:*** *Any partially ordered nonempty set has a maximal chain. (Chains are ordered by inclusion.)*

(iv) ***Zorn's Lemma:*** *Let A be a partially ordered nonempty set such that there is an upper bound for any of its chains. Then there are maximal elements of A.*

(v) ***Well Ordering Principle:*** *Any nonempty set admits a well order.*

Proof. **(i)⇒(ii):** It is enough to consider an element of $\prod_{\emptyset\neq B\subseteq A} B$.

(iii)⇒(iv): If A is a partially ordered nonempty set such that there is an upper bound for any of its chains, and if C is a maximal chain of A, let $u \in A$ be an upper bound of C. If $a \in A$ satisfies $u < a$, then $a \notin C$ and $C \cup \{a\}$ is a chain strictly larger than C, a contradiction. Therefore, u is a maximal element of A.

(iv)⇒(v): Let A be a nonempty set, and let X be the set of pairs $(B, \leq)$, where B is a subset of A and $\leq$ is a well order for B. The subsets of A consisting of a single element are well ordered, so X is nonempty. Define a binary relation on X by declaring $(B_1, \leq_1) \preceq (B_2, \leq_2)$ if $B_1 \subseteq B_2$, $\leq_1$ is the restriction of $\leq_2$ to B_1, and $b_1 \leq_2 b_2$ for any $b_1 \in B_1$ and $b_2 \in B_2 \setminus B_1$.

Any chain in X has an upper bound whose first component is the union of the first components of the elements of the chain. Zorn's Lemma implies that there is a maximal element $(B, \leq)$ in X. But if $B \neq A$ and $a \in A \setminus B$, then $(B, \leq) \preceq (B \cup \{a\}, \leq')$, with $b_1 \leq' b_2$ if and only if $b_1 \leq b_2$, and $b \leq' a$ for any $b, b_1, b_2 \in B$. This contradicts the maximality of $(B, \leq)$. Hence $B = A$, and $\leq$ is a well order of A.

(v)⇒(i): Let I be a nonempty set and let $\{A_i\}_{i\in I}$ be a family of nonempty sets. Let $\leq$ be a well order in $\cup_{i\in I}A_i$, and consider the map $f : I \to \cup_{i\in I}A_i$ such that $f(i)$ is the minimum of A_i for any $i \in I$. This shows that $\prod_{i\in I} A_i$ is not empty.

(ii)⇒(iii): This final step requires a lot of patience.

Let A be a nonempty partially ordered set and let $\mathcal{C}$ the set of chains in A, ordered by inclusion. Clearly $\mathcal{C} \neq \emptyset$ as $\{a\} \in \mathcal{C}$ for any $a \in A$. Take a choice function $f : 2^{\mathcal{C}} \setminus \{\emptyset\} \to \mathcal{C}$, so $f(\mathcal{B}) \in \mathcal{B}$ for any $\emptyset \neq \mathcal{B} \subseteq \mathcal{C}$. Assume that there are no maximal chains. In other words, assume that $\mathcal{C}$ contains no maximal elements.

For any $C \in \mathcal{C}$ consider the following subset of $\mathcal{C}$:

$$\mathcal{S}(C) = \{D \in \mathcal{C} : C \subsetneqq D\}.$$

Since $\mathcal{C}$ has no maximal elements, $\mathcal{S}(C)$ is not empty. Define $g : \mathcal{C} \to \mathcal{C}$ by $g(C) = f(\mathcal{S}(C))\,(\in \mathcal{S}(C))$. Thus, $g(C)$ is a chain in A strictly containing C.

For any chain $B \in \mathcal{C}$, consider the set $\mathfrak{C}_B \subseteq 2^{\mathcal{C}}$ consisting of those subsets $\mathcal{D}$ of $\mathcal{C}$ satisfying the following properties:

(1) $B \in \mathcal{D}$.

(2) If C belongs to $\mathcal{D}$, then also $g(C)$ belongs to $\mathcal{D}$.

(3) Any $C \in \mathcal{D}$ contains B.

(4) For any chain $\mathcal{E} \in 2^{\mathcal{C}}$ (relative to inclusion) with $\mathcal{E} \subseteq \mathcal{D}$, the chain $\cup\mathcal{E}$ in A, obtained as the union of the elements of $\mathcal{E}$, belongs to $\mathcal{D}$.

Note that $\mathfrak{C}_B$ is not empty, because $\{C \in \mathcal{C} : B \subseteq C\}$ belongs to it.

Consider now the intersection $\mathcal{B}$ of the elements in $\mathfrak{C}_B$: $\mathcal{B} = \cap\mathfrak{C}_B$, which is a subset of $\mathcal{C}$ that obviously satisfies conditions (1), (2), (3) and (4). Intuitively, we have

$$\mathcal{B} = \{B, g(B), \ldots, g^n(B), \ldots, \cup_{n\in\mathbb{N}} g^n(B), g\big(\cup_{n\in\mathbb{N}} g^n(B)\big), \ldots\}.$$

Let us check that $\mathcal{B}$ is a chain in $\mathcal{C}$ relative to inclusion. To do this, consider the subset

$$\mathcal{B}^* = \{C \in \mathcal{B} : \forall D \in \mathcal{B}, \quad D \subsetneqq C \;\Rightarrow\; g(D) \subseteq C\}.$$

Note that $B \in \mathcal{B}^*$ trivially, so this subset $\mathcal{B}^*$ is not empty. Also, for any $C \in \mathcal{B}^*$, consider the subset

$$\mathcal{B}_C = \{D \in \mathcal{B} : \text{either } D \subseteq C \text{ or } g(C) \subseteq D\}.$$

It is clear that $\mathcal{B}_C$ satisfies (1) and (3). It also fulfills condition (2), because for $D \in \mathcal{B}_C$, either $D \subsetneqq C$, and hence $g(D) \subseteq C$ as $C \in \mathcal{B}^*$, or $D = C$ and then trivially $g(C) \subseteq g(D)$, or $g(C) \subseteq D$ and then $g(C) \subsetneqq g(D)$.

Finally, $\mathcal{B}_C$ also fulfills (4), because if $\mathcal{E}$ is a chain of elements in $\mathcal{B}_C$, either for any $D \in \mathcal{E}$ we have $D \subseteq C$, and hence $\cup\mathcal{E} \subseteq C$, or there is an element $D \in \mathcal{E}$ with $g(C) \subseteq D$, but then $g(C) \subseteq \cup\mathcal{E}$.

By definition of $\mathcal{B}$, we conclude that $\mathcal{B}_C = \mathcal{B}$, for any $C \in \mathcal{B}^*$.

Now, $\mathcal{B}^*$ satisfies (1) and (3) trivially. It satisfies condition (2), because for $C \in \mathcal{B}^*$ and $D \in \mathcal{B}$, we have $\mathcal{B}_C = \mathcal{B}$, so either $D \subseteq C$ or $g(C) \subseteq D$. Hence, if $D \subsetneqq g(C)$, then $g(C) \nsubseteq D$ and thus $D \subseteq C$. Thus, either $D = C$, so $g(D) = g(C)$, or $D \subsetneqq C$, so $g(D) \subseteq C \subsetneqq g(C)$, as $C \in \mathcal{B}^*$. We conclude that $g(C) \in \mathcal{B}^*$.

If $\mathcal{E}$ is a chain of elements in $\mathcal{B}^*$ and $D \in \mathcal{B}$ satisfies $D \subsetneqq \cup\mathcal{E}$, then, since $\mathcal{B} = \mathcal{B}_C$ for any $C \in \mathcal{E}$, either $D \subseteq C$ or $g(C) \subseteq D$. If $g(C) \subseteq D$ for any $C \in \mathcal{E}$, then $\cup\mathcal{E} \subseteq D$, a contradiction. Hence, there exists an element $C \in \mathcal{E}$ with $D \subseteq C$. But $D \subsetneqq \cup\mathcal{E}$, so there is an element $E \in \mathcal{E}$ such that $D \subsetneqq E$ ($\mathcal{E}$ is a chain). Then, $g(D) \subseteq E$ as $E \in \mathcal{B}^*$. Therefore, $g(D) \subseteq \cup\mathcal{E}$, and this proves that $\cup\mathcal{E}$ belongs to $\mathcal{B}^*$.

By definition of $\mathcal{B}$, we conclude now that $\mathcal{B}^* = \mathcal{B}$.

For any $C, D \in \mathcal{B}$, we have $\mathcal{B}_C = \mathcal{B}$ as $C \in \mathcal{B} = \mathcal{B}^*$, and hence, either $D \subseteq C$ or $C \subsetneqq g(C) \subseteq D$. Thus $\mathcal{B}$ is a chain, as required.

But condition (4) implies that the chain $\cup\mathcal{B}$ belongs to $\mathcal{B}$, and condition (2) gives $g(\cup\mathcal{B}) \in \mathcal{B}$ so, in particular, $g(\cup\mathcal{B}) \subseteq \cup\mathcal{B}$, a contradiction with the definition of g.

□

Chapter 2

Modules

Rings are more general than fields. The concept analogous to that of a vector space over a field, is the concept of a module over a ring. This chapter will deal mainly with modules over principal ideal domains.

§ 1. Definition and examples

1.1 Definition. Let R be a ring. A *left module* over R (or a *left R-module*) is a set M endowed with two operations:

addition: $M \times M \to M$, $(x, y) \mapsto x + y$, and

multiplication by scalars: $R \times M \to M$, $(r, x) \mapsto rx$,

satisfying the following properties:

(i) The addition is associative, commutative, M contains a neutral element for it (this is called the *zero* element and denoted by 0) and any element has an opposite element (the opposite of a is denoted by $-a$).

(ii) For any $x, y \in M$ and $r, s \in R$:

(a) $(r + s)x = rx + sx$ (distributivity relative to the addition in R),

(b) $(rs)x = r(sx)$ (associativity),

(c) $r(x + y) = rx + ry$ (distributivity relative to the addition in M).

If, in addition, the ring R is unital, we must have

(d) $1x = x$ for any $x \in R$.

Any module is, in particular, an *abelian group*. We may define in a similar way a *right R-module*. When we say a module, we will refer to a left module, unless otherwise stated.

1.2 Definition. Let M be a module over a ring R. An R-submodule of M is any nonempty subset N of M which is closed under addition, opposite elements, and multiplication by scalars: $x + y \in N$, $-x \in N$, and $rx \in N$ for any $r \in R$ and $x \in N$. (Notation: $N \leq M$.)

1.3 Examples.

(i) In case R is a field, a left R-module is just a vector space over R. Its submodules are the vector subspaces.

(ii) Any $\mathbb{Z}$-module is, in particular, an abelian group. Conversely, given any abelian group $(A, +)$ we can make A into a $\mathbb{Z}$-module as follows: for any $n \in \mathbb{Z}$ and $a \in A$ define:

$$na = \begin{cases} a + a + \cdots + a \quad n \text{ times} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ (-a) + (-a) + \cdots + (-a) \quad -n \text{ times} & \text{if } n < 0. \end{cases}$$

This gives A the structure of a $\mathbb{Z}$-module, and it is the only way to do so. Hence abelian groups and $\mathbb{Z}$-modules coincide. Moreover, the subgroups are precisely the submodules.

(iii) Any ring R is a module over itself. Its submodules are the left ideals.

(iv) If $M_1, \ldots, M_n$ are modules over the ring R, so is its cartesian product (also called *direct product*) $M_1 \times \cdots \times M_n$, with operations given by $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ and $r(x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$, for any $x_i, y_i \in M_i$, $i = 1, \ldots, n$ and $r \in R$.

(v) If M is a module over the ring R, and I is an ideal of R which *annihilates* M (that is, $rx = 0$ for any $r \in I$ and $x \in M$), then M is naturally a module over the quotient ring R/I, with the multiplication by scalars defined by $(r + I)x = rx$ for any $r \in R$ and $x \in M$.

As for rings (or any other algebraic structure) we must consider the appropriate maps among modules:

1.4 Definition. Let M and N be two modules over a ring R and let $\varphi\colon M \to N$ be a map. Then

- φ is said to be a *homomorphim* if

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(rx) = r\varphi(x),$$

for any $x, y \in M$ and $r \in R$.

- If φ is a homomorphism, then its *kernel* is the subset $\ker \varphi = \varphi^{-1}(0)$ of M, while its *image* is the set $\operatorname{im} \varphi = \varphi(M)$. (It is clear that $\ker \varphi$ is a submodule of M and $\operatorname{im} \varphi$ is a submodule of N.)

- A homomorphism is said to be a *monomorphism* if it is one-to-one, an *epimorphism* if it is surjective, and an *isomorphism* if it is a bijection. Moreover, the homomorphisms $\psi : M \to M$ are called *endomorphisms*. If they are bijective, they are called *automorphisms*.

Let M be a module over a ring R and let N be a submodule of M. Consider the binary relation on M defined by

$$x \sim y \quad \text{if} \quad x - y \in N, \tag{1.5}$$

for any $x, y \in M$. Then $\sim$ is an equivalence relation. The equivalence class of any $x \in M$ is the set

$$x + N = \{x + z : z \in N\}.$$

The quotient set (that is, the set of equivalence classes) is denoted by M/N.

Moreover, if $x, y, z, t \in M$, $r \in R$, and $x \sim y$, $z \sim t$, then also $x+z \sim y+t$ and $rx \sim ry$, so an addition and a multiplication by scalars can be defined on M/N by means of:

$$(x + N) + (y + N) = (x + y) + N,$$
$$r(x + N) = rx + N.$$

With these two operations, the quotient set M/N is an R-module, which is called the *quotient module* of M by N.

With the same arguments used for rings we obtain the usual Isomorphism Theorems:

1.6 Properties. *Let M and N be two R-modules.*

- ***First Isomorphism Theorem:*** *Let $\varphi : M \to N$ be a homomorphism, then the quotient module $M/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$ through the isomorphism*

$$\bar{\varphi} : M/\ker\varphi \to \operatorname{im}\varphi$$
$$x + \ker\varphi \mapsto \varphi(x).$$

- *Let A be a submodule of M, then the map $\pi : M \to M/A$, $x \mapsto x + A$, is an epimorphism, called the* natural projection *of M over M/A. Besides, $\ker\pi = A$. In particular, this shows that any submodule is the kernel of some homomorphism.*

- *Let $\varphi : M \to N$ be a homomorphism, then*

$$\boxed{\begin{array}{l}\varphi \text{ is a monomorphism} \iff \ker\varphi = 0,\\ \varphi \text{ is an epimorphism} \iff \operatorname{im}\varphi = N.\end{array}}$$

- ***Second Isomorphism Theorem:*** *Let A and B be two submodules of M, then $A+B = \{a+b : a \in A, b \in B\}$ is a submodule of M (called the* sum *of A and B), $A \cap B$ is a submodule of A and the map*

$$\begin{aligned} A/A \cap B &\to A + B/B \\ a + A \cap B &\mapsto a + B, \end{aligned}$$

  is an isomorphism.

- ***Third isomorphism theorem:*** *Let A and B be two submodules of M with $A \subseteq B$, then B/A is a submodule of M/A and the quotient modules $(M/A)/(B/A)$ and M/B are isomorphic.*

- *Let A be a submodule of M, then the map*

$$\begin{aligned} \{\textit{submodules of } M \textit{ containing } A\} &\to \{\textit{submodules of } M/A\} \\ B \qquad &\mapsto \qquad B/A, \end{aligned}$$

  is a bijection. The inverse map is given by $\tilde{B} \leq M/A \mapsto B = \{x \in M : x + A \in \tilde{B}\}$.

§ 2. Direct sums. Free modules

2.1 Definition. Let M be a module over a ring R, and let $N_1, \ldots, N_m$ be submodules of M. The sum $N_1 + \cdots + N_m = \{x_1 + \cdots + x_m : x_i \in N_i,\ 1 \leq i \leq m\}$ is said to be *direct* if every $x \in N_1 + \cdots + N_m$ can be written uniquely in the form $x_1 + \cdots + x_m$, with $x_i \in N_i$, $1 \leq i \leq m$. (Notation: $N_1 \oplus \cdots \oplus N_m$.)

In other words, the natural map

$$\begin{aligned} N_1 \times \cdots \times N_m &\to N_1 + \cdots + N_m \\ (x_1, \ldots, x_m) &\mapsto x_1 + \cdots + x_m, \end{aligned}$$

is an isomorphism.

2.2 Definition. Let M be a module over a unital ring R and let $a_1, \ldots, a_n$ be elements in M. Then:

(i) The set $\{a_1, \ldots, a_n\}$ is called a *spanning set* of M if any element x of M can be written as $x = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \ldots, r_n \in R$. That is, any element of M is a linear combination of the a_i's: $M = Ra_1 + \cdots + Ra_n$. In other words, the natural homomorphism of modules $R^n \to M$, $(r_1, \ldots, r_n) \mapsto r_1 a_1 + \cdots + r_n a_n$ is an epimorphism. In this case M is said to be *finitely generated*.

(ii) M is said to be *cyclic* if it has a spanning set consisting of just one element: $M = Ra$ for some $a \in M$.

(iii) The set $\{a_1, \ldots, a_n\}$ is called a *basis* of M if any element x of M can be written uniquely as $x = r_1a_1 + \cdots + r_na_n$ for some $r_1, \ldots, r_n \in R$. That is, the natural homomorphism of modules $R^n \to M$, $(r_1, \ldots, r_n) \mapsto r_1a_1 + \cdots + r_na_n$ is an isomorphism. In this case M is said to be a finitely generated *free module*.

2.3 Example. Given any unital ring R and natural number n, the R-module R^n is free. Its *canonical basis* is $\{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$.

Any free R-module with a basis consisting of n elements is isomorphic to R^n.

2.4 Proposition. *Let $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_m\}$ be two bases of a module M over a unital commutative ring R. Then $n = m$. This common number is called the* rank *of M.*

Proof. There are matrices $A \in \mathrm{Mat}_{n\times m}(R)$ and $B \in \mathrm{Mat}_{m\times n}(R)$ such that:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = A \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \qquad \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = B \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

and by uniqueness of the linear combinations, they satisfy $AB = I_n$ and $BA = I_m$. Take a maximal ideal J of R, apply the natural projection $R \to R/J$ to the entries of A and B to get matrices $\hat{A} \in \mathrm{Mat}_{n\times m}(R/J)$ and $\hat{B} \in \mathrm{Mat}_{m\times n}(R/J)$ which satisfy $\hat{A}\hat{B} = I_n$, $\hat{B}\hat{A} = I_m$ as matrices over R/J, which is a field. But over a field, this is only possible if $n = m$. □

The situation here is worse than for vector spaces. For instance, not every finitely generated module is free. For instance, take the cyclic $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$. It cannot be free as $2x = 0$ for any $x \in M$, and hence $0x = 2x$ for any x, so we never have uniqueness of coefficients in linear combinations.

§ 3. Finitely generated modules over principal ideal domains

3.1 Lemma. *Let R be a PID, and let M be a finitely generated module, generated by n elements. Then any submodule N of M is finitely generated too, and may be generated by m elements, with $m \leq n$.*

Proof. Let $M = Ra_1 + \cdots + Ra_n$. If $n = 0$, the result is clear. Otherwise let

$$I = \{r \in R : \exists r_1, \ldots, r_{n-1} \in R \text{ such that } r_1a_1 + \cdots + r_{n-1}a_{n-1} + ra_n \in N\}.$$

I is an ideal of R, so there is an element $d \in R$ such that $I = (d)$, since R is a PID. As $d \in I$, there are elements $d_1, \ldots, d_{n-1} \in R$ such that $\hat{a}_n =$

$d_1a_1+\cdots+d_{n-1}a_{n-1}+da_n \in N$. Then for any element $a = r_1a_1+\cdots+r_na_n$ in N, $r_n \in I$, so $r_n = sd$ for some $s \in R$, and hence $a - s\hat{a}_n \in N \cap (Ra_1 + \cdots + Ra_{n-1})$. Therefore,

$$N = \big(N \cap (Ra_1 + \cdots + Ra_{n-1})\big) + R\hat{a}_n.$$

Applying an inductive argument, we may assume that $N\cap(Ra_1+\cdots+Ra_{n-1})$ has a spanning set consisting of $m-1 \leq n-1$ elements: $N \cap (Ra_1 + \cdots + Ra_{n-1}) = Rb_1 + \cdots + Rb_{m-1}$, and hence, $N = Rb_1 + \cdots + Rb_{m-1} + R\hat{a}_n$. □

3.2 Definition. Let M be a module over an integral domain R, and let $x \in M$.

(i) The ideal $\operatorname{ann}(x) = \{r \in R : rx = 0\}$ is called the *annihilator* of x.

(ii) The submodule $\operatorname{tor}(M) = \{z \in M : \operatorname{ann}(z) \neq 0\}$ is called the *torsion submodule* of M.

(iii) The module M is said to be *torsion-free* if $\operatorname{tor}(M) = 0$, and it is called a *torsion module* if $M = \operatorname{tor}(M)$.

Note that if x is an element of a module M over an integral domain R, then $\operatorname{ann}(x)$ is the kernel of the homomorphism $R \to M$, $r \mapsto rx$, whose image is the submodule Rx. Hence

$$\boxed{Rx \text{ is isomorphic to } R/\operatorname{ann}(x).}$$

3.3 Theorem. *Let M be a finitely generated module over a PID R. Then there exist $m, n \in \mathbb{N} \cup \{0\}$, $m \leq n$, nonzero elements $d_1, \ldots, d_m \in R \setminus R^\times$ with $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_m$, and elements $u_1, \ldots, u_n \in M$ such that*

- $M = Ru_1 \oplus Ru_2 \oplus \cdots \oplus Ru_n$,
- $\operatorname{ann}(u_i) = (d_i)$ *for* $1 \leq i \leq m$, $\operatorname{ann}(u_i) = 0$ *for* $m+1 \leq i \leq n$.

In particular, M is isomorphic to $R/(d_1) \times \cdots \times R/(d_m) \times R^{n-m}$.

