Ring and module theory

Leandro Vendramin

ABSTRACT. The notes correspond to the bachelor course **Ring and Module Theory** of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences.

CONTENTS

DEPARTMENT OF MATHEMATICS AND DATA SCIENCE, VRIJE UNIVERSITEIT BRUSSEL, PLEINLAAN 2, 1050 BRUSSEL

E-mail address: Leandro.Vendramin@vub.be.

Introduction

The notes correspond to the bachelor course **Ring and Module Theory** of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve two-hour lectures.

The material is somewhat standard. Basic texts on abstract algebra are for example [1], [3] and [4]. Lang's book [5] is also a standard reference, but maybe a little bit more advanced. We based the lectures on the representation theory of finite groups on [7] and [8].

The notes include many exercises, some with full detailed solutions. Mandatory exercises have a green background , while optional ones (bonus exercises) have a yellow background . The notes also include some additional comments. While these are entirely optional, I hope they offer further insight. They are highlighted with a pink background .

We also mention a set of great expository papers written by Keith Conrad. The notes are extremely well-written and are useful at every stage of a mathematical career.

Several of the exercise solutions were written by Silvia Properzi.

Thanks go to Wouter Appelmans, Arne van Antwerpen, Ilaria Colazzo, Luk De Block, Luca Descheemaeker, Carsten Dietzel, Łukas Kubat, Kevin Piterman, Silvia Properzi, Lucas Simons, Senne Trappeniers, Ruben Wellens, and Geoffrey Janssens.

This version was compiled on December 1, 2025 at 14:01. Please send comments and corrections to me at Leandro.Vendramin@vub.be.

§ 1. Rings

The objective of the next five lectures is to extract certain properties inherent to integers and adapt them for broader applications. Initially, we will identify similarities between the ring of integers and the ring of real polynomials, followed by a more in-depth exploration of these specific attributes in more general contexts. A pivotal similarity between integers and real polynomials lies in the existence of the division algorithm. Nevertheless, it is essential to emphasize that $\mathbb{Z}$ and $\mathbb{R}[X]$ are fundamentally distinct entities, like apples and oranges. For instance, in $\mathbb{R}[X]$, the presence of the variable X allows us to utilize formal derivatives (with respect to X), a feature absent in the ring of integers.

1.1. DEFINITION. A **ring** is a non-empty set R with two binary operations, the addition $R \times R \to R$, $(x, y) \mapsto x + y$, and the multiplication $R \times R \to R$, $(x, y) \mapsto xy$, such that the following properties hold:

1) $(R, +)$ is an abelian group.
2) $(xy)z = x(yz)$ for all $x, y, z \in R$.
3) $x(y + z) = xy + xz$ for all $x, y, z \in R$.
4) $(x + y)z = xz + yz$ for all $x, y, z \in R$.
5) There exists $1_R \in R$ such that $x1_R = 1_R x = x$ for all $x \in R$.

Our definition of a ring is that of a ring with identity. In general one writes the identity element 1_R as 1 if there is no risk of confusion.

1.2. DEFINITION. A ring R is said to be **commutative** if $xy = yx$ for all $x, y \in R$.

1.3. EXAMPLE. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings.

Most of the students will have some familiarity with real polynomials from their school days.

1.4. EXAMPLE. The set

$$\mathbb{R}[X] = \left\{ \sum_{i=0}^{n} a_i X^i : n \in \mathbb{Z}_{\geq 0},\ a_0, \ldots, a_n \in \mathbb{R} \right\}$$

of real polynomials in one variable is a commutative ring with the usual operations. For example, if $f(X) = 1 + 5X^3$ and $g(X) = 3X - 2X^3$, then

$$f(X) + g(X) = 1 + 3X + 3X^3,$$
$$f(X)g(X) = 3X - 2X^3 + 15X^4 - 10X^6.$$

Recall that, if

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

and $a_n \neq 0$, then a_n is the **leading coefficient** of $f(X)$ and n is the **degree** of $f(X)$. In this case, we use the notation $n = \deg f(X)$.