Proof. Let $\{x_1, \ldots, x_t\}$ be a spanning set of M. The homomorphism

$$\begin{aligned} \phi : R^t &\to M \\ (r_1, \ldots, r_t) &\mapsto r_1x_1 + \cdots + r_tx_t, \end{aligned}$$

is onto. By the previous lemma, its kernel $K = \ker\phi$ is finitely generated. Let $\{v_1 = (1, 0, \ldots, 0, 0), \ldots, v_t = (0, 0, \ldots, 0, 1)\}$ be the canonical basis of R^t and let $\{w_1, \ldots, w_l\}$ be a spanning set of K. Then there is a matrix $A \in \operatorname{Mat}_{l\times t}(R)$ such that

$$\begin{pmatrix} w_1 \\ \vdots \\ w_l \end{pmatrix} = A \begin{pmatrix} v_1 \\ \vdots \\ v_t \end{pmatrix}.$$

There are invertible matrices (see 5.1) $P \in \mathrm{GL}_l(R)$, $Q \in \mathrm{GL}_t(R)$, such that

$$PAQ = \begin{pmatrix} f_1 & & & & \\ & \ddots & & & \\ & & f_k & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

for some elements $f_1, \dots, f_k \in R \setminus \{0\}$ with $f_1 \,|\, f_2 \,|\, \cdots \,|\, f_k$.

Write

$$\begin{pmatrix} \hat{w}_1 \\ \vdots \\ \hat{w}_l \end{pmatrix} = P \begin{pmatrix} w_1 \\ \vdots \\ w_l \end{pmatrix}, \qquad \begin{pmatrix} \hat{v}_1 \\ \vdots \\ \hat{v}_t \end{pmatrix} = Q^{-1} \begin{pmatrix} v_1 \\ \vdots \\ v_t \end{pmatrix},$$

to obtain

$$\begin{pmatrix} \hat{w}_1 \\ \vdots \\ \vdots \\ \hat{w}_l \end{pmatrix} = \begin{pmatrix} f_1 & & & & \\ & \ddots & & & \\ & & f_k & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix} \begin{pmatrix} \hat{v}_1 \\ \vdots \\ \vdots \\ \hat{v}_t \end{pmatrix}.$$

Since P and Q are invertible, $\{\hat{v}_1, \dots, \hat{v}_t\}$ is a basis of R^t, and $\{\hat{w}_1, \dots, \hat{w}_l\}$ is a spanning set of K. But $\hat{w}_i = 0$ for $i > k$, so $\{\hat{w}_1, \dots, \hat{w}_k\}$ is a spanning set of K.

Then,

$$M = \operatorname{im} \phi = R\phi(\hat{v}_1) + \cdots + R\phi(\hat{v}_t).$$

Now, for $r_1, \dots, r_t \in R$, we have $r_1\phi(\hat{v}_1) + \cdots + r_t\phi(\hat{v}_t) = 0$ if and only if $r_1\hat{v}_1 + \cdots + r_t\hat{v}_t \in K$, and this happens if and only if (as the $\hat{v}_i$'s form a basis) $f_i \,|\, r_i$ for $1 \le i \le k$, and $r_i = 0$ for $k < i \le t$. In particular we get:

- $\operatorname{ann}(\phi(\hat{v}_i)) = (f_i)$ for $1 \le i \le k$, and $\operatorname{ann}(\phi(\hat{v}_i)) = 0$ for $k < i \le t$,
- $M = R\phi(\hat{v}_1) \oplus \cdots \oplus R\phi(\hat{v}_t)$.

Finally, if $f_i \in R^\times$, then $\operatorname{ann}(\phi(\hat{v}_i)) = (f_i) = (1)$, so $\phi(\hat{v}_i) = 0$. (Note that if $f_i \in R^\times$, then $f_1, \dots, f_{i-1} \in R^\times$ too.)

If s denotes the largest index such that $f_i \in R^\times$, we have

$$M = R\phi(\hat{v}_{s+1}) \oplus \cdots \oplus R\phi(\hat{v}_t),$$

and we get the result with $m = k - s$, $n = t - s$, $d_i = f_{s+i}$ and $u_i = \phi(\hat{v}_{s+i})$, for $s + 1 \le i \le t$. □

In the situation of this theorem, we have $\operatorname{tor}(M) = Ru_1 \oplus \cdots \oplus Ru_m$, and hence $n - m$ is the rank of the free module $R/\operatorname{tor}(M)$ $\big(\cong Ru_{m+1} \oplus \cdots \oplus Ru_n\big)$.

This is called the *free rank* of M. With a slight abuse of notation, the elements $d_1, \ldots, d_m$ are called the *invariant factors* of M. We will check later on that they are essentially determined by M itself, and do not depend on the particular generators $u_1, \ldots, u_n$.

3.4 Example. Let $R = \mathbb{Z}$, and let M be the quotient of $\mathbb{Z}^3$ by the submodule K generated by $q_1 = 2e_1+4e_2+2e_3$ and $q_2 = 6e_1+4e_2+5e_3$, where $\{e_1, e_2, e_3\}$ is the canonical basis of $\mathbb{Z}^3$. Let $\phi : \mathbb{Z}^3 \to M$ be the canonical projection, whose kernel K is generated by q_1 and q_2. We have

$$\begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 2 \\ 6 & 4 & 5 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}.$$

Using the computations in Example 5.3 of Chapter 1 we obtain that M is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}$.

3.5 Lemma. *Let M be a module over a PID R.*

Fusion of cyclic modules: *Let x_1, x_2 be two elements of M with* $\operatorname{ann}(x_1) = (a_1) \neq 0$, $\operatorname{ann}(x_2) = (a_2) \neq 0$, *and* $\gcd(a_1, a_2) = 1$. *Then the sum $Rx_1 + Rx_2$ is direct,* $\operatorname{ann}(x_1 + x_2) = (a_1a_2)$, *and $R(x_1 + x_2) = Rx_1 \oplus Rx_2$.*

Fission of cyclic modules: *Let x be an element of M with* $\operatorname{ann}(x) = (a) \neq 0$. *Let $a = a_1a_2$ with* $\gcd(a_1a_2) = 1$. *Then $Rx = R(a_2x) \oplus R(a_1x)$ and* $\operatorname{ann}(a_2x) = (a_1)$, $\operatorname{ann}(a_1x) = (a_2)$.

Proof. Take $s_1, s_2 \in R$ with $s_1a_1 + s_2a_2 = 1$.

For the first part, note that $x_1 = 1x_1 = s_2a_2x_1$ and $x_2 = s_1a_1x_2$, and hence, if $r_1, r_2 \in R$ satisfy $r_1x_1 + r_2x_2 = 0$, then $r_1x_1 = r_1s_2a_2x_1 = s_2a_2(r_1x_1 + r_2x_2) = 0$. In the same vein we prove $r_2x_2 = 0$. Thus, the sum Rx_1+Rx_2 is direct. Also, $Rx_1 = R(s_2a_2)x_1 = R(s_2a_2)(x_1+x_2) \subseteq R(x_1+x_2)$, so $Rx_1 + Rx_2 = R(x_1 + x_2)$. Finally, if $r(x_1 + x_2) = 0$, then as above, $rx_1 = 0 = rx_2$, so $a_i \,|\, r$, $i = 1, 2$, and hence $a_1a_2 \,|\, r$, because a_1 and a_2 are relatively prime. This shows $\operatorname{ann}(x_1 + x_2) = (a_1a_2)$.

For the second part, $x = 1x = s_2(a_2x) + s_1(a_1x) \in R(a_2x) + R(a_1x)$, so $Rx = R(a_2x) + R(a_1x)$. Moreover, for $r \in R$, $r(a_2x) = 0$ if and only if $a_1a_2 \mid a_2r$, if and only if $a_1 \mid r$. Hence $\operatorname{ann}(a_2x) = (a_1)$ and, similarly, $\operatorname{ann}(a_1x) = (a_2)$. The fact that the sum is direct now follows from the arguments above. □

3.6 Example. The $\mathbb{Z}$-module $\mathbb{Z}_{60}$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$. Note that this also follows from the Chinese Remainder Theorem, which gives an isomorphism of rings $\mathbb{Z}_{60} \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$, but the isomorphism in the Chinese Remainder Theorem is an isomorphism of R-modules too.

Any nonzero and nonunit element in R factorizes 'uniquely' into a product of irreducible elements. Therefore, we may use the previous lemma to split the cyclic submodules in the theorem above to get:

3.7 Corollary. *Let M be a finitely generated module over a PID R. Then there are $m \in \mathbb{N} \cup \{0\}$ and elements $v_1, \dots, v_m \in M$, such that $M = Rv_1 \oplus \cdots \oplus Rv_m$, and for each $i = 1, \dots, m$, either* $\operatorname{ann}(v_i) = 0$, *or* $\operatorname{ann}(v_i) = (p_i^{l_i})$ *for a prime p_i and natural number l_i.*

Again with a slight abuse of notation, the powers $p_i^{n_i}$ in the corollary are called *elementary divisors* of M.

Our next aim is to check that both invariant factors and elementary divisors depend only on M (up to associates), and not on the particular decomposition into a direct sum of cyclic modules.

3.8 Theorem. *Let M be a finitely generated torsion module over a PID R.*

Uniqueness of invariant factors: *If $M = Ru_1 \oplus \cdots \oplus Ru_n = R\hat{u}_1 \oplus \cdots \oplus R\hat{u}_m$, with* $\operatorname{ann}(u_i) = (d_i)$, $\operatorname{ann}(\hat{u}_j) = (\hat{d}_j)$, $0 \neq d_i, \hat{d}_j \in R \setminus R^\times$, *for $i = 1, \dots, n$, $j = 1, \dots, m$, and $d_1 | \dots | d_n$, $\hat{d}_1 | \dots | \hat{d}_m$; then $n = m$ and for each $i = 1, \dots, n$, d_i and $\hat{d}_i$ are associates. (That is, $(d_i) = (\hat{d}_i)$.)*

Uniqueness of elementary divisors: *If $M = Rv_1 \oplus \cdots \oplus Rv_n = R\hat{v}_1 \oplus \cdots \oplus R\hat{v}_m$, with* $\operatorname{ann}(v_i) = (p_i^{l_i})$, $\operatorname{ann}(\hat{v}_j) = (\hat{p}_j^{\hat{l}_j})$, *for prime elements $p_i, \hat{p}_j$ and natural numbers l_i and $\hat{l}_j$, $i = 1, \dots, n$, $j = 1, \dots, m$; then $n = m$ and there is a bijection $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ such that p_i and $\hat{p}_{\sigma(i)}$ are associates and $l_i = \hat{l}_{\sigma(i)}$. (That is, the powers of primes involved are the same up to associates.)*

Proof. The previous lemma shows that given any decomposition 'into invariant factors', we can split the direct summands to get a decomposition 'into elementary divisors'. Therefore, it is enough to prove the second part.

Given any prime element $p \in R$, the submodule $\operatorname{tor}_p(M) = \{x \in M : \exists t \in \mathbb{N} \text{ such that } p^t x = 0\}$ equals

$$\operatorname{tor}_p(M) = \bigoplus_{\substack{1 \le i \le n \\ p \approx p_i}} Rv_i = \bigoplus_{\substack{1 \le j \le m \\ p \approx p_j}} R\hat{v}_j,$$

where $p \approx p_i$ denotes that p and p_i are associates. Note that if p_i and p are associates then $Rv_i \cong R/(p_i^{l_i}) = R/(p^{l_i})$. If $\operatorname{ann}(v_i) = (p^{l_i})$, then $Rv_i \cong R/(p^{l_i})$ and $p(Rv_i) \cong (p)/(p^{l_i})$, so the R-module $Rv_i/p(Rv_i)$ is isomorphic to $\big(R/(p^{l_i})\big)/\big((p)/(p^{l_i})\big) \cong R/(p)$. This is an R-module annihilated by the ideal (p), so it is a module over the field $R/(p)$ (See Example 1.3). We obtain, using Exercise 1, the following isomorphisms:

$$\operatorname{tor}_p(M)/p\operatorname{tor}_p(M) \cong \prod_{\substack{1 \le i \le n \\ p \approx p_i}} Rv_i/p(Rv_i) \cong \prod_{\substack{1 \le i \le n \\ p \approx p_i}} R/(p),$$

and hence the number of indices i such that p and p_i are associates coincides with the dimension of the $R/(p)$ vector space $\operatorname{tor}_p(M)/p\operatorname{tor}_p(M)$. The same happens with the number of indices j such that p and $\hat{p}_j$ are associates. This proves that the number of direct summands in both decompositions agree.

Now for any $l \in \mathbb{N}$ and $1 \leq i \leq n$ with p and p_i associates we have $p^l v_i = 0$ if and only if $l \geq l_i$, so

$$p^l \operatorname{tor}_p(M) = \bigoplus_{\substack{1\leq i\leq n \\ p\approx p_i \\ l<l_i}} R(p^l v_i) = \bigoplus_{\substack{1\leq j\leq m \\ p\approx p_j \\ l<\hat{l}_j}} R(p^l \hat{v}_j).$$

and hence for any $l \in \mathbb{N}$, the number of indices i such that p and p_i are associates and $l < l_i$ coincides with the number of indices j such that p and $\hat{p}_j$ are associates and $l < \hat{l}_j$. So the number of indices i such that $l_i = 1, 2, \ldots$ coincides with the corresponding number of indices j. □

3.9 Corollary. ***(The fundamental theorem for finitely generated abelian groups)*** *Let A be a finitely generated abelian group. Then:*

(i) *There are unique numbers $r, m \in \mathbb{N} \cup \{0\}$ and $n_1, \ldots, n_r \in \mathbb{N}$, where $n_1 | n_2 | \ldots | n_r$, such that*

$$A \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \times \mathbb{Z}^m.$$

The numbers $n_1, \ldots, n_r$ are called the invariant factors *and m is called the* free rank *of A.*

(ii) *There are numbers $s, m \in \mathbb{N} \cup \{0\}$, prime natural numbers $p_1 \leq \cdots \leq p_s$, natural numbers $r_1, \ldots, r_s$, and for each $i = 1, \ldots, s$ an increasing sequence $n_{i1} \leq \cdots \leq n_{ir_i}$ of natural numbers, all of them uniquely determined by A, such that*

$$A \cong \left(\mathbb{Z}_{p_1^{n_{11}}} \times \cdots \mathbb{Z}_{p_1^{n_{1r_1}}}\right) \times \cdots \times \left(\mathbb{Z}_{p_s^{n_{s1}}} \times \cdots \mathbb{Z}_{p_s^{n_{sr_s}}}\right) \times \mathbb{Z}^m.$$

The numbers $p_i^{n_{ij}}$, $i = 1, \ldots, s$, $j = 1, \ldots, r_i$, are called elementary divisors *of A, and m is the free rank of A.*

3.10 Example. Any abelian group of order 24 is isomorphic to exactly one of the following groups:

- $\mathbb{Z}_{24} \cong \mathbb{Z}_8 \times \mathbb{Z}_3$: $\{\text{invariant factors}\} = \{24\}$, $\{\text{elementary divisors}\} = \{8, 3\}$,
- $\mathbb{Z}_2 \times \mathbb{Z}_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$: $\{\text{invariant factors}\} = \{2, 12\}$, $\{\text{elementary divisors}\} = \{2, 4, 3\}$, or
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$: $\{\text{invariant factors}\} = \{2, 2, 6\}$, $\{\text{elementary divisors}\} = \{2, 2, 2, 3\}$.

Therefore, up to isomorphism, there are exactly three abelian groups of order 24.

Exercises

1. Let $M_1, \ldots, M_n$ be modules over a ring R, and let $N_i \leq M_i$ for $i = 1, \ldots, n$. Show that $N_1 \times \cdots \times N_n$ is a submodule of $M_1 \times \cdots \times M_n$ and that $(M_1 \times \cdots \times M_n)/(N_1 \times \cdots \times N_n)$ is isomorphic to $(M_1/N_1) \times \cdots \times (M_n/N_n)$.

2. Let M be a module over an integral domain R. Check that $\operatorname{tor}(M)$ is indeed a submodule of M.

3. Let M be a module over an integral domain R. Prove that $M/\operatorname{tor}(M)$ is a torsion-free module.

4. A nonzero module over a ring is said to be *indecomposable* if it cannot be expressed as the direct sum of two nonzero submodules.

   (a) Prove that a finitely generated module over a PID R (R not a field) is indecomposable if and only if it is isomorphic either to R or to $R/(p^n)$ for p a prime and $n \in \mathbb{N}$.

   (b) Show that $\mathbb{Q}$ is an indecomposable $\mathbb{Z}$-module, and that it is not finitely generated.

5. A module M over a ring is said to be *irreducible* (or *simple*) if it is nonzero and the only submodules are 0 and M.
   Prove that a module M over a PID R (R not a field) is irreducible if and only if it is isomorphic to $R/(p)$ for a prime p.

6. How many abelian groups are there, up to isomorphism, of order 60?

7. What are the invariant factors and free rank of the abelian group $\{(x, y, z) \in \mathbb{Z}^3 : 2x + 4y + 2z = 0,\ 6x + 4y + 5z = 0\}$?

8. The invariant factors of a finitely generated abelian group are 4, 12 and 60. What are its elementary divisors?

9. The elementary divisors of a finitely generated module over $\mathbb{R}[X]$ are $X - 2$, $(X - 2)^2$, $(X^2 + 1)^2$, $(X^2 + 1)^2$ and $(X^2 + 1)^3$. What are its invariant factors?

10. Let V be a finite dimensional vector space over a field F, and let $\varphi\colon V \to V$ be an endomorphism of V. Prove that V is a module over $F[X]$ with the multiplication by scalars given by:

$$\begin{aligned} &F[X] \times V \longrightarrow V, \\ &(f(X), v) \mapsto f(X).v = a_0 v + a_1 \varphi(v) + \cdots + a_m \varphi^m(v) \\ &\qquad\qquad \big(f(X) = a_0 + a_1 X + \cdots + a_m X^m\big). \end{aligned}$$

For any $0 \neq v \in V$, $\mathrm{ann}(v) = (p(X))$ for a unique monic polynomial, called the *minimal polynomial* of v relative to f.

Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of V over F, and let $A = (a_{ij})$ be the coordinate matrix of f relative to $\mathcal{B}$, so $f(v_j) = \sum_{i=1}^{n} a_{ij} v_i$, $j = 1, \ldots, n$. Consider the homomorphism of $F[X]$-modules $\Phi : F[X]^n \to V$, $(f_1(X), \ldots, f_n(X)) \mapsto f_1(X).v_1 + \cdots + f_n(X).v_n$.

(a) Prove that the kernel K of Φ is generated by the elements

$$\begin{aligned} &(X - a_{11}, -a_{21}, \ldots, -a_{n1}),\\ &(-a_{12}, X - a_{22}, \ldots, -a_{n2}),\\ &\qquad\vdots\\ &(-a_{1n}, -a_{2n} \ldots, X - a_{nn}). \end{aligned}$$

(b) Prove that the invariant factors of the $F[X]$-module V coincide, up to associates, with the invariant factors of the matrix $XI_n - A \in \mathrm{Mat}_n(F[X])$ which are not units.

(c) Let $p_1(X), \ldots, p_r(X)$, with $p_1(X) \mid p_2(X) \mid \ldots \mid p_r(X)$, be the invariant factors of the $F[X]$-module V, normalized so that $p_i(X)$ is monic for any i. Prove that $p_r(X)$ is the minimal polynomial of the endomorphism f. (The monic polynomials $p_1(X), \ldots, p_r(X)$ are called the *invariant factors* of the endomorphism f.)

11. Consider the $\mathbb{Z}$-module $\{f(X) \in \mathbb{Q}[X] : f(n) \in \mathbb{Z}\ \forall n \in \mathbb{Z}\}$. Show that M is a free module (of infinite dimension) over $\mathbb{Z}$ by proving that the set of polynomials

$$\left\{ \binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!} : n \in \mathbb{N} \cup \{0\} \right\}$$

is a basis for M. (As usual $\binom{X}{0} = 1$ by convention.)

Chapter 3

Polynomials

This chapter is devoted to the study of the rings of polynomials, mainly over a field.

§ 1. Irreducibility

Let R be a unital commutative ring, the ring of polynomials

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N},\, a_0, \ldots, a_n \in R\}$$

is a unital commutative ring too. If R is an integral domain then

$$\begin{cases} \forall p(X), q(X) \in R[X] \setminus \{0\}, \deg p(X)q(X) = \deg p(X) + \deg q(X), \\ R[X]^\times = R^\times, \\ R[X] \text{ is an integral domain too.} \end{cases}$$

The ring of polynomials in n indeterminates $R[X_1, \ldots, X_n]$ is defined recursively as follows:

$$R[X_1, \ldots, X_n] = \big(R[X_1, \ldots, X_{n-1}]\big)[X_n].$$

(Polynomials in X_n with coefficients in $R[X_1, \ldots, X_{n-1}]$.)

Thus, a polynomial in $X_1, \ldots, X_n$ with coefficients in R is a finite sum of terms (called *monomials*) of the form

$$aX_1^{d_1}X_2^{d_2}\cdots X_n^{d_n}, \quad a \in R, d_i \in \mathbb{N} \cup \{0\}\ \forall i = 1, \ldots, n,$$

and

$$\begin{cases} d_i \text{ is the degree in } X_i \text{ of the monomial,} \\ d = d_1 + \cdots + d_n \text{ is the degree of the monomial,} \\ (d_1, \ldots, d_n) \in \big(\mathbb{N} \cup \{0\}\big)^n \text{ is the } \textit{multidegree} \text{ of the monomial.} \end{cases}$$

1.1 Theorem. *Let R and A be unital commutative rings, let $\varphi : R \to A$ be a ring homomorphism with $\varphi(1) = 1$, and let $a_1, \ldots, a_n \in A$. Then there is a unique ring homomorphism $\psi : R[X_1, \ldots, X_n] \to A$ such that $\psi|_R = \varphi$ and $\psi(X_i) = a_i$ for any $i = 1, \ldots, n$.*

Proof. It is enough to prove it for $n = 1$. Consider the map

$$\begin{aligned} \psi : R[X] &\longrightarrow A \\ r_0 + r_1 X + \cdots + r_m X^m &\mapsto \varphi(r_0) + \varphi(r_1)a + \cdots + \varphi(r_n)a^n. \end{aligned}$$

ψ is a ring homomorphism and it is the only ring homomorphism $R[X] \to A$ with $\psi|_R = \varphi$ and $\psi(X) = a$. □

1.2 Example. By the Theorem above, there is a unique ring homomorphism $\psi : \mathbb{R}[X] \to \mathbb{C}$ such that $\psi(r) = r$ for any $r \in \mathbb{R}$ (that is $\psi|_{\mathbb{R}}$ is the inclusion of $\mathbb{R}$ into $\mathbb{C}$) and $\psi(X) = i$. Then ψ is onto, and $\ker \psi = (X^2 + 1)$ (check this!). By the First Isomorphism Theorem:

$$\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1).$$

Assume now that R is a unique factorization domain and that Q is its field of fractions. On many occasions, it is better to deal with $Q[X]$, which is a euclidean domain since Q is a field, than with $R[X]$. Besides, if $p(X) \in Q[X]$ and $a \in R$ is a common multiple of the denominators in the coefficients of $p(X)$, then $ap(X) \in R[X]$.

1.3 Definition. Let R be a UFD and let $0 \neq p(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$. The *content* of $p(X)$ is any greatest common divisor of $a_0, a_1, \ldots, a_n$. (Notation: $c(p) = \gcd(a_0, a_1, \ldots, a_n)$.) If $c(p) = 1$, then $p(X)$ is said to be *primitive*.

Notice that there is an abuse in the definition above, and we should talk about the contents of a polynomials, because the greatest common divisor is determined only up to units in R. Any two contents of the same polynomial are associates. This abuse creates no difficulty, as in the next fundamental result.

1.4 Gauss Lemma. *Let R be a UFD, and $0 \neq p(X), q(X) \in R[X]$. Then $c(p \cdot q)$ and $c(p)c(q)$ are associates. In particular, the product of two primitive polynomials is itself primitive.*

Proof. We will start with the last part of the result, so assume that $p(X) = a_0 + a_1 X + \cdots + a_n X^n$ and $q(X) = b_0 + b_1 X + \cdots + b_m X^m$ are primitive polynomials in $R[X]$. If $p(X)q(X)$ were not primitive, then there would exist a $0 \neq d \in R \setminus R^\times$ which divides all the coefficients of $p(X)q(X)$, and since R is a UFD, by taking an irreducible factor of d, we find an irreducible element $x \in R$ which divides all the coefficients of $p(X)q(X)$.

Since $p(X)$ and $q(X)$ are primitive there are integers s and t such that $x \mid a_i$ for $i < s$ but $x \nmid a_s$ and $x \mid b_j$ for $j < t$ but $x \nmid b_t$. Note that since x is irreducible, and hence prime (Chapter 1, 4.16), $x \nmid a_s b_t$. Now, the coefficient of X^{s+t} in $p(X)q(X)$ is

$$\begin{aligned} c_{s+t} =& a_s b_t && \text{(which is not a multiple of } x\text{)} \\ &+ (a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots) && \text{(a multiple of } x \text{ because of the } b_j\text{'s)} \\ &+ (a_{s-1}b_{t+1} + a_{s-2}b_{t+2} + \cdots) && \text{(a multiple of } x \text{ because of the } a_i\text{'s)} \end{aligned}$$

so that $x \nmid c_{s+t}$, a contradiction.

Now, let $0 \neq p(X), q(X) \in R[X]$ be arbitrary nonzero polynomials. Then, by factoring out greatest common divisors of the coefficients, we find two primitive polynomials $\tilde{p}(X)$ and $\tilde{q}(X)$ such that $p(X) = c(p)\tilde{p}(X)$ and $q(X) = c(q)\tilde{q}(X)$. Then $p(X)q(X) = c(p)c(q)\tilde{p}(X)\tilde{q}(X)$. Since $\tilde{p}(X)\tilde{q}(X)$ is primitive, it follows that $c(p)c(q)$ is a content of $p(X)q(X)$ and this completes the proof. □

1.5 Corollary. *Let R be a UFD, Q its field of fractions and let $0 \neq p(X) \in R[X]$ be a polynomial of degree ≥ 1. Then:*

(i) *If $p(X)$ is irreducible in $R[X]$, so it is as a polynomial in $Q[X]$.*

(ii) *If $p(X)$ is primitive, then the converse in* (i) *holds.*

Proof. For (i) assume that $p(X) = a(X)b(X)$, with $0 \neq a(X), b(X) \in Q[X] \setminus Q[X]^\times$ (so that $\deg a(X), \deg b(X) \geq 1$). Then by considering common multiples of the denominators of the coefficients in $a(X)$ and in $b(X)$, we may find an element $0 \neq d \in R$ such that $dp(X) = \tilde{a}(X)\tilde{b}(X)$, with $\tilde{a}(X), \tilde{b}(X) \in R[X]$ and $\deg a(X) = \deg \tilde{a}(X)$, $\deg b(X) = \deg \tilde{b}(X)$. But then $dc(p)$ and $c(\tilde{a})c(\tilde{b})$ are associates, so there is a unit $u \in R^\times$ such that $udc(p) = c(\tilde{a})c(\tilde{b})$. Write $\tilde{a}(X) = c(\tilde{a})\hat{a}(X)$ and $\tilde{b}(X) = c(\tilde{b})\hat{b}(X)$ and $p(X) = c(p)\hat{p}(X)$, for primitive polynomials $\hat{a}(X), \hat{b}(X), \hat{p}(X) \in R[X]$. Multiplying the equation $dp(X) = \tilde{a}(X)\tilde{b}(X)$ by u and simplifying we get $p(X) = \big(uc(p)\hat{a}(X)\big)\hat{b}(X)$, a contradiction with the irreducibility of $p(X)$.

For (ii), assume that the primitive polynomial $p(X)$ is irreducible as a polynomial in $Q[X]$, but that there are nonunit polynomials $a(X), b(X) \in R[X]$ such that $p(X) = a(X)b(X)$. Then, by irreducibility in $Q[X]$, we may assume that $\deg a(X) = 0$, so that $a(X) = d$ for some $0 \neq d \in R \setminus R^\times$. But then d is a common divisor of the coefficients of $p(X)$, a contradiction with $p(X)$ being primitive. □

Notice that $2X \in \mathbb{Z}[X]$ is irreducible as a polynomial in $\mathbb{Q}[X]$, but it is not so in $\mathbb{Z}[X]$.

1.6 Theorem. *Let R be a unital commutative ring. Then*

$$\boxed{R \text{ is a UFD} \Longleftrightarrow R[X] \text{ is a UFD.}}$$

Proof. Assume first that $R[X]$ is a UFD. Then, in particular, $R[X]$ is an integral domain, and so is R. Also, for any $0 \neq r \in R \setminus R^\times = R \setminus R[X]^\times$, r can be factored, uniquely up to associates, into a product of irreducible elements in $R[X]$, so that $r = q_1 \cdots q_n$, where the q_i's are irreducible elements of degree 0 in $R[X]$. But by the same definition of irreducible elements (see Chapter 1, 4.11), the irreducible elements in R are precisely the irreducible elements of degree 0 in $R[X]$. Thus, r factors as a product of irreducible elements in R. The uniqueness follows from the uniqueness in $R[X]$. Hence, R is a UFD too.

Assume now that R is a UFD. For any $0 \neq p(X) \in R[X]$, $p(X) = c(p)\tilde{p}(X)$, for some primitive $\tilde{p}(X) \in R[X]$. Thus, if $p(X)$ is irreducible, either $c(p)$ is a unit (and hence $p(X)$ is primitive), or $\tilde{p}(X)$ is a unit (and hence $p(X)$ is irreducible in R, because its degree is 0). Therefore

$$\begin{aligned}&\{\text{irreducible elements in } R[X]\}\\ &= \{\text{irreducible elements in } R\} \cup \{\text{irreducible primitive elements in } R[X]\}.\end{aligned}$$

Now, let Q be the field of fractions of R. Then $Q[X]$ is a euclidean domain, and hence it is a UFD too. For any $0 \neq p(X) \in R[X]$, $p(X) = q_1(X) \cdots q_n(X)$, where the $q_i(X)$'s are irreducible elements in $Q[X]$. By multiplying by a common factor of the denominators involved, we find a $0 \neq d \in R$ such that $dp(X) = \tilde{q}_1(X) \cdots \tilde{q}_n(X)$, where the $\tilde{q}_i(X)$'s are polynomials in $R[X]$, which are irreducible in $Q[X]$. But $p(X) = c(p)\hat{p}(X)$ and $\tilde{q}_i(X) = c(\tilde{q}_i)\hat{q}_i(X)$ for any i, where $\hat{p}(X)$ and the $\hat{q}_i(X)$'s are primitive, and these latter polynomials are still irreducible in $Q[X]$. As in the previous proof, we conclude that

$$p(X) = a\hat{q}_1(X) \cdots \hat{q}_n(X)$$

in $R[X]$ for some $0 \neq a \in R$. The $\hat{q}_i(X)$'s are primitive and irreducible in $Q[X]$, hence they are irreducible in $R[X]$ by the previous Corollary. Moreover, since R is a UFD, a is either a unit or a product of irreducible elements in R (and hence in $R[X]$). We conclude that $p(X)$ factors into a product of irreducible polynomials in $R[X]$.

It remains to prove the uniqueness, up to associates, of the factorizations into irreducibles. Thus, let $0 \neq p(X) \in R[X] \setminus R^\times$ and assume that

$$p(X) = a_1 \cdots a_n p_1(X) \cdots p_s(X) = b_1 \cdots b_m q_1(X) \cdots q_t(X),$$

where $a_1, \ldots, a_n, b_1, \ldots, b_m$ are irreducible elements in R and $p_1(X), \ldots, p_s(X), q_1(X), \ldots, q_t(X)$ are primitive irreducible elements in $R[X]$. By Gauss Lemma, $a_1 \cdots a_n$ and $b_1 \cdots b_m$ are contents of $p(X)$, so they are associates. Since R is a UFD, it follows that $n = m$ and, after reordering, we may assume that a_i and b_i are associates for any i. Simplifying, we get a unit $u \in R^\times$ such that $p_1(X) \cdots p_s(X) = uq_1(X) \cdots q_t(X)$. But $Q[X]$ is a UFD too, so

that $s = t$ and, after reordering, we may assume that $p_i(X)$ and $q_i(X)$ are associates in $Q[X]$ for any i. This implies that there are nonzero elements $c_i, d_i \in R$ such that $p_i(X) = \frac{c_i}{d_i} q_i(X)$ for any i, so that $d_i p_i(X) = c_i q_i(X)$ in $R[X]$. Since $p_i(X)$ and $q_i(X)$ are primitive, both c_i and d_i are contents of $d_i p_i(X) = c_i q_i(X)$, so that c_i and d_i are associates in R and hence there is a unit $u_i \in R^\times$ such that $c_i = u_i d_i$. Thus $\frac{c_i}{d_i} = u_i \in R^\times$, and $p_i(X) = u_i q_i(X)$, so $p_i(X)$ and $q_i(X)$ are associates in $R[X]$. □

In particular, $\mathbb{Z}[X]$ is a UFD, but we already know that it is not a PID (see Chapter 1, 2.11).

1.7 Corollary. *If R is a UFD, so is $R[X_1, \ldots, X_n]$ for any $n \in \mathbb{N}$.*

We finish this section with a useful criterion for irreducibility.

1.8 Theorem. ***(Eisenstein's criterion)*** *Let R be an integral domain, $p(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in R[X]$, with $n \geq 1$, and let $P \trianglelefteq_{prime} R$ such that:*

$$\text{(i) } a_0, a_1, \ldots, a_{n-1} \in P, \quad \text{(ii) } a_0 \notin P^2.$$

Then $p(X)$ is irreducible in $R[X]$.

Proof. Assume that $p(X) = f(X)g(X)$, with $f(X), g(X) \in R[X] \backslash R^\times$. Since $p(X)$ is monic, $\deg f(X) = m \geq 1$, $\deg g(X) = m' \geq 1$, $m + m' = n$. Let $f(X) = \sum_{i=0}^{m} c_i X^i$ and $g(X) = \sum_{i=0}^{m'} d_i X^i$. Consider the ring epimorphism ('reduction modulo P'):

$$\psi : R[X] \longrightarrow (R/P)[X]$$
$$q(X) = \sum_{i=0}^{m} b_i X^i \mapsto \bar{q}(X) = \sum_{i=0}^{m} (b_i + P) X^i.$$

(ψ is induced by the composition $R \to R/P \hookrightarrow (R/P)[X]$ by means of 1.1.) Notice that R/P is an integral domain. Now $\bar{p}(X) = \bar{f}(X)\bar{g}(X)$. But (i) implies that $\bar{p}(X) = X^n$, so that $\bar{f}(X) = (c_m + P)X^m$ and $\bar{g}(X) = (d_{m'} + P)X^{m'}$. Hence $c_0 + P = d_0 + P = 0$ because $n \geq 1$. Thus $c_0, d_0 \in P$ and $a_0 = c_0 d_0 \in P^2$, a contradiction. □

1.9 Corollary. ***(Eisenstein's criterion for $\mathbb{Z}[X]$)*** *Let $f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in \mathbb{Z}[X]$ and let p be a prime number such that $p \,|\, a_0, \ldots, a_{n-1}$ and $p^2 \nmid a_0$. Then $f(X)$ is irreducible.*

1.10 Examples.

- $X^4 + 10X + 5$ is irreducible in $\mathbb{Z}[X]$ by Eisenstein's Criterion with $p = 5$.

- For any prime p and any $n \geq 1$, $X^n - p \in \mathbb{Z}[X]$ is irreducible.
- Let p be a prime number and let $f(X) = 1 + X + \cdots + X^{p-1} \in \mathbb{Z}[X]$. As an element in $\mathbb{Q}(X)$, $f(X) = \dfrac{X^p - 1}{X - 1}$, so that

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + pX^{p-2} + \binom{p}{2} X^{p-3} + \cdots + \binom{p}{p-1},$$

Since $p, \binom{p}{2}, \ldots, \binom{p}{p-1}$ are all multiples of p, while $\binom{p}{p-1} = p$ is not a multiple of p^2, we conclude that $f(X+1)$ is irreducible in $\mathbb{Z}[X]$ by Eisenstein's Criterion. But the ring homomorphism $\psi : \mathbb{Z}[X] \to \mathbb{Z}[X]$ which is the identity on $\mathbb{Z}$ and maps X to $X - 1$ is an isomorphism (the inverse is the identity on $\mathbb{Z}$ and maps X to $X+1$). Hence $f(X) = \psi\big(f(X+1)\big)$, so $f(X)$ is irreducible too. (The image of an irreducible element under an isomorphism is irreducible too.)

The last example shows how Eisenstein's Criterion can be used sometimes in situations where it does not apply directly.

§ 2. Roots

This section will deal with basic facts on roots of polynomials, which are extensions to a more general setting of well-known facts about roots of real or complex polynomials.

2.1 Definition. Let $R \leq D$ be two integral domains, $p(X) \in R[X]$ and $c \in D$. Then c is said to be a *root* of $p(X)$ if $p(c) = 0$.

Notice that $p(c)$ is the image of $p(X)$ under the unique (evaluation) homomorphism $\psi_c : R[X] \to D$, such that $\psi_c|_R$ is the inclusion of R into D and $\psi_c(X) = c$.

2.2 Theorem. *Let R be an integral domain, $p(X) \in R[X]$ and $a \in R$. Then a is a root of $p(X)$ if and only if $X - a \,|\, p(X)$ in $R[X]$.*

Proof. Let Q be the field of fractions of R. Since $Q[X]$ is a euclidean domain with the degree as norm, we may divide in $Q[X]$ to get $p(X) = q(X)(X-a) + r$, where $q(X) \in Q[X]$ and $r \in Q$ (since its degree is 0). But $p(X), X - a \in R[X]$ and $X - a$ is monic, so the quotient and remainder obtained by means of the division algorithm are in $R[X]$ too. Thus $q(X) \in R[X]$ and $r \in R$. Now, since $p(a) = q(a)(a - a) + r = r$, $p(a) = 0$ if and only if $r = 0$ if and only if $X - a \,|\, p(X)$. □

2.3 Corollary. *Let F be a field and let $0 \neq p(X) \in F[X]$. Then:*

(i) *$p(X)$ has a factor of degree 1 in $F[X]$ if and only if it has a root in F.*

(ii) *If* $\deg p(X) = 2$ *or* 3*, then* $p(X)$ *is reducible in* $F[X]$ *if and only if it has a root in* F*.*

2.4 Proposition. *Let* R *be a UFD,* $p(X) = a_0 + a_1X + \cdots + a_nX^n \in R[X]$*,* Q *the field of fractions of* R *and* $\frac{r}{s} \in Q$ *with* $r, s \in R$ *such that* $\gcd(r, s) = 1$*. Then, if* $\frac{r}{s}$ *is a root of* $p(X)$*,* $r \,|\, a_0$ *and* $s \,|\, a_n$*.*

Proof. If $0 = p\left(\frac{r}{s}\right) = a_0 + a_1\frac{r}{s} + \cdots + a_n\frac{r^n}{s^n} = \frac{1}{s^n}\left(a_0s^n + a_1rs^{n-1} + \cdots + a_nr^n\right)$, then $a_0s^n + a_1rs^{n-1} + \cdots + a_nr^n = 0$, but all the summands except perhaps the last one are multiples of s, so that $s \mid a_nr^n$. Since R is a UFD and $\gcd(r, s) = 1$, we conclude that $s \,|\, a_n$. Similarly, $r \,|\, a_0$. □

2.5 Definition. Let $R \leq D$ be two integral domains, $p(X) \in R[X]$ and $c \in D$. Then c is said to be a root of $p(X)$ with *multiplicity* $m\,(\in \mathbb{N})$ if $p(X)$ is a multiple of $(X - c)^m$ but not of $(X - c)^{m+1}$ in $D[X]$. If $m = 1$ (respectively $m = 2$, $m = 3$), c is said to be a *simple* (respectively *double*, *triple*) root.

2.6 Theorem. *Let* R *be an integral domain,* $0 \neq p(X) \in R[X]$*,* $n \in \mathbb{N}$*,* $c_i \in R$ *a root of* $p(X)$ *of multiplicity* m_i*,* $i = 1, \ldots, n$*, with* $c_i \neq c_j$ *for* $i \neq j$*. Then there exists a* $q(X) \in R[X]$ *such that* $q(c_i) \neq 0$ *for any* $i = 1, \ldots, n$ *and* $p(X) = (X - c_1)^{m_1} \cdots (X - c_n)^{m_n}q(X)$*.*

In particular, the number of roots of $p(X)$*, counted according to their multiplicities, does not exceed the degree of* $p(X)$*.*

Proof. Let Q be the field of fractions of R. Then $X - c_i$ is irreducible in $Q[X]$ for any i and the $(X - c_i)$'s are not associates pairwise. Our hypotheses imply that $(X - c_i)^{m_i} \mid p(X)$ in $R[X]$, so in $Q[X]$ too. But $Q[X]$ is a euclidean domain, and hence a UFD too. Therefore, there exists a $q(X) \in Q[X]$ such that $p(X) = (X - c_1)^{m_1} \cdots (X - c_n)^{m_n}q(X)$ in $Q[X]$. Since $(X - c_1)^{m_1} \cdots (X - c_n)^{m_n}$ is monic, the quotient $q(X)$, obtained through the division algorithm, belongs to $R[X]$. Moreover, for any i, $q(c_i) \neq 0$ because, otherwise, $X - c_i$ would divide $q(X)$ and hence $(X - c_i)^{m_i+1}$ would divide $p(X)$, a contradiction. □

2.7 Corollary. *Let* R *be an integral domain and let* $p(X), q(X) \in R[X]$ *polynomials of degree* $\leq n \in \mathbb{N}$*. If there are different elements* $c_1, \ldots, c_{n+1} \in R$ *such that* $p(c_i) = q(c_i)$ *for any* $i = 1, \ldots, n + 1$*, then* $p(X) = q(X)$*.*

We will consider now polynomials over a field. Our purpose is to show that given any polynomial, there is a larger field which contains all its roots.

2.8 Definition. Let F and K be fields such that F is a subring of K. Then K is said to be a *field extension* of F and F is said to be a *subfield* of K. (Notation: K/F.)

More generally, we say that K/F is a field extension if there is a ring monomorphism $\iota : F \hookrightarrow K$. In this case, we can identify F with its image under ι, which is indeed a subfield of K.

If K/F is a field extension and $\alpha \in K$, the smallest subfield of K containing F and α will be denoted by $F(\alpha)$. It is clear that

$$F(\alpha) = \{p(\alpha)q(\alpha)^{-1} : p(X), q(X) \in F[X] \text{ and } q(\alpha) \neq 0\}$$

because this is a subfield of K containing F and α, and any other subfield containing F and α must contain all the elements $p(\alpha)q(\alpha)^{-1}$ above. In the same vein, for any $\alpha_1, \ldots, \alpha_n \in K$, the smallest subfield of K containing F and the α_i's $(i = 1, \ldots, n)$ is

$$\begin{aligned} (2.9)\quad & F(\alpha_1, \ldots, \alpha_n) = \{p(\alpha_1, \ldots, \alpha_n)q(\alpha_1, \ldots, \alpha_n)^{-1} : \\ & p(X_1, \ldots, X_n), q(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n] \text{ and } q(\alpha_1, \ldots, \alpha_n) \neq 0\}. \end{aligned}$$

2.10 Theorem. *Let F be a field and $0 \neq p(X) \in F[X]$ an irreducible polynomial. Then:*

(i) *$F[X]/\big(p(X)\big)$ is a field extension of F and it contains at least a root of $p(X)$.*

(ii) *If K/F is a field extension and $\alpha \in K$ is a root of $p(X)$, then there is an isomorphism of fields: $\psi : F[X]/\big(p(X)\big) \longrightarrow F(\alpha)\,(\leq K)$ such that $\psi\Big(a + \big(p(X)\big)\Big) = a$ for any $a \in F$ and $\psi\Big(X + \big(p(X)\big)\Big) = \alpha$.*

Proof. For (i), since $F[X]$ is a euclidean domain (so a PID) and $p(X)$ is irreducible, it is prime and hence $\big(p(X)\big) \trianglelefteq_{\text{prime}} F[X]$, but since $p(X) \neq 0$ and $F[X]$ is a PID, $\big(p(X)\big) \trianglelefteq_{\max} F[X]$ and, thus, $F[X]/\big(p(X)\big)$ is a field. Moreover F embeds into $F[X]/\big(p(X)\big)$ by means of $a \mapsto a + \big(p(X)\big)$, which is a monomorphism. Finally, let $\alpha = X + \big(p(X)\big)$, then trivially (!!)

$$p(\alpha) = p(X) + \big(p(X)\big) = 0,$$

and α is a root of $p(X)$ in $K = F[X]/\big(p(X)\big)$.