More generally, if R is a commutative ring, then $R[X]$ is a commutative ring. This construction allows us to define the polynomial ring $R[X, Y]$ in two commuting variables X and Y and coefficients in R as $R[X, Y] = (R[X])[Y]$. One can also define the ring $R[X_1, \ldots, X_n]$ of polynomials in n commuting variables $X_1, \ldots, X_n$ with coefficients in R as

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

1.5. EXAMPLE. If A is an abelian group, then the set $\text{End}(A)$ of group homomorphisms $A \to A$ is a ring with

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(g(x)), \quad f, g \in \text{End}(A) \text{ and } x \in A.$$

If X is a set, we write $|X|$ to denote the size of X.

1.6. EXERCISE. Let R be a ring. Prove the following facts:
1) $x0 = 0x = 0$ for all $x \in R$.
2) $x(-y) = -xy$ for all $x, y \in R$.
3) If $1 = 0$, then $|R| = 1$.

1.7. EXAMPLE. The real vector space $H(\mathbb{R}) = \{a1 + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ with basis $\{1, i, j, k\}$ is a ring with the multiplication induced by the formulas

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j.$$

As an example, let us perform a calculation in $H(\mathbb{R})$:

$$(1 + i + j)(i + k) = i + k - 1 + ik + ji + jk = i + k - 1 - j - k + i = -1 + 2i - j,$$

as $ik = i(ij) = -j$ and $ji = -k$. This is the ring of real **quaternions**.

1.8. EXAMPLE. Let $n \geq 2$. The abelian group $\mathbb{Z}/n = \{0, 1, \ldots, n-1\}$ of integers modulo n is a ring with the usual multiplication modulo n.

1.9. EXAMPLE. Let $n \geq 1$. The set $M_n(\mathbb{R})$ of real $n \times n$ matrices is a ring with the usual matrix operations. Recall that if $a = (a_{ij})$ and $b = (b_{ij})$, the multiplication ab is given by

$$(ab)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Note that $M_n(\mathbb{R})$ is conmutative if and only if $n = 1$.

Similarly, for any ring R one defines the ring $M_n(R)$ of $n \times n$ matrices with coefficients in R.

1.10. EXAMPLE. Let R and S be rings. Then $R \times S = (\{(r, s) : r \in R, s \in S\}$ is a ring with the operations

$$(r, s) + (r_1, s_1) = (r + r_1, s + s_1), \quad (r, s)(r_1, s_1) = (rr_1, ss_1).$$

The zero of $R \times S$ is $(0_R, 0_S)$ and the unit element of $R \times S$ is $(1_R, 1_S)$. The ring $R \times S$ is known as the **direct product** of R and S.

1.11. DEFINITION. Let R be a ring. A **subring** S of R is a subset S such that $(S, +)$ is a subgroup of $(R, +)$ such that $1 \in S$ and if $x, y \in S$, then $xy \in S$.

For example, $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is a chain of subrings.

1.12. EXAMPLE. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This is known as the ring of **Gauss integers**.

A **square-free** integer is an integer that is divisible by no perfect square other than 1. Some examples: 2, 3, 5, 6, 7, and 10. The numbers 4, 8, 9, and 12 are not square-free.

1.13. EXAMPLE. Let N be a square-free integer. Then $\mathbb{Z}[\sqrt{N}]$ is a subring of $\mathbb{C}$.

If N is a square-free integer, then $a + b\sqrt{N} = c + d\sqrt{N}$ in $\mathbb{Z}[\sqrt{N}]$ if and only if $a = c$ and $b = d$. Why?

1.14. EXAMPLE. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$.

Why in the ring $\mathbb{Q}[\sqrt{2}]$ equality $a + b\sqrt{2} = c + d\sqrt{2}$ implies $a = c$ and $b = d$?

1.15. EXAMPLE. If R is a ring, then the **center**

$$Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$$

is a subring of R.

If S is a subring of a ring R, then the zero-element of S is the zero-element of R, i.e., $0_R = 0_S$. Moreover, the additive inverse of an element $s \in S$ is the additive inverse of s as an element of R.

1.16. EXERCISE.
   1) If S and T are subrings of R, then $S \cap T$ is a subring of R.
   2) If $R_1 \subseteq R_2 \subseteq \cdots$ is a sequence of subrings of R, then $\cup_{i \geq 1} R_i$ is a subring of R.
   3) If S and T are subrings of R such that $S \cup T$ is a subring, then $S \subseteq T$ or $T \subseteq S$.