As for (ii), we already know that there is a unique ring homomorphism $\psi_\alpha : F[X] \to K$ such that its restriction to F is the inclusion of F into K and $\psi_\alpha(X) = \alpha$. Then $p(X) \in \ker \psi_\alpha \subsetneq F[X]$, so that $\big(p(X)\big) \subseteq \ker \psi_\alpha$ and they are equal because $\big(p(X)\big)$ is a maximal ideal. On the other hand, $\operatorname{im} \psi_\alpha$ is a subfield of K (isomorphic to $F[X]/\big(p(X)\big)$ by the First Isomorphism Theorem), contained in $F(\alpha)$ and containing α. Since $F(\alpha)$ is the smallest such subfield, it follows that $\operatorname{im} \psi_\alpha = F(\alpha)$. □

2.11 Remark. It has been proven that any irreducible polynomial in $F[X]$ has some root in some extension of F. As any nonconstant polynomial is a

product of irreducible ones, it turns out that any polynomial of degree ≥ 1 has some root in some extension of F.

There is a particular noteworthy example of such an extension to keep in mind: $\mathbb{R} \hookrightarrow \mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$.

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

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

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

2.13 Example. $\mathbb{C}$ is a splitting field of $X^2+1 \in \mathbb{R}[X]$.

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

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

Proof. It is enough to concatenate the following isomorphisms:

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

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

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

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

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

Now, if $\deg p(X) = n > 1$, we know by Theorem 2.10 above that there exists a field extension of F which contains a root α_1 of some irreducible factor of $p(X)$. Let $K_1 = F(\alpha_1)$. Then, in $K_1[X]$, $p(X) = (X-\alpha_1)q(X)$,

and $\deg q(X) = n-1$. By induction hypothesis, there exists a splitting field E of $q(X)$ over K_1. Hence, in $E[X]$, $q(X) = a(X-\alpha_2)\cdots(X-\alpha_n)$ for some $\alpha_2,\ldots,\alpha_n \in E$ and $E = K_1(\alpha_2,\ldots,\alpha_n)$. But then, in $E[X]$, $p(X) = (X-\alpha_1)q(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ and $E = K_1(\alpha_2,\ldots,\alpha_n) = F(\alpha_1,\ldots,\alpha_n)$; so that E is a splitting field of $p(X)$ over F.

Induction on $n = \deg p(X)$ will be used too for (ii). Again, if $n \leq 1$, then $E = F$ and $\hat{E} = \hat{F}$ because the roots (if any) of $p(X)$ (respectively $\hat{p}(X)$) are in F (respectively in $\hat{F}$). Hence $\sigma = \varphi$. Now, if $n > 1$, let $p_1(X)$ be an irreducible factor of $p(X)$ and $\hat{p}_1(X)$ the corresponding irreducible factor of $\hat{p}(X)$. Let $\alpha \in E$ be a root of $p_1(X)$ and $\beta \in \hat{E}$ a root of $\hat{p}_1(X)$. Thus $F \leq F(\alpha) \leq E$ and $\hat{F} \leq \hat{F}(\beta) \leq \hat{E}$ and, by the previous Lemma, there exists $\sigma_1 : F(\alpha) \to \hat{F}(\beta)$, a field isomorphism, extending φ and such that $\sigma_1(\alpha) = \beta$.

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

2.16 Definition. Let F be a field and let $p(X) = a_0 + a_1X + \ldots + a_nX^n \in F[X]$. The *derivative* of $p(X)$ is the polynomial $p'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}$.

The usual rules of differentiation are easily checked:

2.17 Properties. *Let F be a field and let $p(X), q(X) \in F[X]$. Then*

- $\big(p(X)+q(X)\big)' = p'(X) + q'(X)$,
- $\big(p(X)q(X)\big)' = p'(X)q(X) + p(X)q'(X)$.

2.18 Theorem. *Let F be a field, $0 \neq p(X) \in F[X]$, and E a splitting field of $p(X)$ over F. Then $p(x)$ has no multiple roots in E if and only if $\gcd\big(p(X), p'(X)\big) = 1$.*

Proof. First notice that $\gcd\big(p(X), p'(X)\big)$ is computed by means of the Euclidean Algorithm, and therefore the same value is obtained over F or over E. We will work over E. Let $\alpha \in E$ be a root of $p(X)$ of multiplicity m. Hence, in $E[X]$, $p(X) = (X-\alpha)^m q(X)$, with $q(\alpha) \neq 0$. Thus, $p'(X) = m(X-\alpha)^{m-1}q(X) + (X-\alpha)^m q'(X)$, so $p'(\alpha) = 0$ if and only if

$m \geq 2$. Therefore, $\gcd\big(p(X), p'(X)\big) \neq 1$ if and only if there is an irreducible factor of $p(X)$ dividing $p'(X)$, if and only if (since E is a splitting field) there is a common root $\alpha \in E$ of $p(X)$ and $p'(X)$, if and only if there is a root $\alpha \in E$ of $p(X)$ of multiplicity ≥ 2. □

We cannot finish this section devoted to the roots of polynomials without mentioning Vieta's formulae.

2.19 Vieta's formulae. Let F be a field, $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$ a monic polynomial and let E be a splitting field of $p(X)$ over F. Then in $E[X]$, $p(X) = (X - \alpha_1)\cdots(X - \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. Hence,

$$\begin{cases} a_{n-1} = -(\alpha_1 + \cdots + \alpha_n), \\ a_{n-2} = \displaystyle\sum_{1 \leq i_1 < i_2 \leq n} \alpha_{i_1}\alpha_{i_2}, \\ a_{n-3} = -\displaystyle\sum_{1 \leq i_1 < i_2 < i_3 \leq n} \alpha_{i_1}\alpha_{i_2}\alpha_{i_3}, \\ \quad \vdots \qquad \vdots \\ a_0 = (-1)^n \alpha_1\alpha_2\cdots\alpha_n \end{cases} \qquad \textbf{(Vieta's formulae)}$$

2.20 Example. Consider the field $F = \mathbb{Z}/p\mathbb{Z}$ of p elements (for a prime p), and let $f(X) = X^{p-1} - 1$. By Fermat's Little Theorem $1, 2, \ldots, p-1$ are roots of $f(X)$ in F, so that $f(X) = (X-1)(X-2)\cdots(X-(p-1))$. Then, by Vieta's formulae $-1 = a_0 = (-1)^{p-1}1 \cdot 2 \cdot \cdots \cdot (p-1)$ in F, that is

$$(p-1)! \equiv -1 \pmod{p} \qquad \textbf{(Wilson's Theorem)}$$

Moreover, if $n > 1$ is not prime and q is a prime dividing n, then $q \mid (n-1)!$, so $q \nmid (n-1)! + 1$ and $(n-1)! \not\equiv -1 \pmod{n}$. Therefore for $n \in \mathbb{N}$, $n > 1$,

$$\boxed{n \text{ is prime} \iff (n-1)! \equiv -1 \pmod{n}}$$

and this gives a criterion to know if a number is prime, without looking at its divisors! The only problem is that for large n, $(n-1)!$ is huge, so this is not an efficient method.

§ 3. Resultant and discriminant

3.1 Definition. Let F be a field, $f(X) = a_0 + a_1X + \cdots + a_nX^n, g(X) = b_0 + b_1X + \cdots + b_mX^m \in F[X]$ with $n, m \geq 1$ (although we admit that a_n or b_m may be 0). Then the *resultant* of $f(X)$ and $g(X)$ is the determinant:

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

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{n+m \text{ columns}}$$

The matrix whose determinant is computed above is called the *Sylvester matrix* of the polynomials $f(X)$ and $g(X)$. Moreover, if $\deg f(X) = n$ and $\deg g(X) = m$ (that is, if $a_n \neq 0 \neq b_m$), then we write simply $\mathrm{Res}(f,g)$.

3.2 Properties. *Let F, $f(X)$ and $g(X)$ be as above. Then:*

1. $\mathrm{Res}_{n,m}(f,g) = 0$ *if and only if either $a_n = b_m = 0$, or $f(X)$ and $g(X)$ have a common root in a field extension of F. (This latter condition is equivalent to the condition* $\gcd(f,g) \neq 1$*.)*

Proof. If any of $f(X)$ and $g(X)$ is 0 the result is trivial, so we will assume that $f(X) \neq 0 \neq g(X)$. Now, $\mathrm{Res}_{n,m}(f,g) = 0$ if and only if the homogeneous system of linear equations (transpose matrix)

$$\begin{pmatrix} a_n & 0 & \dots & 0 & 0 & b_m & 0 & \dots & 0 & 0 \\ a_{n-1} & a_n & \ddots & \vdots & \vdots & b_{m-1} & b_m & \ddots & \vdots & \vdots \\ a_{n-2} & a_{n-1} & \ddots & 0 & \vdots & b_{m-2} & b_{m-1} & \ddots & 0 & \vdots \\ \vdots & \vdots & \dots & a_n & 0 & \vdots & \vdots & \dots & b_n & 0 \\ \vdots & \vdots & \dots & \vdots & a_n & \vdots & \vdots & \dots & \vdots & b_m \\ a_0 & \vdots & \dots & \vdots & \vdots & b_0 & \vdots & \dots & \vdots & \vdots \\ 0 & a_0 & \dots & \vdots & \vdots & 0 & b_0 & \dots & \vdots & \vdots \\ \vdots & 0 & \ddots & a_1 & a_2 & \vdots & 0 & \ddots & b_1 & b_2 \\ \vdots & \vdots & \ddots & a_0 & a_1 & \vdots & \vdots & \ddots & b_0 & b_1 \\ 0 & 0 & \dots & 0 & a_0 & 0 & 0 & \dots & 0 & b_0 \end{pmatrix} \begin{pmatrix} x_{m-1} \\ x_{m-2} \\ \vdots \\ x_1 \\ x_0 \\ y_{n-1} \\ y_{n-2} \\ \vdots \\ y_1 \\ y_0 \end{pmatrix} = 0$$

has a nontrivial solution. But this last condition is equivalent to the existence of polynomials $g_1(X) = x_0 + x_1X + \cdots + x_{m-1}X^{m-1}$ and $f_1(X) = y_0 + y_1X + \cdots + y_{n-1}X^{n-1}$ in $F[X]$, with at least one of them nonzero, such that

$$f(X)g_1(X) + g(X)f_1(X) = 0.$$

Thus, we have to prove that there are polynomials $f_1(X)$ and $g_1(X)$ satisfying the conditions above if and only if either $a_n = b_m = 0$, or $f(X)$ and $g(X)$ have a common root in a field extension of F:

$\Leftarrow\big)$ If $a_n = b_m = 0$ then we may take $f_1(X) = -f(X)$ (of degree $\leq n-1$) and $g_1(X) = g(X)$ (of degree $\leq m-1$). While if $f(X)$ and $g(X)$ have a common root in some field extension, then $\gcd\big(f(X), g(X)\big) \neq 1$. In this case, if $d(X) = \gcd\big(f(X), g(X)\big)$, then $f(X) = d(X)\hat{f}(X)$ and $g(X) = d(X)\hat{g}(X)$, with $\deg \hat{f}(X) \leq n-1$ and $\deg \hat{g}(X) \leq m-1$. Then with $f_1(X) = -\hat{f}(X)$ and $g_1(X) = \hat{g}(X)$, $f(X)g_1(X) + g(X)f_1(X) = d(X)\hat{f}(X)\hat{g}(X) - d(X)\hat{g}(X)\hat{f}(X) = 0$.

$\Rightarrow\big)$ If $f(X)g_1(X) + g(X)f_1(X) = 0$ with $f_1(X)$ and $g_1(X)$ not simultaneously 0 and of degrees $\leq n-1$ and $\leq m-1$ respectively, then if $\gcd\big(f(X), g(X)\big) = 1$, it follows that $f(X) \mid f_1(X)$ and $g(X) \mid g_1(X)$, and this is only possible if $a_n = b_m = 0$. On the other hand, if $\gcd\big(f(X), g(X)\big) = d(X)$, with $\deg d(X) \geq 1$, then any root of $d(X)$ in a field extension of F is a common root of $f(X)$ and $g(X)$. □

2. *If $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ in some field extension of F, then*

$$\mathrm{Res}_{n,m}(f,g) = a^m \prod_{i=1}^{n} g(\alpha_i).$$

Besides, if $g(X) = b(X-\beta_1)\cdots(X-\beta_m)$ in some field extension, then also

$$\mathrm{Res}_{n,m}(f,g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Proof. If $\deg g(X) = 0$ (so $b_1 = \cdots = b_m = 0$) the result is clear because the Sylvester matrix is triangular: $\mathrm{Res}_{n,m}(f,g) = a^m b_0^n = a^m \prod_{i=1}^{m} g(\alpha_i)$. Also, if $a = 0$ the result is trivial ($0 = 0$).

Therefore, we assume $a \neq 0$ and $\deg g(X) \geq 1$. Let $K = F(X_1, \ldots, X_n, Y)$ be the field of fractions of the polynomial ring $F[X_1, \ldots, X_n, Y]$ and consider the polynomials (the trick consists of substituting the roots of $f(X)$ by new variables):

$$\left.\begin{aligned} \hat{f}(X) &= a(X-X_1)\cdots(X-X_n) \\ \hat{g}(X) &= g(X) - Y \end{aligned}\right\} \in K[X]$$

That is, we substitute the roots of $f(X)$ by variables, in order to avoid problems that may arise if some of the roots are equal, and we slightly change $g(X)$. By computing the determinant of the Sylvester matrix of $\hat{f}(X)$ and $\hat{g}(X)$, we check that $\mathrm{Res}_{n,m}(\hat{f},\hat{g}) \in F[X_1, \ldots, X_n, Y]$, so we may write $\mathrm{Res}_{n,m}(\hat{f},\hat{g}) = r(X_1, \ldots, X_n, Y) \in F[X_1, \ldots, X_n, Y]$.

Note that $\mathrm{Res}_{n,m}(f,g) = r(\alpha_1,\ldots,\alpha_n,0)$, since $f(X)$ is obtained from $\hat{f}(X)$ by substituting the X_i's by the α_i's. Also, by the well-known properties of the determinants, it is clear that $r(X_1,\ldots,X_n,Y)$ is a polynomial of degree n in Y, leading coefficient $(-1)^n a^m$ and constant term (obtained by substituting Y by 0) $\mathrm{Res}_{n,m}(\hat{f},g)$.

By property **1**, $\mathrm{Res}_{n,m}\big(\hat{f}, g-g(X_i)\big) = 0$, because X_i is a common root of $\hat{f}(X)$ and of $g(X)-g(X_i)$. Therefore, $Y-g(X_i)\,|\,r(X_1,\ldots,X_n,Y)$. But, since $g(X_i)\neq g(X_j)$ for any $i\neq j$ because $\deg g(X)\geq 1$, we get

$$r(X_1,\ldots,X_n,Y) = (-1)^n a^m \prod_{i=1}^{n}\big(Y-g(X_i)\big)$$

since both are polynomials in Y of the same degree, same leading coefficient and same roots. Hence,

$$\mathrm{Res}_{n,m}(f,g) = r(\alpha_1,\ldots,\alpha_n,0) = a^m\prod_{i=1}^{n} g(\alpha_i),$$

as desired. The last part is a direct consequence of this. □

3. *If $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ in some field extension of F and $n\geq 2$, then*

$$\mathrm{Res}_{n,n-1}(f,f') = (-1)^{\binom{n}{2}} a^{2n-1} V(\alpha_1,\ldots,\alpha_n)^2,$$

where

$$V(\alpha_1,\ldots,\alpha_n) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} \Big(= \prod_{1\leq i<j\leq n}(\alpha_j-\alpha_i)\Big)$$

is the Vandermonde determinant (see Exercise 14).

Proof. $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$, so $f'(X) = a\sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$ and, hence, $f'(\alpha_i) = a\prod_{j\neq i}(\alpha_i-\alpha_j)$. Hence property **2** implies that

$$\begin{aligned}
\mathrm{Res}_{n,n-1}(f,f') &= a^{n-1}\prod_{i=1}^{n} f'(\alpha_i) \\
&= a^{2n-1}\prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i-\alpha_j) \\
&= (-1)^{\binom{n}{2}} a^{2n-1}\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2 \\
&= (-1)^{\binom{n}{2}} a^{2n-1} V(\alpha_1,\ldots,\alpha_n)^2.
\end{aligned}$$

□

3.3 Definition. Let F be a field and $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ a polynomial of degree $n \geq 2$ ($a_n \neq 0$). The *discriminant* of $f(X)$ is the scalar (in F) $\mathrm{D}(f) = (-1)^{\binom{n}{2}} a_n^{-1} \operatorname{Res}_{n,n-1}(f, f')$.

By property **3** of the resultants, if $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ ($a \neq 0$) in some field extension of F, then $\mathrm{D}(f) = a^{2n-2}V(\alpha_1, \ldots, \alpha_n)^2$. Note that $V(\alpha_1, \ldots, \alpha_n)$ may not belong to F, but $V(\alpha_1, \ldots, \alpha_n)^2 = \frac{\mathrm{D}(f)}{a^{2n-2}}$ does belong to F.

3.4 Corollary. *Let F be a field and $f(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$ a polynomial of degree $n \geq 2$. Then $\mathrm{D}(f) = 0$ if and only if f has a multiple root in some field extension of F.*

3.5 Example. Let $f(X) = aX^2 + bX + c$, $a \neq 0$. Then

$$\mathrm{D}(f) = -a^{-1} \operatorname{Res}_{2,1}(f, f') = -a^{-1} \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}$$

$$= -a^{-1} \begin{vmatrix} a & b & c \\ 0 & -b & -2c \\ 0 & 2a & b \end{vmatrix} = b^2 - 4ac.$$

§ 4. The Fundamental Theorem of Algebra

This section is devoted to prove the famous:

4.1 The Fundamental Theorem of Algebra. $\mathbb{C}$ *contains the roots of any complex polynomial.*

Actually, this result has little to do with Algebra, and nowadays it is not so fundamental, but it has been very important in the historical development of Mathematics. Many proofs have been given and from time to time new proofs appear. The first widely accepted proof is attributed to Gauss in his Ph.D. thesis in 1799. Later on he gave many different proofs. For a recent proof mainly based on Linear Algebra, you may consult in the library an article by Harm Derksen: 'The Fundamental Theorem of Algebra and Linear Algebra', American Mathematical Monthly **110** (2003), 620–623. The proof below is essentially due to Argand (in 1814), based on a previous (and flawed) proof by d'Alembert (in 1746).

Proof. It is enough to prove that any $f(X) \in \mathbb{C}[X]$ with $\deg f(X) \geq 1$ has a root in $\mathbb{C}$, because then we may proceed by induction on $\deg f(X)$: if $\alpha \in \mathbb{C}$ is a root, then $f(X) = (X - \alpha)g(X)$ and we may proceed with $g(X)$.

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{C}[X]$, $a_n \neq 0$, $n \geq 1$, and consider the corresponding function $f : \mathbb{C} \to \mathbb{C}$, $z \mapsto f(z)$. For $0 \neq z \in \mathbb{C}$ we may write

$$f(z) = a_n z^n \left(1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right).$$

Now, the quantity inside the parenthesis tends to 1 as $|z| \to \infty$, while $\lim_{|z|\to\infty} |a_n z^n| = \infty$. Thus, if $C = |a_0| = |f(0)|$, then there is a real number $R > 0$ such that $|f(z)| > C$ for any $z \in \mathbb{C}$ with $|z| > R$.

But $\bar{B}(0, R) = \{z \in \mathbb{C} : |z| \leq R\}$ is closed and bounded, and the function given by $|f(z)|$ is continuous, so it has an absolute minimum in $\bar{B}(0, R)$. Let $z_0 \in \bar{B}(0, R)$ be a point at which this minimum is attained. Hence $|f(z_0)| \leq |f(0)| = C$ and, therefore, $|f(z_0)| \leq |f(z)|$ for any $z \in \mathbb{C}$. That is, z_0 is an absolute minimum of $|f(z)|$. Therefore, we have to check that $f(z_0) = 0$. Assume, on the contrary, that $f(z_0) \neq 0$. We will arrive to a contradiction by finding an element $z_1 \in \mathbb{C}$ with $|f(z_1)| < |f(z_0)|$.

We may express $f(X)$ as

$$f(X) = c_0 + c_1(X - z_0) + \cdots + c_n(X - z_0)^n,$$

with $c_0 = f(z_0) \neq 0$, let $T = X - z_0$ and let $m \geq 1$ be such that $c_1 = \cdots = c_{m-1} = 0$ but $c_m \neq 0$ (such m exists since $\deg f(X) \geq 1$). Thus $f(X) = c_0 + c_m T^m + T^{m+1} g(T)$, with $g(T) \in \mathbb{C}[T]$. Take $\alpha \in \mathbb{C}$ such that $\alpha^m = -\frac{c_0}{c_m}$ and let $\beta = \lambda\alpha$ with $\lambda \in \mathbb{R}$ and $0 \leq \lambda \leq 1$. Then

$$\begin{aligned} f(z_0 + \beta) &= c_0 + c_m\beta^m + \beta^{m+1} g(\beta) \\ &= c_0 + \lambda^m c_m \alpha^m + \lambda^{m+1}\alpha^{m+1} g(\lambda\alpha) \\ &= c_0 \left(1 - \lambda^m + \lambda^{m+1} c_0^{-1} \alpha^{m+1} g(\lambda\alpha)\right), \end{aligned}$$

and hence

$$|f(z_0 + \lambda\alpha)| \leq |c_0| \left(1 - \lambda^m + \lambda^m |\lambda c_0^{-1} \alpha^{m+1} g(\lambda\alpha)|\right).$$

But $\lim_{\lambda\to 0} |\lambda c_0^{-1} \alpha^{m+1} g(\lambda\alpha)| = 0$, so there exists $0 < \delta < 1$ such that $|\lambda c_0^{-1} \alpha^{m+1} g(\lambda\alpha)| < \frac{1}{2}$ for any $0 < \lambda < \delta$. Therefore, for $0 < \lambda < \delta$, we get

$$|f(z_0 + \lambda\alpha)| \leq |c_0| \left(1 - \lambda^m + \frac{1}{2}\lambda^m\right) = |c_0| \left(1 - \frac{1}{2}\lambda^m\right) < |c_0|,$$

a contradiction. □

4.2 Corollary. *The monic irreducible polynomials in $\mathbb{R}[X]$ are exactly the polynomials $X - a$, $a \in \mathbb{R}$ and $X^2 + bX + c$, $b, c \in \mathbb{R}$ with $b^2 - 4c < 0$.*

Proof. Assume that $p(X) \in \mathbb{R}[X]$ is monic and irreducible. Let $\alpha \in \mathbb{C}$ be a root of $p(X)$.

- If $\alpha = a \in \mathbb{R}$, then $X - a \,|\, p(X)$ and by irreducibility, $p(X) = X - a$.
- Otherwise, $\alpha \in \mathbb{C} \setminus \mathbb{R}$, but then $\bar{\alpha}$ is another root of $p(X)$, since $p(\bar{\alpha}) = \overline{p(\alpha)} = 0$. Let $b = -(\alpha + \bar{\alpha})$ and $c = \alpha\bar{\alpha}$. Then $b, c \in \mathbb{R}$ and $X^2 + bX + c = (X - \alpha)(X - \bar{\alpha}) \,|\, p(X)$ in $\mathbb{C}[X]$. But the division algorithm of $p(X)$ by $X^2 + bX + c$ gives always real coefficients, so $X^2 + bX + c \,|\, p(X)$ in $\mathbb{R}[X]$. By irreducibility, $p(X) = X^2 + bX + c$. Besides, since $p(X)$ has no real roots, $b^2 - 4c < 0$. □

Exercises

1. Let A be a unital commutative ring and let $i, n \in \mathbb{N}$ with $i \leq n$.
   (a) Prove that $A[X_{i+1}, \ldots X_n]$ is isomorphic to the quotient ring $A[X_1, \ldots, X_n]/(X_1, \ldots X_i)$.
   (b) Conclude that if A is an integral domain, then $(X_1, \ldots, X_i)$ is a prime ideal of $A[X_1, \ldots, X_n]$, and that if A is a field then $(X_1, \ldots, X_n)$ is a maximal ideal.

2. Let I be an ideal of a unital commutative ring A.
   (a) Prove that the set $I[X]$ of the polynomials in $A[X]$ with coefficients in I is an ideal of $A[X]$, and that it is the smallest ideal containing I.
   (b) Show that $I[X]$ is contained in (I, X), that $A[X]/I[X]$ is isomorphic to $(A/I)[X]$ and that $A[X]/(I, X)$ is isomorphic to A/I.
   (c) Conclude that if P is a prime ideal of A, then $P[X]$ and (P, X) are prime ideals of $A[X]$, and that if M is a maximal ideal of A, then so is (M, X) of $A[X]$.

3. Prove that $\mathbb{Z}[X]/(X^2 + 2) \cong \mathbb{Z}[\sqrt{-2}]$. Show that $(X^2 + 2)$ is a prime ideal in $\mathbb{Z}[X]$ which is not maximal, and find a maximal ideal containing it.

4. Prove that (X, Y) is not a principal ideal of $\mathbb{Q}[X, Y]$

5. (a) Prove that there exists a ring monomorphism from $\mathbb{Z}_2[X]$ into $B = \mathbb{Z}_2[X, Y]/(XY + 1)$ such that the image of X is a unit in B.
   (b) Show that $\mathbb{Z}_2[X]$ and B are not isomorphic.
   (c) Show that there is a monomorphism from B into the field of fractions of $\mathbb{Z}_2[X]$.

(d) Conclude that the field of fractions of $\mathbb{Z}_2[X]$ and $\mathbb{Z}_2[X,Y]/(XY+1)$ are isomorphic.

6. Prove the following version of Eisenstein's criterion: Let P be a prime ideal of a UFD R and let $p(X) = a_0 + \cdots + a_n X^n$ be a polynomial in $R[X]$ with $n \geq 1$. Assume that $a_n \notin P$, $a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$. Then prove that $p(X)$ is irreducible in $Q[X]$, where Q denotes the field of fractions of R.

7. Let p be an odd prime in $\mathbb{N}$ and $n \in \mathbb{N}$. Prove that $X^n - p$ is irreducible over $\mathbb{Z}[i]$.

8. Show that $X^3 - X$ has 6 roots in $\mathbb{Z}_6$.

9. Check that the polynomial $f(X) = X \in \mathbb{Z}_6[X]$ factors as $f(X) = (3X+4)(4X+3)$, so it is not irreducible. Moreover:

   (a) The reductions of $f(X)$ modulo the ideals (2) and (3) of $\mathbb{Z}_6$ are irreducible.

   (b) If $f(X) = g(X)h(X)$ is any factorization in $\mathbb{Z}_6[X]$, then the reduction of $g(X)$ (respectively $h(X)$) modulo (2) is either 1 or X (respectively X or 1) and something similar happens modulo (3). Determine all the possible factorizations of $f(X)$ in $\mathbb{Z}_6[X]$.

10. Describe the units, the nilpotent elements and the zero divisors of the rings $\mathbb{Z}_4[X]$ and $\mathbb{Z}_6[X]$.

11. Let F be a field, $a_1, \ldots, a_n$ different elements of F and $b_1, \ldots, b_n$ not necessarily different elements in F. Let $p_i(X) = \prod_{j \neq i}(X - a_j)$ $(i = 1, \ldots, n)$ and let $f(X) = \sum_{i=1}^{n} b_i \frac{p_i(X)}{p_i(a_i)}$. Prove that $f(X)$ is the unique polynomial in $F[X]$ of degree $\leq n-1$ such that $f(a_i) = b_i (i = 1, \ldots, n)$. (This is *Lagrange's interpolation method.*)

12. Find polynomials $f(X) \in \mathbb{Q}[X]$ of degree at most 3 such that

    - $f(0) = f(1) = 1$, $f(2) = 3$, $f(3) = 4$,
    - $f(-2) = 0$, $f(-1) = -2$, $f(1) = 3$, $f(2) = 4$.

13. Find factorizations in $\mathbb{Z}[X,Y]$ of the following polynomials:

    - $X^3 + YX^2 + (Y - 2Y^2)X - Y^2$,
    - $Y^2X^3 + Y^3X + Y^3X^2 - Y^4 - 2Y^4X - X^3 - YX^2 - YX + 2Y^2X + Y^2$.

[9] Use the Chinese Remainder Theorem.
[12] Use the previous exercise.

14. Use that $\mathbb{Z}[X_1, \ldots, X_n]$ is a unique factorization domain to prove that the Vandermonde determinant

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ X_1^2 & X_2^2 & \ldots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{vmatrix}$$

equals $\prod_{1 \leq i < j \leq n} (X_j - X_i)$. To do so, note that the Vandermonde determinant is a polynomial $p(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$. Check that for any $1 \leq i < j \leq n$, the irreducible polynomial $X_j - X_i$ divides $p(X_1, \ldots, X_n)$. Hence $\prod_{1 \leq i < j \leq n} (X_j - X_i) \,|\, p(X_1, \ldots, X_n)$. Finally, check that both polynomials have the same degree and the same coefficient of the monomial $X_2 X_3^2 \cdots X_n^{n-1}$; hence they are equal.

15. Prove that the following polynomials are irreducible in $\mathbb{Q}[X]$:

    (a) $\frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$,
    (b) $2X^5 - 6X^3 + 9X^2 - 15$,
    (c) $X^3 + 6X^2 + 17X + 3$,
    (d) $X^4 + 4X^3 + 6X^2 + 2X + 1$.

16. Find factorizations of the following polynomials:

    (a) $X^2 + X + 1$ over $\mathbb{Z}_2[X]$,
    (b) $X^4 + 1$ over $\mathbb{Z}_5[X]$,
    (c) $X^4 + 10X^2 + 1$ over $\mathbb{Z}[X]$.

17. Prove that the polynomial $(X-1)(X-2)\cdots(X-n)-1$ is irreducible in $\mathbb{Z}[X]$ for any $n \in \mathbb{N}$, while the polynomial $(X-1)(X-2)\cdots(X-n)+1$ is irreducible if $n \neq 4$.

18. Prove that $p(X) = X^3 + 9X + 6$ is irreducible over $\mathbb{Q}[X]$. Let α be a root of $p(X)$ in some field extension of $\mathbb{Q}$. Compute the inverse of $1 + \alpha$ in $\mathbb{Q}(\alpha)$.

19. Check that $p(X) = X^3 + X + 1$ is irreducible over $\mathbb{Z}_2$ and let α be a root in some extension. Compute the powers of α in $\mathbb{Z}_2(\alpha)$.

20. Let $p(X) = X^3 - 2 \in \mathbb{Q}[X]$. The roots of $p(X)$ in $\mathbb{C}$ are $\alpha = \sqrt[3]{2}$, $\beta = \sqrt[3]{2}\,\frac{-1 + i\sqrt{3}}{2}$ and $\gamma = \sqrt[3]{2}\,\frac{-1 - i\sqrt{3}}{2}$. Prove, by defining explicitly some isomorphisms, that $\mathbb{Q}(\beta) \cong \mathbb{Q}(\alpha) \cong \mathbb{Q}(\gamma)$.

21. Compute the discriminant of $X^3 + pX + q$ and of $X^n + a$.

22. Prove the following properties of the resultant and discriminant:

    (a) $\mathrm{Res}_{n,m}(f, g) = (-1)^{nm} \mathrm{Res}_{m,n}(g, f)$.
    (b) If $f(X) = \sum_{i=0}^{n} a_i X^i$, then $\mathrm{Res}(f, X - 1) = (-1)^n \sum_{i=0}^{n} a_i$.
    (c) $\mathrm{Res}(fg, h) = \mathrm{Res}(f, h)\,\mathrm{Res}(g, h)$.
    (d) $\mathrm{D}(fg) = \mathrm{D}(f)\,\mathrm{D}(g)\,\mathrm{Res}(f, g)^2$.

23. Let $p \in \mathbb{N}$ be a prime, $f(X) = \pm p + a_1 X + a_2 X^2 + \cdots + a_n X^n$ a polynomial in $\mathbb{Z}[X]$ such that $\sum_{i=1}^{n} |a_i| < p$. Prove that $f(X)$ is irreducible in $\mathbb{Q}[X]$.

[22] For the last two items, factor $f(X)$ and $g(X)$ in some extension.

[23] Prove that such polynomial cannot have roots in $\mathbb{C}$ of norm ≤ 1 and use the Fundamental Theorem of Algebra.

Chapter 4

Fields

In this chapter the basic facts of finite field extensions will be studied. This will allow us to prove the impossibility of solving the classical problems of 'trisecting an angle', 'doubling a cube' or 'squaring a circle' by means of ruler and compass.

§ 1. Algebraic extensions

1.1. Let F be a field with unity $1_F = 1$. Consider the map (see Exercise 29 in Chapter 1):

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

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

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

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

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

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

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

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

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

1.2 Examples.

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

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

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

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

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

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

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

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

To show that $\{1, \theta, \dots, \theta^{n-1}\}$ is a spanning set, take an arbitrary element $q(X)+\big(p(X)\big) \in K$. Since $F[X]$ is a euclidean domain, there are polynomials $c(X), r(X) \in F[X]$ with $\deg r(X) \leq n-1$ such that $q(X) = c(X)p(X) + r(X)$. If $r(X) = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}$, then

$$q(X) + \big(p(X)\big) = r(X) + \big(p(X)\big) = r_0 1 + r_1\theta + \cdots + r_{n-1}\theta^{n-1}$$

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

Therefore,

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

and the operations in K are given by:

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

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

Let us consider a couple of examples:

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

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

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

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

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

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

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

is a ring homomorphism and there are two possibilities:

1. $\ker \psi = 0$. In this case there is no nonzero polynomial in $F[X]$ for which α is a root, and ψ extends to a ring monomorphism $F(X) \hookrightarrow K$, whose image is $F(\alpha)$. In particular, $[F(\alpha) : F] = [F(X) : F] \geq \dim_F F[X] = \infty$. Then α is said to be *transcendental* over F.

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

Examples.

- $\mathbb{C}/\mathbb{R}$ is algebraic, because for any $\alpha = a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$, α is a root of $(X - \alpha)(X - \bar{\alpha}) = X^2 - 2aX + (a^2 + b^2) \in \mathbb{R}[X]$.

- $\mathbb{Q}(X)/\mathbb{Q}$ is not algebraic.

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

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

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

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

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

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

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

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

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

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

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

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

$$[L : F] = |I||J| = [L : K][K : F]. \qquad \square$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§ 2. Quadratic, cubic and quartic equations

The goal of this section is to give formulae for the solution by radicals of the algebraic equations of degree at most 4 over fields of characteristic $\neq 2, 3$. These formulae were obtained by mathematicians in the Italian *Cinquecento*, and constituted the most important advance in Mathematics since the classical Greek period.

In what follows F will denote an arbitrary ground field of characteristic $\neq 2, 3$ (although for the quadratic equation we may just assume the characteristic to be $\neq 2$). The coefficients of the quadratic, cubic and quartic equations considered will always belong to F.

2.1. Let us start with the well-known solution of the quadratic equation, that can always be assumed to be monic:

$$x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 - \frac{1}{4}\big(b^2 - 4c\big),$$

with $y = x + \dfrac{b}{2}$, the equation

$$x^2 + bx + c = 0 \qquad (*)$$

becomes

$$y^2 = \frac{1}{4}\big(b^2 - 4c\big),$$

and it follows then that the solutions to the quadratic equation $(*)$ are given by the classical formula

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

These solutions belong to the field $K = F(\sqrt{b^2 - 4c})$, which either equals F or is a quadratic field extension of F.

2.2. Now, consider the cubic equation

$$x^3 + ax^2 + bx + c = 0.$$

As before, with $y = x + \dfrac{a}{3}$, the previous equation becomes an equation of the form

$$y^3 + py + q = 0,$$

for suitable coefficients p, q. Therefore it is enough to deal with the cubic equations of the form:

$$x^3 + px + q = 0. \qquad (**)$$

Consider the discriminant $D = \mathrm{D}(X^3 + pX + q) = -\big(4p^3 + 27q^2\big)$ and let $1 \neq \omega$ be a cubic root of 1 (in some field extension of F if necessary). Thus ω is a root of $X^2 + X + 1$ and hence we may take $\omega = \frac{-1+\sqrt{-3}}{2} \in F(\sqrt{-3})$. Let K be a splitting field of $(X^2 + 3)(X^3 + pX + q)$, so that K contains ω and the solutions to $(**)$. Hence, over K:

$$X^3 + pX + q = (X - \alpha)(X - \beta)(X - \gamma),$$

with $\alpha, \beta, \gamma \in K$. Therefore,

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha\beta + \alpha\gamma + \beta\gamma = p \\ \alpha\beta\gamma = -q \end{cases}$$

Take $\theta_1, \theta_2 \in K$ such that

$$\begin{cases} \alpha = \theta_1 + \theta_2, \\ \beta = \omega\theta_1 + \omega^2\theta_2. \end{cases}$$

Then, since $\gamma = -\alpha - \beta$ and $1 + \omega + \omega^2 = 0$, we get $\gamma = \omega^2\theta_1 + \omega\theta_2$ and

$$3\theta_1 = \alpha + \omega^2\beta + \omega\gamma, \quad 3\theta_2 = \alpha + \omega\beta + \omega^2\gamma.$$

Thus,

$$\begin{aligned} 9\theta_1\theta_2 &= \alpha^2 + \beta^2 + \gamma^2 + (\omega + \omega^2)(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= \alpha^2 + \beta^2 + \gamma^2 - (\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= (\alpha + \beta + \gamma)^2 - 3(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= -3p, \end{aligned}$$

so that

$$\theta_1\theta_2 = -\frac{p}{3}.$$

Now,

$$(\theta_1 + \theta_2)^3 = \begin{cases} \alpha^3 = -p\alpha - q \\ \theta_1^3 + \theta_2^3 + 3\theta_1\theta_2(\theta_1 + \theta_2) = \theta_1^3 + \theta_2^3 - p\alpha \end{cases}$$

so that $\theta_1^3 + \theta_2^3 = -q$ and hence, since $\theta_1^3\theta_2^3 = \left(-\frac{p}{3}\right)^3$, θ_1^3 and θ_2^3 are the solutions of the quadratic equation

$$y^2 + qy - \frac{p^3}{27} = 0.$$

Thus we may take

$$\begin{aligned} \theta_1^3 &= \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} + \frac{\sqrt{-3D}}{18} \\ \theta_2^3 &= \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} - \frac{\sqrt{-3D}}{18} \end{aligned}$$

and we arrive at Cardano's formulae (which date back to the XVI century):

$$\theta_1 = \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{-3D}}{18}}, \qquad \theta_2 = \sqrt[3]{-\frac{q}{2} - \frac{\sqrt{-3D}}{18}},$$

where the cubic roots are taken so that $\theta_1\theta_2 = -\frac{p}{3}$, and once these values are fixed, the solutions to $(**)$ are given by:

$$\alpha = \theta_1 + \theta_2, \quad \beta = \omega\theta_1 + \omega^2\theta_2, \quad \gamma = \omega^2\theta_1 + \omega\theta_2.$$

The practical way to solve the equation $(**)$ works as follows. Put $x = u + v$ (think of $u = \theta_1$, $v = \theta_2$) to get

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

that is satisfied if

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

Thus, such u^3 and v^3 are the solutions of the quadratic equation $y^2 + qy - \frac{p^3}{27} = 0$ and proceed as above.

2.3. Finally, consider the quartic equations. As before, it is enough to deal with the quartic equations of the form

$$x^4 + px^2 + qx + r = 0. \qquad (***)$$

Let K be a splitting field of $X^4 + pX^2 + qX + r$ over F, so that there are $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in K$ such that

$$X^4 + pX^2 + qX + r = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4).$$

Consider the following elements in K:

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

Thus,

$$\left.\begin{aligned} (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \theta_1 \\ (\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = 0 \end{aligned}\right\} \Longrightarrow \alpha_1 + \alpha_2 = \sqrt{-\theta_1},\ \alpha_3 + \alpha_4 = -\sqrt{-\theta_1}.$$

Working in the same way with θ_2 and θ_3 we get:

$$\begin{cases} \alpha_1 + \alpha_2 = \sqrt{-\theta_1},\ \alpha_3 + \alpha_4 = -\sqrt{-\theta_1}, \\ \alpha_1 + \alpha_3 = \sqrt{-\theta_2},\ \alpha_2 + \alpha_4 = -\sqrt{-\theta_2}, \\ \alpha_1 + \alpha_4 = \sqrt{-\theta_3},\ \alpha_2 + \alpha_4 = -\sqrt{-\theta_3}, \end{cases}$$

where the roots $\sqrt{-\theta_1}$, $\sqrt{-\theta_2}$ and $\sqrt{-\theta_3}$ have to be taken so that its product is

$$\begin{aligned} &(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4) \\ &\quad = \alpha_1^3 + \alpha_1^2(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_1(\alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) + \alpha_2\alpha_3\alpha_4 \\ &\quad = \alpha_1^3 - \alpha_1^3 + \left(\sum_{1 \le i < j < k \le 4} \alpha_i\alpha_j\alpha_k \right) = -q. \end{aligned}$$

(That is, once two of the roots are chosen, the third one is determined.) Now $\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3} = 3\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 2\alpha_1$, and in a similar vein:

$$\begin{cases} \alpha_1 = \frac{1}{2}\left(\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}\right) \\ \alpha_2 = \frac{1}{2}\left(\sqrt{-\theta_1}-\sqrt{-\theta_2}-\sqrt{-\theta_3}\right) \\ \alpha_3 = \frac{1}{2}\left(-\sqrt{-\theta_1}+\sqrt{-\theta_2}-\sqrt{-\theta_3}\right) \\ \alpha_4 = \frac{1}{2}\left(-\sqrt{-\theta_1}-\sqrt{-\theta_2}+\sqrt{-\theta_3}\right) \end{cases}$$

that gives the solutions to the quartic equation, provided we know how to obtain the θ_i's. But (check the missing details!),

$$\begin{cases} \theta_1+\theta_2+\theta_3 = 2\sum_{1\le i<j\le 4}\alpha_i\alpha_j = 2p, \\ \theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = \ldots = p^2-4r, \\ \theta_1\theta_2\theta_3 = -(\alpha_1+\alpha_2)^2(\alpha_1+\alpha_3)^2(\alpha_1+\alpha_4)^2 = -q^2, \end{cases}$$

so that $\theta_1,\theta_2,\theta_3$ are the solutions to the cubic equation:

$$z^3-2pz^2+(p^2-4r)z+q^2=0,$$

that we already know how to solve by radicals.

The practical way to work is the following method, due to Ferrari (a pupil of Cardano): If $q=0$ in $(***)$, the equation is quadratic in x^2, so it can be solved using the formula for the quadratic equations. Otherwise, take a new element u (think of u as $-\theta_1$), then

$$\begin{aligned} x^4+&px^2+qx+r \\ &= \left(x^2+\frac{p+u}{2}\right)^2-ux^2-\frac{(p+u)^2}{4}+qx+r \\ &= \left(x^2+\frac{p+u}{2}\right)^2-\left(\sqrt{u}x-\frac{q}{2\sqrt{u}}\right)^2+\frac{q^2}{4u}-\frac{(p+u)^2}{4}+r \end{aligned}$$

and choose u so that $\frac{q^2}{4u}-\frac{(p+u)^2}{4}+r=0$ or, equivalently, $u(p+u)^2-4ur-q^2=0$, or

$$u^3+2pu^2+(p^2-4r)u-q^2=0,$$

and this is a cubic equation that we already know how to solve in u. Finally, for each value of u, the original equation becomes a pair of quadratic equations

$$x^2+\frac{p+u}{2} = \pm\left(\sqrt{u}x-\frac{q}{2\sqrt{u}}\right),$$

and again we know how to solve these.

§ 3. Ruler and compass constructions

There are a number of classical geometrical problems that dates back at least to the fifth century BC that involve the construction of lengths or angles using only a ruler (without marks) and a compass. Among them, we will deal with the following three, that were left unresolved by the great Greek mathematicians:

1. **Doubling the cube:** Given a cube, construct the side of a cube that has twice the volume of the first.
2. **Trisecting an angle:** Construct an angle that is one-third of a given arbitrary angle.
3. **Squaring the circle:** Construct a square with the same area as a given circle.

You may browse through internet and find many sites devoted to these and related problems. For instance, you may perform some constructions at the URL

`http://wims.unice.fr/`

Let us fix a couple of points in the euclidean plane, so that our unit of length will be the distance between these points, and the segment joining these two points will be our 'unit segment'. The steps that we are allowed to do are the following (starting with our two points):

(i) To draw a line that passes through two points already constructed.