1.17. DEFINITION. Let R be a ring. An element $x \in R$ is a **unit** if there exists $y \in R$ such that $xy = yx = 1$.

The set $\mathcal{U}(R)$ of units of a ring R form a group with the multiplication. For example, $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ and $\mathcal{U}(\mathbb{Z}/8) = \{1, 3, 5, 7\}$.

1.18. EXERCISE. Compute $\mathcal{U}(\mathbb{R}[X])$.

1.19. DEFINITION. A **division ring** is a ring $R \neq \{0\}$ such that $\mathcal{U}(R) = R \setminus \{0\}$.

The ring $H(\mathbb{R})$ of **real quaternions** is a non-commutative division ring. Find the inverse of an arbitrary element $a1 + bi + cj + dk \in H(\mathbb{R})$.

1.20. DEFINITION. A **field** is a commutative division ring (with $1 \neq 0$).

For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. If p is a prime number, then $\mathbb{Z}/p$ is a field.

1.21. EXERCISE. Prove that $\mathbb{Q}[\sqrt{2}]$ is a field. Find the multiplicative inverse of a non-zero element of the form $x + y\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

More challenging: Prove that

$$\mathbb{Q}[\sqrt[3]{2}] = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} : x, y, z \in \mathbb{Q}\}$$

is a field. What is the inverse of a non-zero element of the form $x + y\sqrt[3]{2} + z\sqrt[3]{4}$?

§ 2. Ideals

2.1. DEFINITION. Let R be a ring. A **left ideal** of R is a subset $I \subseteq R$ such that $(I, +)$ is a subgroup of $(R, +)$ and $RI \subseteq I$, i.e. $ry \in I$ for all $r \in R$ and $y \in I$.

Similarly, one defines **right ideals**, one needs to replace the condition $RI \subseteq I$ by the inclusion $IR \subseteq I$.

2.2. EXAMPLE. Let $R = M_2(\mathbb{R})$. Then

$$I = \left(\begin{array}{cc} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{array} \right) = \left\{ \left(\begin{array}{cc} x & y \\ 0 & 0 \end{array} \right) : x, y \in \mathbb{R} \right\}$$

is a right ideal R that is not a left ideal.

Can you find an example of a left ideal that is not a right ideal?

2.3. DEFINITION. Let R be a ring. An **ideal** of R is a subset that is both a left and a right ideal of R.

If R is a ring, then $\{0\}$ and R are both ideals of R.

2.4. EXERCISE. Let R be a ring.
1) If $\{I_\alpha : \alpha \in \Lambda\}$ is a collection of ideals of R, then $\cap_\alpha I_\alpha$ is an ideal of R.
2) If $I_1 \subseteq I_2 \subseteq \cdots$ is a sequence of ideals of R, then $\cup_{i \geq 1} I_i$ is an ideal of R.

2.5. EXAMPLE. Let $R = \mathbb{R}[X]$. If $f(X) \in R$, then the set

$$(f(X)) = \{f(X)g(X) : g(X) \in R\}$$

of multiples of $f(X)$ is an ideal of R. One can prove that this is the smallest ideal of R containing $f(X)$.

If R is a ring and X is a subset of R, one defines the ideal generated by X as the smallest ideal of R containing X, that is

$$(X) = \bigcap \{I : I \text{ ideal of } R \text{ such that } X \subseteq I\}.$$

One proves that

$$(X) = \left\{ \sum_{i=1}^m r_i x_i s_i : m \in \mathbb{Z}_{\geq 0},\ x_1, \ldots, x_m \in X,\ r_1, \ldots, r_m, s_1, \ldots, s_m \in R \right\},$$

where by convention, the empty sum is equal to zero. If $X = \{x_1, \ldots, x_n\}$ is a finite set, then we write $(X) = (x_1, \ldots, x_n)$.

2.6. EXERCISE. Prove that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 0$.

2.7. EXERCISE. Let $n \geq 2$. Find the ideals of $\mathbb{Z}/n$.

2.8. EXERCISE. Find the ideals of $\mathbb{R}$.

A similar exercise is to find the ideals of any division ring.

2.9. EXERCISE. Let R be a commutative ring. Prove that every ideal of $M_n(R)$ is of the form $M_n(I)$ for some ideal I of R.

2.10. DEFINITION. Let R be a ring and I be an ideal of R. Then I is **principal** if $I = (x)$ for some $x \in R$.

The division algorithm shows that every ideal of $\mathbb{Z}$ is principal, see Exercise 2.6.

The ring $\mathbb{R}[X]$ of real polynomials also has a division algorithm. Given the polynomials $f(X) \in \mathbb{R}[X]$ and $g(X) \in \mathbb{R}[X]$ with $g(X) \neq 0$, there are polynomials $q(X) \in \mathbb{R}[X]$ and $r(X) \in \mathbb{R}[X]$ such that
$$f(X) = q(X)g(X) + r(X),$$
where $r(X) = 0$ or $\deg r(X) < \deg g(X)$.

For example, if $f(X) = 2X^5 - X$ and $g(X) = X^2 + 1$, then
$$f(X) = q(X)g(X) + r(X),$$
where $q(X) = 2X^3 - 2X$ and $r(X) = X$.

2.11. EXERCISE. Prove that every ideal of $\mathbb{R}[X]$ is principal.

If K is a field, there is a division algorithm in the polynomial ring $K[X]$. Then one proves that every ideal of $K[X]$ is principal.

2.12. EXERCISE. Let R be a commutative ring and $x \in R$. Prove that $x \in \mathcal{U}(R)$ if and only if $(x) = R$. What happens if R is non-commutative?

A division ring (and, in particular, a field) has only two ideals.

§ 3. Ring homomorphisms

3.1. DEFINITION. Let R and S be rings. A map $f\colon R \to S$ is a **ring homomorphism** if $f(1) = 1$, $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in R$.

Our definition of a ring is that of a ring with identity. This means that the identity element 1 of a ring R is part of the structure. For that reason, in the definition of a ring homomorphism f one needs $f(1) = 1$.

3.2. EXAMPLE. The map $f\colon \mathbb{Z}/6 \to \mathbb{Z}/6$, $x \mapsto 3x$, satisfies
$$f(xy) = f(x)f(y) \quad \text{and} \quad f(x+y) = f(x) + f(y)$$
for all $x, y \in \mathbb{Z}/6$. However, f is not a ring homomorphism because $f(1) = 3$.

If R is a ring, then the identity map $\mathrm{id}\colon R \to R$, $x \mapsto x$, is a ring homomorphism.

3.3. EXAMPLE. The inclusions $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ are ring homomorphisms.

More generally, if S is a subring of a ring R, then the inclusion map $S \hookrightarrow R$ is a ring homomorphism.

3.4. EXAMPLE. Let R be a ring. The map $\mathbb{Z} \to R$, $k \mapsto k1$, is a ring homomorphism.

3.5. EXAMPLE. Let $x_0 \in \mathbb{R}$. The evaluation map $\mathbb{R}[X] \to \mathbb{R}$, $f \mapsto f(x_0)$, is a ring homomorphism.

The **kernel** of a ring homomorphism $f\colon R \to S$ is the subset
$$\ker f = \{x \in R : f(x) = 0\}.$$
One proves that the kernel of f is an ideal of R. Moreover, recall from group theory that $\ker f = \{0\}$ if and only if f is injective. The image
$$f(R) = \{f(x) : x \in R\}$$

is a subring of S. In general, $f(R)$ is not an ideal of S.

3.6. EXAMPLE. The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[X]$ is a ring homomorphism. Then $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not an ideal of $\mathbb{Z}[X]$.

3.7. EXAMPLE. Let R and S be rings and $R \times S$ be the direct product (see Example 1.10). The map $R \to R \times S$, $r \mapsto (r, 0)$ is an injective ring homomorphism. The map

$$\pi_R \colon R \times S \to R, \quad (r, s) \mapsto r,$$

is a surjective ring homomorphism with $\ker \pi_R = \{(0, s) : s \in S\} = \{0\} \times S$.