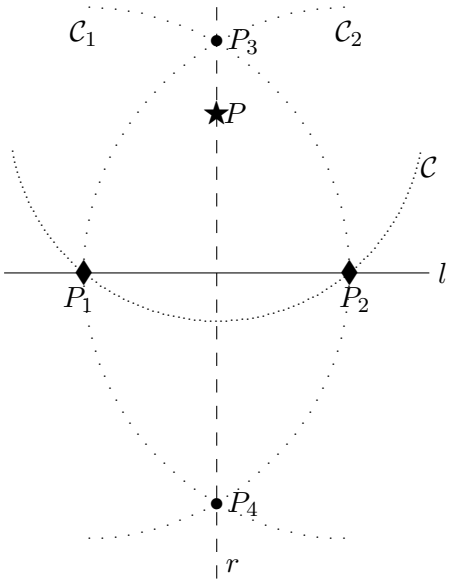
(ii) To find the intersection point of two lines already constructed (we may have to extend them until the intersection point is achieved).

(iii) To draw a circle with center already constructed and with radius the length between two points already constructed.

(iv) To find the intersection of a line and a circle or of two circles already constructed.

With these steps we may easily, given a line l and a point P not in the line, to draw a line perpendicular to l and passing through P. Also, it is easy to draw a line parallel to l through P (see Figure 4.1).

Now, given two segments of length a and b it is quite easy to construct segments of length $a \pm b$, and Figure 4.2 shows how to construct segments of length ab and $\frac{a}{b}$ (assuming $b \neq 0$). Here Thales' Theorem is used.



To draw a perpendicular line to l through P take the intersection $\{P_1, P_2\}$ of the circle $\mathcal{C}$ with center P and large enough radius with l, then consider the intersection $\{P_3, P_4\}$ of the circles $\mathcal{C}_1$ and $\mathcal{C}_2$ with centers P_1 and P_2 and passing through P_2 and P_1 respectively. The line r joining P_3 and P_4 is the line sought for. (Note that l may contain P.)
Now, to draw a parallel line to l through P, it is enough to draw a perpendicular line to r through P.

Figure 4.1: Ruler and compass constructions of perpendicular lines

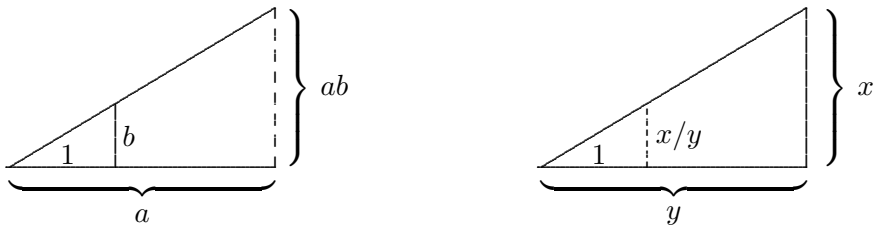


Figure 4.2: 'Ruler and compass multiplication and division'

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

Thus, it is clear that $0, 1, 2, \ldots, n, \ldots$ are all constructible. Hence so are all the rational numbers.

Consider $C = \{x \in \mathbb{R} : x \text{ is constructible}\}$.

3.2 Proposition. *C is a subfield of $\mathbb{R}$ and an extension of $\mathbb{Q}$. Moreover, for any $a \in C$ with $a > 0$, $\sqrt{a} \in C$.*

Proof. We have already seen that $\mathbb{Q} \subseteq C$ and that C is a subfield of $\mathbb{R}$ since it contains the addition, subtraction, product and division (if possible) of any two elements in C. Besides, Figure 4.3 shows how to construct a segment of length $\sqrt{a}$, starting with a segment of length $a > 0$. □

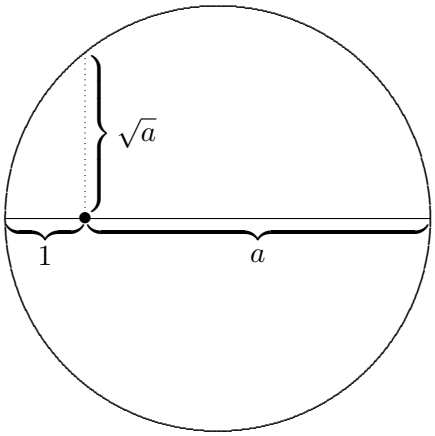
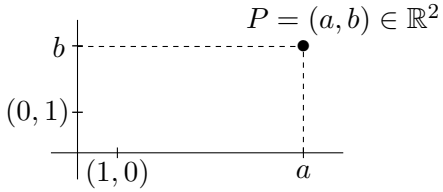


Figure 4.3: 'Ruler and compass construction of square roots'

Let us fix a point that will be our origin for a coordinate system of the euclidean plane. With ruler and compass we construct two perpendicular lines meeting at the origin, these will be our coordinate axes, and draw the points with coordinates $(1, 0)$ and $(0, 1)$ (at a unit distance from the origin)



$P = (a, b)$ is constructible if and only if so are $a, b \in \mathbb{R}$, that is, if and only if $a, b \in C$.

Let $F/\mathbb{Q}$ be a field extension with $F \subseteq \mathbb{R}$. Then we will say that:

(i) a line l (in $\mathbb{R}^2$) *belongs to* F if it passes through two points with coordinates in F,

(ii) a circle $\mathcal{C}$ *belongs to* F if the coordinates of its center and the length of its radius are in F.

3.3 Lemma. *Let F be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{R}$, and let l be a line in $\mathbb{R}^2$ and $\mathcal{C}$ a circle in $\mathbb{R}^2$. Then:*

(i) *l belongs to F if and only if there are $a, b, c \in F$ such that $l = \{(x, y) \in \mathbb{R}^2 : ax + by + c = 0\}$.*

(ii) *If $\mathcal{C}$ belongs to F, then there are $a, b, c \in F$ such that $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 + ax + by + c = 0\}$. The converse is true if F is closed for square roots (that is, $0 < a \in F \Rightarrow \sqrt{a} \in F$).*

Proof. (i) If $P = (p_1, p_2)$, $Q = (q_1, q_2)$ are points of l with $p_1, p_2, q_1, q_2 \in F$, then an equation for l is

$$(q_2 - p_2)(x - p_1) - (q_1 - p_1)(y - p_2) = 0,$$

which is $ax + by + c = 0$ with $a = q_2 - p_2$, $b = p_1 - q_1$ and $c = (p_2 - q_2)p_1 + (q_1 - p_1)p_2$ in F.

Conversely, if l has an equation $ax + by + c = 0$ with $a, b, c \in F$, then if $a \neq 0 \neq b$, l passes through the points $(\frac{-c}{a}, 0)$ and $(0, \frac{-c}{b})$ with coordinates in F, while if $a = 0$, l passes through $(0, \frac{-c}{b})$ and $(1, \frac{-c}{b})$, and if $b = 0$ through $(\frac{-c}{a}, 0)$ and $(\frac{-c}{a}, 1)$.

(ii) If $P = (p, q)$ is the center of $\mathcal{C}$, r its radius, and $p, q, r \in F$, then an equation of $\mathcal{C}$ is $(x - p)^2 + (y - q)^2 = r^2$, which is $x^2 + y^2 + ax + by + c = 0$ with $a = -2p$, $b = -2q$ and $c = p^2 + q^2 - r^2$ in F. Conversely, if F is closed for square roots and $\mathcal{C}$ has an equation $x^2 + y^2 + ax + by + c = 0$ with $a, b, c \in F$, then the equation of $\mathcal{C}$ can be written as

$$\left(x + \frac{a}{2}\right)^2 + \left(y + \frac{b}{2}\right)^2 = \frac{a^2}{4} + \frac{b^2}{4} - c,$$

so that its center is $(\frac{-a}{2}, \frac{-b}{2})$, with coordinates in F, and its radius is $\frac{1}{2}\sqrt{a^2 + b^2 - 4c}$, also in F. □

3.4 Proposition. *Let F be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{R}$. Then:*

1. *If l_1 and l_2 are nonparallel lines that belong to F, then the coordinates of $l_1 \cap l_2$ are in F.*

2. *If l is a line and $\mathcal{C}$ a circle that belong to F and $l \cap \mathcal{C} \neq \emptyset$, then there is a $u \in \mathbb{R}$ such that $u^2 \in F$ and $l \cap \mathcal{C}$ consists of one or two points with coordinates in $F(u)$.*

3. *If $\mathcal{C}_1$ and $\mathcal{C}_2$ are two circles that belong to F and $\mathcal{C}_1 \cap \mathcal{C}_2 \neq \emptyset$, then there is a $u \in \mathbb{R}$ such that $u^2 \in F$ and $\mathcal{C}_1 \cap \mathcal{C}_2$ consists of one or two points with coordinates in $F(u)$.*

Proof. Item 1 follows from the fact that the solution of a system of linear equations over a field, that has a unique solution, belongs to this field.

Now, to prove item 3, we have to deal with a system of equations of the form

$$\begin{cases} \mathcal{C}_1 : x^2 + y^2 + ax + by + c = 0 \\ \mathcal{C}_2 : x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

with $a, b, c, a', b', c' \in F$. But subtracting both equations it follows that $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{C}_1 \cap l$ with l the line with equation $(a-a')x+(b-b')y+(c-c') = 0$. Therefore, it is enough to prove item 2.

Thus, consider the system of equations:

$$\begin{cases} l : ax + by + c = 0 \\ \mathcal{C} : x^2 + y^2 + dx + ey + f = 0 \end{cases} \qquad a, b, c, d, e, f \in F$$

where we may assume, without loss of generality, that $a \neq 0$. Let $P = (x_0, y_0) \in l \cap \mathcal{C}$, then $x_0 = -\dfrac{c + by_0}{a}$, so that

$$\frac{(c + by_0)^2}{a^2} + y_0^2 - d\frac{c + by_0}{a} + ey_0 + f = 0,$$

which is equivalent to

$$(a^2 + b^2)y_0^2 + (2bc - abd + ea^2)y_0 + (c^2 - adc + a^2 f) = 0,$$

and this shows that $y_0 \in F(u)$ with $u^2 = (2bc - abd + ea^2)^2 - 4(a^2 + b^2)(c^2 - adc + a^2 f) \in F$, and hence also $x_0 = -\dfrac{c + by_0}{a} \in F(u)$, as required. □

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

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

Proof. If $a \in C$, then it can be constructed using the allowed steps from the two starting points. Because of the previous Proposition at each step the coordinates are either in the same field where the coordinates of the points constructed so far are, or in a field that is a quadratic extension of the previous one. Hence the result.

Conversely, let $F_i = F_{i-1}(u_i)$ with $u_i^2 \in F_{i-1}$ and $u_i \notin F_{i-1}$ (quadratic extensions) for $i = 1, \ldots, n$, and with $F_0 = \mathbb{Q}$. Then $F_0 = \mathbb{Q} \subseteq C$ and if $F_{i-1} \subseteq C$ for some $i = 1, \ldots, n$, then $u_i^2 \in C$, so $u_i \in C$ as C is closed for

square roots. Thus, $F_i \subseteq C$ too. Therefore $F_n \subseteq C$ and, since $a \in F_n$, then $a \in C$.

For the last part notice that $2^n = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}]$, so that $[\mathbb{Q}(a) : \mathbb{Q}]$ is a power of 2. □

Remark. With 'Galois Theory' (you will study it shortly) it can be proved that for any $a \in \mathbb{R}$, $a \in C$ if and only if $[K : \mathbb{Q}]$ is a power of 2, where K is the splitting field of $m_{a,\mathbb{Q}}(X)$ ($K \subseteq \mathbb{C}$).

We have reached to the point where we can show that the ancient Greek mathematicians could not solve the classical problems mentioned at the beginning of the section because *it is impossible to do so*!

3.6 Theorem. *The classical problems of doubling the cube, trisecting an angle and squaring the circle are not solvable with ruler and compass.*

Proof.

- The cube of side 1 can be doubled if and only if $\sqrt[3]{2} \in C$, but $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ because $X^3 - 2$ is irreducible (Eisenstein's criterion), and 3 is not a power of 2.

- If we had a method to trisect any angle we would be able to trisect $\theta = \dfrac{\pi}{3}$ (which can be constructed with ruler and compass since it is any of the angles of an equilateral triangle). But to construct the angle $\dfrac{\pi}{9}$ is equivalent to construct $\cos\frac{\pi}{9} = \alpha$. However, since

$$\left(\cos\frac{\pi}{9} + i\sin\frac{\pi}{9}\right)^3 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + i\frac{\sqrt{3}}{2},$$

  taking the real parts we get $\alpha^3 - 3\alpha(1-\alpha^2) = \frac{1}{2}$, or $(2\alpha)^3 - 3(2\alpha) - 1 = 0$. But $X^3 - 3X - 1$ is irreducible in $\mathbb{Q}[X]$ (it has no rational roots). Hence $m_{\alpha,\mathbb{Q}}(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$ and $[\mathbb{Q}(\alpha), \mathbb{Q}] = 3$, which is not a power of 2.

- The unit circle can be squared if and only if $\sqrt{\pi} \in C$ and this, in particular, would imply that $\sqrt{\pi}$ is algebraic over $\mathbb{Q}$, and hence so would be π. However, Lindemann proved in 1882 that π is transcendental over $\mathbb{Q}$. (You may find a proof of this fact in the appendix to this Chapter. Although elementary (that is, it does not use any complicated result), it is not an easy proof and you will need some patience to grasp it.) □

Exercises

1. Let α be a root of $X^3 - X + 1 \in \mathbb{Q}[X]$. Compute the inverse and the minimal polynomial of the elements $\beta = 2 - 3\alpha + 2\alpha^2$ and $\gamma = 1 - 2\alpha + 3\alpha^2$ of $\mathbb{Q}(\alpha)$.

2. Let α be an algebraic element over a field F with minimal polynomial of odd degree. Prove that $F(\alpha) = F(\alpha^2)$. Provide an example showing that this is no longer valid for even degree.

3. Find elements α, β such that $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{3}, i, \omega) = \mathbb{Q}(\beta)$, where $\omega^3 = 1 \neq \omega$.

4. Prove that there exist finite field extensions of $\mathbb{Q}$ of arbitrary degree. Is this true also for $\mathbb{R}$?

5. What is the degree of the field extension $\mathbb{C}/\mathbb{Q}$?

6. Find the minimal polynomials over $\mathbb{Q}$ of the real numbers $\sqrt{2} + 5$, $\sqrt[3]{2} + 5$, $\sqrt{-1 + \sqrt{2}}$ and $\sqrt{2} - \sqrt[3]{3}$.

7. Find subfields of $\mathbb{C}$ that are splitting fields over $\mathbb{Q}$ of the polynomials $X^3 - 1$, $X^4 + 5X^2 + 6$, $X^6 - 8$ and $(X^2 - 2)(X^3 - 2)$. For each case, compute the degree of the corresponding extensions over $\mathbb{Q}$.

8. Prove that $p(X) = X^3 + X + 1$ is irreducible over $\mathbb{F}_2[X]$ and that if ζ is a root of $p(X)$ (in some extension), then $\mathbb{F}_2(\zeta)$ is a splitting field of $p(X)$. Compute all the roots of $p(X)$ (in terms of ζ) and the degree $[\mathbb{F}_2(\zeta) : \mathbb{F}_2]$.

9. Find all the monic irreducible polynomials of degree 2 and 3 over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$.

10. Construct fields with 8, 9 and 16 elements.

11. Let $p, n \in \mathbb{N}$ with p prime and let K be a splitting field of $f_n(X) = X^{p^n} - X$ over $\mathbb{F}_p$. Prove that K is precisely the set of roots of $f_n(X)$. Deduce that $[K : \mathbb{F}_p] = n$.

12. Let K be a finite field.

    (a) Show that there are $p, n \in \mathbb{N}$, with p prime, such that K contains p^n elements.

    (b) Prove that any element in K is a root of the polynomial $f_n(X)$ considered in the previous exercise.

[12] (b) For any $0 \neq \alpha \in K$ the map $\varphi : K^\times \to K^\times$, $\varphi(\gamma) = \alpha\gamma$, is a bijection, and hence $\prod_{\gamma \in K^\times} \gamma = \prod_{\gamma \in K^\times} \varphi(\gamma) = \alpha^{|K|-1} \prod_{\gamma \in K^\times} \gamma$. Thus, $\alpha^{|K|-1} = 1$.

(c) Conclude that, up to isomorphism, the only finite fields are those constructed in the previous exercise.

13. Find the (complex) roots of the polynomial $X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

Appendix: π is transcendental

It is possible to prove the existence of transcendental real numbers (over $\mathbb{Q}$) by using Set Theory, because the set of algebraic real numbers is countable, while the set of all real numbers is not. This was shown by Cantor in 1874. However, no particular transcendental number is singled out in this way. Previously, Liouville (1844) showed some strange transcendental numbers like $\sum_{n=1}^{\infty} 10^{-n!}$. It was Hermite (1873) who proved that e is transcendental, and soon thereafter Lindemann (1882) did the same with π.

Here we will use the ideas of Hermite and Lindemann, following the exposition by I.N. Stewart: *Galois Theory*, (2^{nd} edition), Chapman and Hall, London 1989, in order to prove that π is transcendental.

A polynomial $p(X_1, \ldots, X_r) \in F[X_1, \ldots, X_r]$ (where F is an arbitrary field) is said to be *symmetric* if $p(X_1, \ldots, X_r) = p(X_{\sigma(1)}, \ldots, X_{\sigma(r)})$ for any permutation σ. The most important examples of symmetric polynomials are the so called *elementary symmetric polynomials*:

$$\begin{cases} s_1 = X_1 + \cdots + X_r, \\ s_2 = \displaystyle\sum_{1 \le i < j \le r} X_i X_j, \\ s_3 = \displaystyle\sum_{1 \le i < j < k \le r} X_i X_j X_k, \\ \quad \vdots \qquad \vdots \\ s_r = X_1 \cdots X_r. \end{cases}$$

A.1 Lemma. *Let $p(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$ be a symmetric polynomial. Then there is a polynomial $q(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$, of degree at most the degree of $p(X_1, \ldots, X_r)$, such that $p(X_1, \ldots, X_r) = q(s_1, \ldots, s_r)$.*

(For instance, $X_1^2 + \cdots + X_r^2 = s_1^2 - 2s_2$, so here $q(X_1, \ldots, X_r) = X_1^2 - 2X_2$.)

Proof. Order the monomials in $\mathbb{Z}[X_1, \ldots, X_r]$ first by degree and then lexicographically: $X_1^{n_1} \cdots X_r^{n_r} > X_1^{m_1} \cdots X_r^{m_r}$ if either $n_1 + \cdots + n_r > m_1 + \cdots + m_r$, or $n_1 + \cdots + n_r = m_1 + \cdots + m_r$ and there is a j, $0 \le j \le r-1$, such that $n_i = m_i$ for $i = 1, \ldots j$ and $n_{j+1} > m_{j+1}$.

If $p(X_1, \ldots, X_r)$ is symmetric and $X_1^{n_1} \cdots X_r^{n_r}$ is its greatest monomial with nonzero coefficient $a \neq 0$, by symmetry it follows that $n_1 \ge \cdots \ge n_r$. But the greatest monomial of $s_1^{n_1 - n_2} s_2^{n_2 - n_3} \cdots s_r^{n_r}$ is

$$X_1^{n_1 - n_2} (X_1 X_2)^{n_2 - n_3} \cdots (X_1 \cdots X_r)^{n_r} = X_1^{n_1} \cdots X_r^{n_r}$$

too. Hence, $\tilde{p}(X_1,\ldots,X_r) = p(X_1,\ldots,X_r) - as_1^{n_1-n_2}s_2^{n_2-n_3}\cdots s_r^{n_r}$ is a symmetric polynomial with a greatest monomial lower than the greatest monomial of $p(X_1,\ldots,X_r)$. If $\tilde{p}(X_1,\ldots,X_r) = 0$ we are done. Otherwise, we repeat the process with $\tilde{p}(X_1,\ldots,X_r)$ until we reach the result. □

A.2 Corollary. *Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial such that $f(X) = (X-\alpha_1)\cdots(X-\alpha_m)$ $(\alpha_1,\ldots,\alpha_m \in \mathbb{C})$. Then the polynomials $f_1(X) = f(X)$, $f_2(X) = \prod_{1\le i<j\le m}\big(X-(\alpha_i+\alpha_j)\big)$, $f_3(X) = \prod_{1\le i<j<k\le m}\big(X-(\alpha_i+\alpha_j+\alpha_k)\big)$, ... , $f_m(X) = X-(\alpha_1+\cdots+\alpha_m)$ also belong to $\mathbb{Q}[X]$.*

Proof. It is enough to realize that the coefficients of these polynomials are symmetric in $\alpha_1,\ldots,\alpha_m$ so, by the Lemma above, they are polynomial expressions in $\alpha_1+\cdots+\alpha_m$, ... , $\alpha_1\cdots\alpha_m \in \mathbb{Q}$. □

A.3 Corollary. *Let $f(X) = a_0 + a_1X + \cdots + a_rX^r$ and $g(X)$ be two polynomials in $\mathbb{Z}[X]$ of degree $r, m \ge 1$ respectively. Let $\beta_1,\ldots,\beta_r \in \mathbb{C}$ be the roots (possibly repeated) of $f(X)$. Then $g(\beta_1)+\cdots+g(\beta_r) \in \frac{1}{a_r^m}\mathbb{Z}$.*

Proof. Because of the previous Lemma, $g(X_1)+\cdots+g(X_r) = q(s_1,\ldots,s_r)$, with $q(X_1,\ldots,X_r) \in \mathbb{Z}[X_1,\ldots,X_r]$ of degree $\le m$. Since $\beta_1+\cdots+\beta_r = -\frac{a_{r-1}}{a_r}$, ..., $\beta_1\cdots\beta_r = \frac{(-1)^r a_0}{a_r}$, we get

$$g(\beta_1)+\cdots+g(\beta_s) = q\left(-\frac{a_{r-1}}{a_r},\ldots,\frac{(-1)^r a_0}{a_r}\right) \in \frac{1}{a_r^m}\mathbb{Z}. \qquad \square$$

A.4 Theorem. (Lindemann, 1882) *π is transcendental (over $\mathbb{Q}$).*

Proof. Assume, on the contrary, that π is algebraic over $\mathbb{Q}$, then so is $i\pi \in \mathbb{C}$. Let $f(X) \in \mathbb{Q}[X]$ be a monic polynomial such that $f(X) = (X-\alpha_1)\cdots(X-\alpha_m)$ with $\alpha_1 = i\pi, \alpha_2,\ldots,\alpha_m \in \mathbb{C}$. Since $e^{i\pi}+1 = 0$, one gets

$$(e^{\alpha_1}+1)\ldots(e^{\alpha_m}+1) = 0. \tag{A.5}$$

Consider now the polynomials $f_1(X) = f(X),\ldots,f_m(X)$ in Corollary A.2, as well as its product $g(X) = f_1(X)\cdots f_m(X)$, whose roots are the sums $\alpha_{i_1}+\cdots+\alpha_{i_r}$ $(1 \le i_1 < \ldots < i_r \le m)$. Thus, by expanding the expression in equation (A.5) one gets

$$1 + \sum_{\gamma \text{ root of } g(X)} e^{\gamma} = 0, \tag{A.6}$$

in which each root appears as many times as indicated by its multiplicity. Some of these roots $\alpha_{i_1}+\cdots+\alpha_{i_r}$ may be 0, so $g(X) = X^N\tilde{g}(X)$ for some $N \ge 0$ with $\tilde{g}(X) \in \mathbb{Q}[X]$ and $\tilde{g}(0) \ne 0$, and equation (A.6) becomes

$$k + \sum_{\gamma \text{ root of } \tilde{g}(X)} e^{\gamma} = 0, \tag{A.7}$$

where $k = 1 + N \in \mathbb{N}$. By clearing denominators in $\tilde{g}(X)$, we get a polynomial $q(X) = a_0 + a_1X + \cdots + a_rX^r \in \mathbb{Z}[X]$ ($a_r \neq 0 \neq a_0$) such that $q(X) = a_r(X - \beta_1)\cdots(X - \beta_r)$ with

$$k + \sum_{j=1}^{r} e^{\beta_j} = 0. \tag{A.8}$$

Consider now a prime number $p \in \mathbb{N}$ larger than k, a_0 and a_r, take $s = pr - 1$ and the polynomial

$$h(X) = a_r^s x^{p-1} \frac{q(X)^p}{(p-1)!} \in \mathbb{Q}[X]$$

of degree $rp + p - 1 = s + p$, as well as the polynomial obtained by adding $h(X)$ and its derivatives:

$$H(X) = h(X) + h'(X) + \cdots + h^{(s+p)}(X).$$

Since $H'(X) = H(X) - h(X)$, it follows that

$$\frac{d}{dx}\left(e^{-x}H(x)\right) = -e^{-x}h(x),$$

so

$$e^{-x}H(x) - H(0) = -\int_0^x e^{-y}h(y)\,dy.$$

Make the change of variables $y = \lambda x$ and multiply both sides by e^x to get:

$$H(x) - e^xH(0) = -x\int_0^1 e^{(1-\lambda)x}h(\lambda x)\,d\lambda.$$

Now substitute $x = \beta_j$ and add for $j = 1, \ldots, r$ to get:

$$\sum_{j=1}^{r} H(\beta_j) + kH(0) = -\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\lambda)\beta_j}h(\lambda\beta_j)\,d\lambda. \tag{A.9}$$

Notice that by the very definition of h, $h^{(t)}(\beta_j) = 0$ for $0 < t < p$. Moreover, for $t \geq p$, $h^{(t)}(\beta_j)$ is a polynomial with integer coefficients in β_j of degree $\leq s$, and with all the coefficients being multiples of $a_r^s p$, because we have to derive $q(x)^p$ at least p times to get a nonzero summand. By Corollary A.3 we know that

$$\sum_{j=1}^{r} h^{(t)}(\beta_j) \in pa_r^s \frac{1}{a_r^s}\mathbb{Z} = p\mathbb{Z}, \quad t = p, \ldots, p + s,$$

so the left hand side in equation (A.9) is $pm + kH(0)$ for some $m \in \mathbb{Z}$.

On the other hand,

$$\begin{aligned} &h^{(t)}(0) = 0 \quad \text{for } t = 0, \ldots, p-2, \\ &h^{(p-1)}(0) = a_r^s a_0^p \quad (a_r \neq 0 \neq a_0), \\ &h^{(t)}(0) \in p\mathbb{Z} \quad \text{for } t > p, \end{aligned}$$

so the left hand side in equation (A.9) is an integer of the form $pm + ka_r^s a_0^p$ with $m \in \mathbb{Z}$, which is not a multiple of p because $p > k, a_0, a_r$. In particular, this is always a nonzero integer.

However, if $M > 0$ is an upper bound of $|\lambda\beta_j|$ and $|q(\lambda\beta_j)|$ ($0 \leq \lambda \leq 1$, $1 \leq j \leq r$), then the right hand side of equation (A.9) is bounded by a multiple of $\dfrac{M^{2p-1}}{(p-1)!}$. And since $\lim_{n\to\infty} \dfrac{M^{2n-1}}{(n-1)!} = 0$, with p large enough we get that the modulus of the right hand side of equation (A.9) is smaller than 1, a contradiction that completes the proof. □

Epilogue: Groups and Galois Theory

Galois Theory (a name that comes after Évariste Galois, 1811–1832) deals with the symmetries of the roots of polynomials, and is motivated by problems like

- Are there solutions by radicals to the equations of degree ≥ 5? The answer is no (Theorem of Abel–Ruffini).
- Which regular polygons can be constructed with ruler and compass? Here the answer is that the regular polygon of n sides is constructible if and only if $n = 2^r p_1 \cdots p_s$, where $r, n \in \mathbb{Z}_{\geq 0}$ and $p_1, \ldots, p_s$ are different Fermat primes (of the form $2^{2^m} + 1$).

The algebraic structure used to study symmetries is that of *group*.

E.1 Definition. A *group* is a set G endowed with a binary operation $G \times G \to G$, $(x, y) \mapsto xy$, which is associative ($(xy)z = x(yz)$ for any $x, y, z \in G$), there is a neutral element ($e \in G$ such that $ex = xe = x$ for any $x \in G$), and for any element of G there is an inverse ($\forall x \in G$, $\exists y \in G$ such that $xy = yx = e$, notation: $y = x^{-1}$).

If the operation is also commutative, then the group is said to be *abelian*.

The cardinal of a group G is called the *order* of G (denoted by $|G|$).

E.2 Examples.

- Any ring R is an abelian group with the addition.
- The symmetries of an equilateral triangle form a group. More precisely, fix an equilateral triangle and consider

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

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

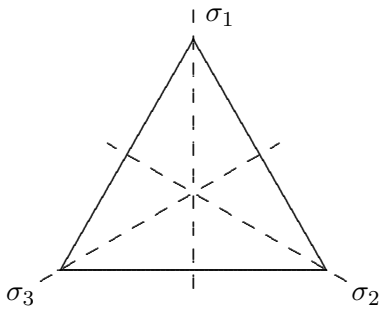


Figure E.1: Symmetries of an equilateral triangle.

Each isometry fixing the triangle permutes the vertices. The three symmetries correspond to the transposition of two vertices.

- Let X be a set, then

$$S_X = \{f : X \to X : f \text{ is a bijection}\}$$

is a group with the composition of maps as the binary operation. This is called the *symmetric group* on X. In particular, for $X = \{1, \ldots, n\}$, S_X is denoted by S_n and called the *symmetric group of degree* n. Its elements are called *permutations*, any permutation σ can be identified with the two rows matrix $\left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{smallmatrix}\right)$. The order of S_n is $n!$. Notice that the group of symmetries of an equilateral triangle can be identified with S_3, by looking at the permutation of the vertices performed by any isometry in G.

E.3 Definition. Let G and K be two groups.

(i) A subset H of G that is closed for the operation in G and for inverses is called a *subgroup* of G (notation: $H \leq G$). Moreover, if H is a subgroup of G and for any $x \in H$ and $y \in G$, $yxy^{-1} \in H$, then H is called a *normal subgroup* of G (notation: $H \trianglelefteq G$).

(ii) A map $f : G \to K$ is said to be a *homomorphism of groups* if $f(xy) = f(x)f(y)$ for any $x, y \in G$. As for rings, one talks about isomorphisms, monomorphisms, epimorphisms and automorphisms.

The proof of the next result is completely analogous to the proof of the corresponding result for rings.

E.4 Proposition. *Let $f : G \to K$ be a homomorphism of groups. Then:*

(i) $\ker f = \{x \in G : f(x) = e\}$ *is a normal subgroup of* G*, called the* kernel *of* f*.*

(ii) $\operatorname{im} f = \{f(x) : x \in G\}$ *is a subgroup of* K*, called the* image *of* f*.*

E.5 Examples. Let F be a field of characteristic $\neq 2$ and let $1 \neq n \in \mathbb{N}$.

- Let $\{e_1, \ldots, e_n\}$ be the canonical basis of F^n and let $\mathrm{GL}(F^n) = \{f : F^n \to F^n : f \text{ is linear and bijective}\}$. Then $\mathrm{GL}(F^n)$ is a group (the *general linear group*) with the composition of maps. Then

  – The map

  $$\begin{aligned} \varphi : S_n &\longrightarrow \mathrm{GL}(F^n) \\ \sigma &\mapsto \varphi_\sigma : F^n \to F^n, \end{aligned}$$

  where φ_σ is the linear map such that $\varphi_\sigma(e_i) = e_{\sigma(i)}$ for any $i = 1, \ldots, n$, is a monomorphism. (Notice that $\varphi_\sigma(x_1, \ldots, x_n) = \big(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\big)$.)

  – $\det : \mathrm{GL}(F^n) \to F^\times$ is an epimorphism of groups, where $F^\times = F \setminus \{0\}$ is a group with the multiplication. Moreover, $\det(\varphi_\sigma) = \pm 1$ for any $\sigma \in S_n$. ($\{\pm 1\} \leq F^\times$.)

  – The composition of the two homomorphisms above, gives an epimorphism $\operatorname{sgn} : S_n \to \{\pm 1\}$, $\sigma \mapsto \operatorname{sgn}(\sigma) = \det(\varphi_\sigma)$, which is called *signature*.

- $A_n = \ker \operatorname{sgn}$ is a normal subgroup of S_n, called the *alternating group*.

  A *transposition* is an element of S_n that leaves fixed any element in $\{1, \ldots, n\} \setminus \{i, j\}$ for some $1 \leq i < j \leq n$ and permutes i and j. It is denoted by (i, j).

  Any permutation in S_n is a product of transpositions:

  Proof. It is done by induction on n. If $n = 2$ this is clear since $S_2 = \{id, (1, 2)\}$ (and $id = (1, 2)^2$). So assume the result is valid for $n - 1$. Let $\sigma \in S_n$ arbitrary. If $\sigma(n) = n$, then the restriction $\sigma|_{\{1,\ldots,n-1\}}$ belongs to S_{n-1}, so by the induction hypotheses, it is a product of transpositions (fixing n). Otherwise, $\sigma(n) = m < n$, then $\tau = (m, n)\sigma$ fixes n, so it is a product of transpositions, and so is $\sigma = (m, n)\tau$. □

  The signature of any transposition is -1. Therefore, for any $\sigma \in S_n$, $\sigma \in A_n$ if and only if σ is a product of an even number of transpositions.

Given any group G and a subgroup $H \leq G$, the following relation between elements of G is defined: $x \sim y$ if there exists $h \in H$ such that $x = yh$ (that is, if $y^{-1}x \in H$). This is clearly an equivalence relation, and the equivalence class of any $x \in G$ is $xH = \{xh : h \in H\}$, which has cardinal $|H|$. The quotient set (that is, the set of the equivalence classes) is denoted by G/H and its cardinal is called the *index* of H and denoted by $[G : H]$. Thus $|G| = [G : H]|H|$ (there are $[G : H]$ equivalence classes, all of them of cardinal $|H|$).

Normal groups play the role of ideals for rings. As for them:

E.6 Proposition. *Let G be a group and N a normal subgroup, then the map*

$$\begin{aligned} G/N \times G/N &\longrightarrow G/N \\ (xN, yN) &\mapsto xyN \end{aligned}$$

is well defined and makes G/N a group, which is called the quotient group *of G by N.*

E.7 Properties. *(With essentially the same proof as for rings.)*

- ***First Isomorphism Theorem:*** *Let $f : G \to K$ be a homomorphism of groups, then the quotient group $G/\ker f$ is isomorphic to $\operatorname{im} f$ through the isomorphism*

$$\begin{aligned} \bar{f} : G/\ker f &\to \operatorname{im} f \\ x \ker f &\mapsto f(x). \end{aligned}$$

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

- ***Second Isomorphism Theorem:*** *Let H be a subgroup and N a normal subgroup of the group G, then $HN = \{hn : h \in H, n \in N\}$ is a subgroup of G, $H \cap N$ is a normal subgroup of H and the map*

$$\begin{aligned} H/H \cap N &\to HN/N \\ x(H \cap N) &\mapsto xN, \end{aligned}$$

  is an isomorphism.

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

- *Let N be a normal subgroup of the group G, then the maps*

$$\begin{aligned} \{\textit{subgroups of } G \textit{ containing } N\} &\to \{\textit{subgroups of } G/N\} \\ H &\mapsto H/N, \end{aligned}$$

is a bijection, and the same happens if we consider only normal subgroups.

E.8 Example. For $n \geq 2$, $\operatorname{sgn} : S_n \to \{\pm 1\}$ is an epimorphism with kernel A_n, so that $S_n/A_n \cong \{\pm 1\}$. Hence $[S_n : A_n] = 2$ and $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

E.9 Definition. Let F be a field.

- If K/F is a field extension, the group

$$\begin{aligned} \operatorname{Gal}(K/F) = \{f : K \to K : \\ f \text{ automorphism such that } f(a) = a \ \forall a \in F\} \end{aligned}$$

(the set of automorphisms that fix the elements of F) is called the *Galois group* of the extension.

- For $0 \neq p(X) \in F[X]$, let K be a splitting field of $p(X)$ over F. Then $\operatorname{Gal}(K/F)$ is called the *Galois group* of $p(X)$.

Let $p(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in F[X]$, let K be a splitting field of $p(X)$ over F and let $\alpha \in K$ be a root of $p(X)$, so $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. For any $f \in \operatorname{Gal}(K/F)$, $f(a_i) = a_i$ for any $i = 0, \ldots, n-1$ and, therefore,

$$0 = f(0) = a_0 + a_1 f(\alpha) + \cdots + a_{n-1} f(\alpha)^{n-1} + f(\alpha)^n,$$

that is, $f(\alpha)$ is another root of $p(X)$ in K. Hence, f induces a permutation of the roots of $p(X)$. Moreover, if $\alpha_1, \ldots, \alpha_r \in K$ are the different roots of $p(X)$, the map

$$\begin{aligned} \operatorname{Gal}(K/F) &\longrightarrow S_r \\ f &\mapsto \sigma_f \text{ such that } \sigma_f(i) = j \text{ if } f(\alpha_i) = \alpha_j, \end{aligned}$$

is a monomorphism of groups, because any $f \in \operatorname{Gal}(K/F)$ is determined by its action on $\{\alpha_1, \ldots, \alpha_r\}$ as $K = F(\alpha_1, \ldots, \alpha_r)$. In particular, we conclude that $\operatorname{Gal}(K/F)$ is finite and its order is $\leq r!$.

Many properties of the polynomial $p(X)$ (its solubility by radicals, for instance) depend on its Galois group. Therefore, in order to continue the study of polynomials and field extensions, it is necessary first to study Group Theory. But this is the subject of another course.

Previous exams

Here are some previous exams of the same subject (and by the same lecturer).

June 2003

1. An integral domain R is said to be *almost euclidean* if there is a map $f : R \to \mathbb{Z}_{\geq 0}$ such that

   (a) $f(0) = 0$, $f(a) > 0$ if $a \neq 0$,

   (b) If $b \neq 0$ then $f(ab) \geq f(a)$ $\forall a \in R$,

   (c) $\forall a, b \in R$, if $b \neq 0$ then either a is a multiple of b, or there are $x, y \in R$ such that $0 < f(ax + by) < f(b)$.

   Show that any almost euclidean integral domain is a principal ideal domain.

2. Prove that if $m \in \mathbb{N}$ and $2^m + 1$ is prime, then m is a power of 2 (in this case $2^m + 1$ is called a *Fermat prime*).
   Show that $2^{11} \equiv 5^3 \pmod{641}$, $5^4 \equiv -2^4 \pmod{641}$ and, without actually computing $2^{2^5} + 1$, check that $2^{2^5} + 1$ is a multiple of 641.

3. Consider the following polynomials in $\mathbb{F}_7[X]$ ($\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$): $p(X) = X^4 + 5X^3 + 6X^2 + 5X + 1$ and $q(X) = X^4 + 1$. Find their greatest common divisor $d(X)$, as well as polynomials $a(X), b(X) \in \mathbb{F}_7[X]$ such that $a(X)p(X) + b(X)q(X) = d(X)$.

4. Prove that the polynomial $f(X) = X^5 - 2 \in \mathbb{Q}[X]$ is irreducible. Let K be a splitting field of $f(X)$ over $\mathbb{Q}$, compute the degree $[K : \mathbb{Q}]$.

[2] -1 is a root of $X^{2a+1} + 1$, so $X + 1$ is a factor of $X^{2a+1} + 1$.

July 2003

The value of the first question is twice the value of each of the second and third questions.

1. Prove the following assertions:
   (a) $\mathbb{Z}[\sqrt{-2}]$ is an euclidean domain.
   (b) $\mathbb{Z}[\sqrt{-2}]^\times = \{1, -1\}$ (set of units).
   (c) $\sqrt{-2}$ is an irreducible element of $\mathbb{Z}[\sqrt{-2}]$.
   (d) If $x, y \in \mathbb{Z}$ satisfy $x^2 + 2 = y^3$ then the elements $x + \sqrt{-2}$ and $x - \sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$ are relatively prime.
   (e) With x and y as above, prove that there exists an element $\alpha \in \mathbb{Z}[\sqrt{-2}]$ such that $x + \sqrt{-2} = \alpha^3$.
   (f) Prove that the only solutions in $\mathbb{Z}$ of the equation $x^2 + 2 = y^3$ are given by $x = \pm 5$ and $y = 3$.

2. Prove that $p(X) = X^4 + X^3 + X^2 + X + 1$ is irreducible over the field $\mathbb{F}_2$ of two elements. Let $\alpha = X + (p(X))$ be the class of X in the quotient field $K = \mathbb{F}_2[X]/(p(X))$. Compute the inverse of $\alpha^3 + \alpha + 1$ in K.

3. Find a map $f : \mathbb{Z}^3 \to \mathbb{Z}$ such that $f(x, y, z) \equiv x \pmod 3$, $f(x, y, z) \equiv y \pmod 5$ and $f(x, y, z) \equiv z \pmod 7$ $\forall x, y, z \in \mathbb{Z}$.

[1] Part (f) constitutes one of the many results proved by Fermat.

September 2003

1. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of p elements (p is a prime number).
   (a) How many monic reducible polynomials of degree 2 exist over $\mathbb{F}_p$?
   (b) Conclude that there are irreducible monic polynomials of degree 2 over $\mathbb{F}_p$.
   (c) Construct explicitly a field with 25 elements.

2. For any $n \in \mathbb{N}$ consider the polynomial $X^n - 1 \in \mathbb{Q}[X]$.
   (a) Prove that $X^n - 1$ has no repeated irreducible factors.
   (b) Prove that if d is a divisor of n, then $X^d - 1$ divides $X^n - 1$.
   (c) Show that if $n > m$, then the greatest common divisor of $X^n - 1$ and $X^m - 1$ coincides with the greatest common divisor of $X^{n-m} - 1$ and $X^m - 1$.
   (d) Conclude that for $n, m \in \mathbb{N}$, the greatest common divisor of $X^n - 1$ and $X^m - 1$ is $X^d - 1$, where $d = \gcd(n, m)$.
   (e) Let $p_n(X)$ be the (monic) least common multiple of the polynomials $X^d - 1$, where d runs over the divisors of n, $d \neq n$. Check that $p_n(X)$ divides $X^n - 1$ and consider the quotient $\varphi_n(X) = (X^n - 1)/p_n(X)$. Compute $\varphi_8(X)$ and $\varphi_{10}(X)$.

3. Recall that an element e of a ring R is an *idempotent* if $e^2 = e$. Use the Chinese Remainder Theorem to find 8 idempotent elements in $\mathbb{Z}/385\mathbb{Z}$.

4. Let $\omega = \cos\frac{2\pi}{7} + i \sin\frac{2\pi}{7} \in \mathbb{C}$ (a primitive seventh root of unity)
   (a) Show that $m_{\omega,\mathbb{Q}}(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$. In particular, prove that $\omega^3 + \omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} + \omega^{-3} = 0$.
   (b) Conclude that for $\alpha = \omega + \omega^{-1}$ $\left(= 2\cos\frac{2\pi}{7}\right)$, $m_{\alpha,\mathbb{Q}}(X)$ is a cubic polynomial (degree 3).
   (c) Is it possible to construct with ruler and compass the regular heptagon?

June 2004

1. (a) For any nonzero integers $a, b, c \in \mathbb{Z}$, prove that the equation

$$ax + by = c$$

has an integer solution if and only if $\gcd(a, b)$ divides c.

(b) Obtain all the integer solutions to the equation

$$6x + 9y = -33.$$

2. Let Δ be the discriminant of a real polynomial $p(X) \in \mathbb{R}[X]$ of degree 4 and assume that $\Delta \neq 0$. Prove that if all the roots of $p(X)$ are real, then $\Delta > 0$, while if only two of them are real then $\Delta < 0$. (Note that if $p(\alpha) = 0$, then $p(\bar{\alpha}) = 0$ too.)

3. Let $\mathbb{F}_p$ be the field of p elements (p a prime number) and let $K/\mathbb{F}_p$ be a field extension of degree 2. Prove that for any $b, c \in \mathbb{F}_p$, the polynomial $f(X) = X^2 + bX + c$ has a root in K.

4. Consider the quotient rings $R_2 = \mathbb{Z}[i]/(2)$ and $R_3 = \mathbb{Z}[i]/(3)$.

(a) How many elements do the rings R_2 and R_3 contain?

(b) Is any of them a field?

July 2004

1. Are there integers x, y such that $3145x + 23001y = 85$?

2. Let a, n be natural numbers with $\gcd(a, n) = 1$. Prove that the integers $0, a, 2a, 3a, \ldots, (n-1)a$ form a complete set of representatives of the congruence classes modulo n.

3. Does the class of the polynomial $X^3 + 3X + 1$ in $\mathbb{R}[X]/(X^4 + 1)$ have an inverse? If so, compute it.

4. Let $p \in \mathbb{N}$ be a prime number.

   (a) Show that quotient rings $\mathbb{Z}[i]/(p)$ and $\mathbb{F}_p[X]/(X^2+1)$ are isomorphic.

   (b) Deduce that p is irreducible in $\mathbb{Z}[i]$ if and only if there is no natural number m such that $m^2 \equiv -1 (\text{mod } p)$.

September 2004

1. Cakes are sold in boxes that may contain 3 or 7 of them. If only full boxes are sold, prove that you can buy any amount of cakes greater than 11.

2. (a) Prove that if $n \equiv 3 (\text{mod } 4)$, then there are no integer solutions to the equation $x^2 + y^2 = n$.
   (b) Deduce that any prime number p that is congruent to 3 modulo 4 remains prime in $\mathbb{Z}[i]$.

3. Find, if possible, two polynomials $f(X), g(X) \in \mathbb{F}_2[X]$ such that
$$(X^3 + 1)f(X) + (X^3 + X^2 + X + 1)g(X) = X^2 + 1.$$

4. Let $p \in \mathbb{N}$ be an odd prime number.
   (a) Prove that $(p-1)! \equiv -1 \,(\text{mod } p)$. (Wilson's Theorem)
   (b) Prove that for any $0 \neq a \in \mathbb{F}_p$, there is a unique $b \in \mathbb{F}_p$ such that $ab = -1$.
   (c) Prove that if there is no $n \in \mathbb{N}$ such that $n^2 \equiv -1 \,(\text{mod } p)$, then $(p-1)! \equiv (-1)^{\frac{p-1}{2}} \,(\text{mod } p)$, while if there exists $n \in \mathbb{N}$ such that $n^2 \equiv -1 \,(\text{mod } p)$, then $(p-1)! \equiv (-1)^{\frac{p-3}{2}} \,(\text{mod } p)$.
   (d) Conclude that p is congruent to 3 modulo 4 if and only if the polynomial $X^2 + 1 \in \mathbb{F}_p[X]$ is irreducible.

June 2005

1. Consider the following subset of $\mathrm{Mat}_2(\mathbb{R})$:

$$R = \left\{ \begin{pmatrix} x & y \\ -2y & x \end{pmatrix} : x, y \in \mathbb{Z} \right\}$$

   (a) Check that R is a subring of $\mathrm{Mat}_2(\mathbb{R})$.

   (b) Prove that R is isomorphic to the ring $\mathbb{Z}[\sqrt{-2}]$ $\big(= \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$, which is a subring of $\mathbb{C}\big)$.

2. Let ρ be an irreducible element of the ring of Gaussian integers $\mathbb{Z}[i]$. Prove that there is a prime natural number p that belongs to (ρ).

3. Let F be a field of characteristic $p > 0$.

   (a) Prove that $f(X) = X^p - X - a$ $(a \in F)$ has no multiple roots (in a splitting field).

   (b) Prove that if α is a root, so is $\alpha + 1$.

4. Let F be a field, $0 \neq p(X) \in F[X]$, and E a splitting field of $p(X)$ over F. Show that $[E : F] \leq (\deg p(x))!$

July 2005

1. Prove that for any natural number n, there is a prime p that divides $4n+3$ and is congruent to 3 modulo 4.

2. If $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 - 1$, then prove that:
   (a) $\gcd(y+i, y-i) = 1$ (in $\mathbb{Z}[i]$),
   (b) there exists a Gaussian integer $\alpha \in \mathbb{Z}[i]$ such that $y + i = \alpha^3$,
   (c) $x = 1$, $y = 0$.

3. Consider the polynomial $f(X) = X^3 - X^2 + X + 2 \in \mathbb{Q}[X]$.
   (a) Check that $f(X)$ is irreducible.
   (b) Let $\theta = X + \big(f(X)\big) \in \mathbb{Q}[X]/\big(f(X)\big)$. Express the elements $(\theta^2 + \theta + 1)(\theta^2 - 1)$ and $(\theta - 1)^{-1}$ in the form $a + b\theta + c\theta^2$, with $a, b, c, \in \mathbb{Q}$.

4. Let F be a field and $0 \neq f(X) \in F[X]$ a monic irreducible polynomial. Prove that the following statements are equivalent:
   (a) $f(X)$ has a multiple root (in an algebraic closure),
   (b) $\gcd(f, f') \neq 1$,
   (c) $f'(X) = 0$,
   (d) F has characteristic $p > 0$ and $f(X)$ is a polynomial in X^p,
   (e) all the roots of $f(X)$ are multiple.

September 2005

1. Given any $n \in \mathbb{Z}$, prove that $\gcd(12n+5, 5n+2) = 1$.

2. Let $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X]$ be a monic irreducible polynomial, let $\alpha \in \mathbb{C}$ be a root of $f(X)$, and let $\mathbb{Z}[\alpha] = \{g(\alpha) : g(X) \in \mathbb{Z}[X]\}$.

   (a) Prove that $\mathbb{Z}[\alpha]$ is a subring of $\mathbb{C}$.

   (b) Let p be a prime natural number and let $\bar{a}$ denote the class of a modulo p ($\bar{a} = a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$). Consider the polynomial $\bar{f}(X) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_{n-1}X^{n-1} + X^n \in \mathbb{F}_p[X]$. Prove that

   $$\mathbb{Z}[\alpha]/(p) \cong \mathbb{F}_p[X]/\big(\bar{f}(X)\big)\,.$$

3. Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial of degree 3, and let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ be its roots. Consider the splitting field of $f(X)$ over $\mathbb{Q}$: $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

   (a) Check that $E = \mathbb{Q}(\alpha_1, \alpha_2)$.

   (b) Prove that $[E : \mathbb{Q}]$ is either 3 or 6.

   (c) Prove that if the discriminant of $f(X)$ is not a square in $\mathbb{Q}$, then $[E : \mathbb{Q}] = 6$.

4. Obtain the factorization into irreducible polynomials of $X^4 + 22 \in \mathbb{F}_{23}[X]$.

June 2006

1. (a) Find the roots of the polynomial $X^2 - 5$ over the field of 11 elements $\mathbb{F}_{11}$.
   (b) Find a maximal ideal of $\mathbb{Z}[X]$ containing 11 and $X^2 - 5$.

2. Let F be a field.
   (a) Prove that the ideal (X, Y) of the ring of polynomials $F[X, Y]$ is not principal.
   (b) Show that the ideal (Y) is prime.

3. Show that the polynomial $X^4 - 2 \in \mathbb{F}_5[X]$ is irreducible.

4. Consider the polynomial $f(X) = X^3 + X + 1 \in \mathbb{F}_3[X]$, and let K be the splitting field of $f(X)$ over $\mathbb{F}_3$.
   (a) Compute the degree $[K : \mathbb{F}_3]$.
   (b) Find an element $\gamma \in K$ such that $\gamma^8 = 1$, but $\gamma^i \neq 1$ for $i = 1, \ldots, 7$.

June 2007

1. (a) Show that there exists a unique ring homomorphism $\varphi : \mathbb{Z}[X] \to \mathrm{Mat}_3(\mathbb{Z})$, such that
$$\varphi(X) = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 2 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$
   (b) Compute its kernel.

2. Consider the quotient ring $R = \mathbb{Z}[X]/(15, X^2 - 3)$.
   (a) How many elements does R have?
   (b) How many maximal ideals does R have?

3. Consider the rational polynomial $p(X) = X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$.
   (a) Prove that $p(X)$ is irreducible.
   (b) Show that there is a splitting field K of $p(X)$ contained in $\mathbb{R}$.
   (c) Prove that the degree $[K : \mathbb{Q}]$ is 4.

4. Prove the following generalization of Gauss Lemma: Let R be a unital commutative ring and denote by $C\big(p(X)\big)$ the ideal generated by the coefficients of any polynomial $p(X) \in R[X]$. If $f(X), g(X) \in R[X]$ are polynomials with $C\big(f(X)\big) = R = C\big(g(X)\big)$, then $C\big(f(X)g(X)\big) = R$ too.

[4] Otherwise, there would exist a maximal ideal M of R containing $C\big(f(X)g(X)\big)$.

June 2008

1. (a) Devise a procedure to compute two natural numbers, assuming that you know their sum and their least common multiple.
   (b) Apply your procedure to the case in which the sum is 2761 and the least common multiple is 6024.

2. Consider the ring $\mathbb{Z}[\sqrt{5}]$ (a subring of $\mathbb{R}$), with the norm given by $N(a+b\sqrt{5}) = |a^2 - 5b^2|$, for any $a, b \in \mathbb{Z}$.
   (a) Are there elements of norm 2?
   (b) Check that $1+\sqrt{5}$ and 2 are not associates and that $N(1+\sqrt{5}) = N(2)$.
   (c) Prove that $\mathbb{Z}[\sqrt{5}]$ is not a unique factorization domain.

3. Let I be an ideal of a unital commutative ring, and let $\sqrt{I} = \{a \in R : \exists n \in \mathbb{N} \text{ such that } a^n \in I\}$.
   (a) Show that $\sqrt{I}$ is an ideal of R.
   (b) Show that $R/\sqrt{I}$ has no nilpotent elements.
   (c) Show that $\sqrt{I}$ is the intersection of the prime ideals of R containing I.

4. (a) Show that the polynomial $p(X) = X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ is irreducible.
   (b) Prove that $K = \mathbb{F}_2[X]/(X^3 + X^2 + 1)$ is, up to isomorphism, the unique field with eight elements.
   (c) In this unique field, find an element whose minimal polynomial over $\mathbb{F}_2$ is $X^3 + X + 1$.

September 2008

1. Can you find examples of ideals I in a unital commutative ring R with the following properties?
   (a) I is principal and not maximal.
   (b) I is maximal and not principal.
   (c) I is principal and not prime.
   (d) I is prime and not principal.
   (e) I is maximal and not prime.
   (f) I is prime and not maximal.
   (g) I is principal and prime but not maximal.

2. (a) Factor the polynomial $X^5 - 1$ into a product of irreducible polynomials in $\mathbb{Q}[X]$. Check that your factors are indeed irreducible.
   (b) How many maximal ideals does the ring $\mathbb{Q}[X]/(X^5 - 1)$ have? And $\mathbb{R}[X]/(X^5 - 1)$?

3. (a) For what values of $a \in \mathbb{F}_5$ is the ring $R = \mathbb{F}_5[X]/(X^2 + aX + 1)$ a field?
   (b) How many zero divisors does the ring R contain for $a = 0$?

4. (a) Prove that the element $XY - Z^2 \in \mathbb{Q}[X, Y, Z]$ is irreducible.
   (b) Show that the quotient ring $R = \mathbb{Q}[X, Y, Z]/(XY - Z^2)$ is an integral domain, and that any element is uniquely the class, modulo $(XY - Z^2)$, of an element of the form $f(X, Y) + g(X, Y)Z$, for some $f(X, Y), g(X, Y) \in \mathbb{Q}[X, Y]$.
   (c) Prove that the element $X + (XY - Z^2) \in R$ is irreducible but not prime.
   (d) Conclude that R is not a unique factorization domain.

June 2012

1. Which of the following subsets of $n \times n$ matrices form a subring of $\mathrm{Mat}_n(\mathbb{R})$?

   (a) The set of symmetric matrices.

   (b) The set of upper triangular matrices ($a_{ij} = 0$ for $i > j$).

   (c) The matrices whose entries are 0 except possibly in the first column.

   Does any of these subsets form a left or right ideal of $\mathrm{Mat}_n(\mathbb{R})$?

2. How many abelian groups are there, up to isomorphism, of order 56? For all of them write their invariant factors and their elementary divisors.

3. Consider the ring homomorphism $\varphi : \mathbb{F}_3[X] \to \mathbb{Z}[\sqrt{-5}]/(3)$ that takes X to $\sqrt{-5} + (3)$.

   (a) Prove that φ is onto.

   (b) Compute its kernel.

   (c) Use the above to prove that (3) is contained in precisely two maximal ideals M_1 and M_2 of $\mathbb{Z}[\sqrt{-5}]$.

   (d) Check that $M_1 M_2 = (3)$.

4. Let R be a unital ring, and let a, b be two elements in R.

   (a) Prove that if ab is nilpotent, then so is ba.

   (b) Show that if ab is nilpotent, then both $1 - ab$ and $1 - ba$ are invertible.

   (c) Prove that if $1 - ab$ is invertible, then so is $1 - ba$.

September 2012

1. Let R be an integral domain.
   (a) Prove that (X) is a prime ideal of $R[X]$.
   (b) Prove that R is a field if and only if $R[X]$ is a principal ideal domain.

2. The invariant factors of a finitely generated module M over $\mathbb{F}_2[X]$ are $X^4 + X^2 + 1$ and $X^5 + X^4 + X^3 + X^2 + X + 1$.
   (a) What are its elementary divisors?
   (b) If the free rank of M is 0, how many elements are there in M?

3. Given field extensions L/K and K/F and an element $\alpha \in L$:
   (a) What is the relationship between the minimal polynomials of α over K and over F?
   (b) Give an example where these two polynomials coincide and an example where they don't.

4. (a) Construct explicitly the field K of 9 elements as a quotient of $\mathbb{F}_3[X]$.
   (b) Prove that $X^2 + 1$ divides $X^9 - X$ in $\mathbb{F}_3[X]$.
   (c) Prove, in general, that any irreducible polynomial of degree n over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p prime) divides $X^{p^n} - X$.

June 2013

1. Give an example, and justify your choice, of each of the following:
   (a) a unique factorization domain which is not a principal ideal domain,
   (b) an infinite field of characteristic 5.

2. Prove that $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$ (a subring of $\mathbb{C}$) is an euclidean domain with the norm given by

$$N(a + b\sqrt{-2}) = a^2 + 2b^2,$$

   for any $a, b \in \mathbb{Z}$.

3. How many abelian groups of order 36 are there, up to isomorphism? For each of these groups, give its invariant factors and its elementary divisors.

4. Consider the ring of polynomials over the field of 3 elements: $\mathbb{F}_3[X]$.
   (a) Prove that $(X^3 - X + 1)$ is a maximal ideal of $\mathbb{F}_3[X]$.
   (b) How many elements does the field $\mathbb{F}_3[X]/(X^3 - X + 1)$ contain?
   (c) Find the inverse of the class of $X + 1$ modulo $(X^3 - X + 1)$.

[2] Given $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$, show that, in $\mathbb{C}$, $\frac{\alpha}{\beta} = p + q\sqrt{-2}$ for some $p, q \in \mathbb{Q}$. Take the 'quotient' of α and β to be $a + b\sqrt{-2}$ with $a, b \in \mathbb{Z}$ such that $|p - a| \leq \frac{1}{2}$ and $|q - b| \leq \frac{1}{2}$.

September 2013

1. Give an example, and justify your choice, of each of the following:
   (a) an integral domain which is not a unique factorization domain,
   (b) a unital ring with nilpotent elements,
   (c) a field of 8 elements.

2. Give an example of a field extension $K/\mathbb{Q}$ with $[K : \mathbb{Q}] = 327$.
   Is there a field extension $K/\mathbb{R}$ with $[K : \mathbb{R}] = 327$? Why?

3. Let G be an abelian group and let $\pi : G \to \mathbb{Z}$ be a nonzero homomorphism of groups such that its kernel contains exactly 5 elements.
   (a) Prove that G is finitely generated.
   (b) Compute its invariant factors and its free rank.

4. Consider the ring of polynomials over the field of 5 elements: $\mathbb{F}_5[X]$.
   (a) Prove that $(X^2 + 2)$ is a maximal ideal of $\mathbb{F}_5[X]$.
   (b) Let $\theta = X + (X^2 + 2)$ (the class of X modulo our maximal ideal). Compute the minimal polynomial over $\mathbb{F}_5$ of $2\theta + 1$.

June 2014

1. Prove that a unital ring R is an integral domain if and only if there is a monomorphism $\varphi : R \to F$ from R into a field F.

   Give an example of a field containing as subrings both an integral domain which is not a principal ideal domain and a principal ideal domain which is not euclidean.

2. Let G be a finite abelian group and H a subgroup of G such that $|G/H| = 10$ and the elementary divisors of H are $\{2, 2, 2, 3\}$.

   Determine the possibilities for G, up to isomorphism.

3. (a) Show that if p is an odd prime, then $(p-3)! \times 2 \equiv -1 \pmod{p}$.
   (b) Prove that if $a \in \mathbb{Z}$ is not divisible by 3, then $a^7 \equiv a \pmod{63}$.

4. Consider the set

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

   (a) Show that $\overline{\mathbb{Q}}$ is a field. (Prove the necessary auxiliary results.)
   (b) Compute the degree $[\overline{\mathbb{Q}} : \mathbb{Q}]$.
   (c) Prove that any $0 \neq f(X) \in \mathbb{Q}[X]$ splits in $\overline{\mathbb{Q}}$.

September 2014

1. Prove that a finite integral domain is a field. How many elements does it contain?

   Give an example of an infinite field containing both a subfield of 9 elements and a subring which is a euclidean domain but not a field.

2. Consider the set

$$\mathbb{Z}_{(2)} := \left\{ \frac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus 2\mathbb{Z} \right\}.$$

   Prove that $\mathbb{Z}_{(2)}$ is a subring of $\mathbb{Q}$ and that it is a principal ideal domain.

3. Let V be a torsion $\mathbb{Q}[X]$-module and W a submodule such that the elementary divisors of W are $\{X-1, X-1, X-1, X^2+1\}$, while the elementary divisors of V/W are $\{X-1\}$.

   Determine the possibilities for V, up to isomorphism.

4. (a) List the irreducible polynomials in $\mathbb{F}_2[X]$ of degree ≤ 4.
   (b) Take an irreducible polynomial of degree 4 in your list and use it to construct a field of 16 elements.
   (c) Find a basis over $\mathbb{F}_2$ of this field and write the multiplication table of the elements of this basis.

June 2015

1. (a) How many units are there in $\mathbb{Z}_{25}$?
   (b) Is this set of units a subring?
   (c) Is this set of units an abelian group (with the multiplication)?
   (d) If so, compute its invariant factors.

2. (a) Prove that $\mathbb{R}[X]/(X^3 - X^2 + X - 1)$ is isomorphic to $\mathbb{R} \times \mathbb{C}$.
   (b) Deduce that for any $a \in \mathbb{R}$ and for any $z \in \mathbb{C}$ there is a unique real polynomial $f(X)$ of degree at most two such that $f(1) = a$ and $f(i) = z$.

3. Let R be a principal ideal domain, M a finitely generated R-module, p a prime element in R and N a submodule of M. Define M_p by $M_p := \{x \in M : px = 0\}$.
   (a) Prove that M_p is a vector space over the field $R/(p)$ and that its dimension equals the number of elementary divisors of M that are powers of p.
   (b) Prove that the number of elementary divisors of N is less than or equal to the number of elementary divisors of M.

4. Consider the field $\mathbb{F}_4$ of four elements. Find an irreducible polynomial of degree two over $\mathbb{F}_4$ and use it to construct a field with 16 elements.

September 2015

1. Prove that $2 + 3i$ and $5 + 3i$ are relatively prime in $\mathbb{Z}[i]$, and find $u, v \in \mathbb{Z}[i]$ such that $1 = u(2 + 3i) + v(5 + 3i)$.

2. (a) Prove that $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbb{Q}[X]$, but it has two different irreducible factors in $\mathbb{R}[X]$.
   (b) Deduce that $\mathbb{Q}[X]/(X^4 + X^3 + X^2 + X + 1)$ is a field and that $\mathbb{R}[X]/(X^4 + X^3 + X^2 + X + 1)$ is isomorphic to $\mathbb{C} \times \mathbb{C}$.

3. Let M be a finitely generated abelian group (i.e.; $\mathbb{Z}$-module) and let N be a subgroup of M.
   (a) Give an example where $\mathrm{tor}(M) = 0$ but $\mathrm{tor}(M/N) \neq 0$.
   (b) Prove that the free rank of M is the maximum of the ranks of the free submodules of M.
   (c) Prove that the free rank of M/N is less than or equal to the free rank of M.

4. Construct explicitly a field with 121 elements.

June 2017

1. (a) What are the invariant factors and elementary divisors of the abelian group $\mathbb{Z}_8 \times \mathbb{Z}_{28}$?
   (b) How many abelian groups of order 224 are there, up to isomorphism?

2. (a) Define Euclidean domain, principal ideal domain, and unique factorization domain.
   (b) Give examples of a principal ideal domain which is not a Euclidean domain, and of a unique factorization domain which is not a principal ideal domain.
   (c) Is $\mathbb{Z}[\sqrt{-2}]$ a principal ideal domain? Why?

3. (a) Before doing any computation, explain why are there polynomials $f(X) \in \mathbb{R}[X]$ that satisfy the following three conditions:

   $$f(X)-1 \in \big(X^2-2X+1\big),\ f(X)-2 \in \big(X+1\big),\ f(X)-3 \in \big(X^2-9\big).$$

   (b) Find one such polynomial.

4. Consider the real number $\tau = \frac{1+\sqrt{5}}{2}$. Prove the following assertions:
   (a) $\mathbb{Z}[\tau] := \{a + b\tau : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$.
   (b) $\mathbb{Z}[\tau]$ is isomorphic to $\mathbb{Z}[X]/\big(X^2 - X - 1\big)$.
   (c) The ideal of $\mathbb{Z}[\tau]$ generated by 2 is maximal.
   (d) The quotient $\mathbb{Z}[\tau]/\big(2\big)$ is isomorphic to the field of four elements.

September 2017

1. Let R be a principal ideal domain, and let M be an R-module such that $M = Rx \oplus Ry$, where $x, y \in M$ satisfy $\operatorname{ann}(x) = \big(a\big)$, $\operatorname{ann}(y) = \big(b\big)$, with $0 \neq a, b \in R \setminus R^\times$.
   (a) Prove that the number of invariant factors of M is at most 2.
   (b) Give an explicit example with a unique invariant factor.

2. (a) Are the ideals $\big(3\big)$, $\big(2 + \sqrt{-5}\big)$, and $\big(3, 2 + \sqrt{-5}\big)$, of the ring $\mathbb{Z}[\sqrt{-5}]$, prime?
   (b) Is any of these ideals maximal?

3. (a) Prove that $\mathbb{Z}[i]$ (the ring of Gaussian integers) is a Euclidean domain.
   (b) Show that $\mathbb{Q}(i)$ is its field of fractions (up to isomorphism).
   (c) Prove that any irreducible element in $\mathbb{Z}[i]$ has an associate of the form $a + bi$, with $a, b \in \mathbb{Z}_{\geq 0}$.

4. Give examples (and explain why!) of:
   (a) an infinite algebraic field extension,
   (b) a field extension of degree 229,
   (c) a field extension $\mathbb{K}$ of $\mathbb{F}_2$ with $[\mathbb{K} : \mathbb{F}_2] = 3$,
   (d) a non algebraic field extension of $\mathbb{F}_2$.