3.8. EXAMPLE. The map $\mathbb{C} \to M_2(\mathbb{R})$, $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, is an injective ring homomorphism.

3.9. EXAMPLE. The map $\mathbb{Z}[i] \to \mathbb{Z}/5$, $a + bi \mapsto a + 2b \bmod 5$, is a ring homomorphism with $\ker f = \{a + bi : a + 2b \equiv 0 \bmod 5\}$.

3.10. EXERCISE. There is no ring homomorphism $\mathbb{Z}/6 \to \mathbb{Z}/15$. Why?

3.11. EXERCISE. If $f \colon \mathbb{R}[X] \to \mathbb{R}$ is a ring homomorphism such that the restriction $f|_{\mathbb{R}}$ of f onto $\mathbb{R}$ is the identity, then there exists $x_0 \in \mathbb{R}$ such that f is the evaluation map at x_0.

§ 4. Quotients

Let R be a ring and I be an ideal of R. Then R/I is an abelian group with

$$(x + I) + (y + I) = (x + y) + I$$

and the **canonical map** $R \to R/I$, $x \mapsto x + I$, is a surjective group homomorphism with kernel I. Recall that R/I is the set of cosets $x + I$, where

$$x + I = y + I \Longleftrightarrow x - y \in I.$$

Note that here we only used that I is an additive subgroup of R. We need an ideal to put a ring structure on the set R/I of cosets modulo I. As in the case of the integers, we use the following notation. For $x, y \in R$ we write

$$x \equiv y \bmod I \Longleftrightarrow x - y \in I.$$

How can we put a ring structure on R/I? It makes sense to define a multiplication on R/I so that the canonical map $R \to R/I$ is a surjective ring homomorphism. For that purpose, we define

$$(x + I)(y + I) = (xy) + I.$$

Since I is an ideal of R, this multiplication is well-defined. In fact, let $x + I = x_1 + I$ and $y + I = y_1 + I$. We want to show that $xy + I = x_1 y_1 + I$. Since $x - x_1 \in I$,

$$xy - x_1 y = (x - x_1)y \in I$$

because I is a right ideal. Similarly, since $y - y_1 \in I$, it follows that

$$x_1 y - x_1 y_1 = x_1(y - y_1) \in I,$$

as I is a left ideal. Thus

$$xy - x_1 y_1 = xy - x_1 y + x_1 y - x_1 y_1 = (x - x_1)y + x_1(y - y_1) \in I.$$

4.1. THEOREM. *Let R be a ring and I be an ideal of R. Then R/I with*

$$(x + I) + (y + I) = (x + y) + I, \quad (x + I)(y + I) = (xy) + I,$$

is a ring and the canonical map $R \to R/I$, $x \mapsto x + I$, is a surjective ring homomorphism with kernel I.

We have already seen that multiplication is well-defined. The rest of the proof is left as an exercise. As an example, we show that the left distributive property holds in R/I because it holds in R, that is

$$\begin{aligned}
(x + I)\left((y + I) + (z + I)\right) &= (x + I)(y + z + I) \\
&= x(y + z) + I \\
&= xy + xz + I \\
&= (xy + I)(xz + I) \\
&= (x + I)(y + I) + (x + I)(z + I).
\end{aligned}$$

4.2. EXERCISE. Prove Theorem 4.1.

4.3. EXAMPLE. Let $R = (\mathbb{Z}/3)[X]$ and $I = (2X^2 + X + 2)$ be the ideal of R generated by the polynomial $2X^2 + X + 2$. If $f(X) \in R$, the division algorithm allows us to write

$$f(X) = (2X^2 + X + 2)q(X) + r(X),$$

for some $q(X), r(X) \in R$, where either $r(X) = 0$ or $\deg r(X) < 2$. This means that $r(X) = aX + b$ for some $a, b \in \mathbb{Z}/3$. Note that

$$f(X) \equiv aX + b \bmod (2X^2 + X + 2)$$

for some $a, b \in \mathbb{Z}/3$, so the quotient ring R/I has nine elements. Can you find an expression for the product $(aX + b)(cX + d)$ in R/I?

An **isomorphism** between the rings R and S is a bijective ring homomorphism $R \to S$. If such a homomorphism exists, then R and S are said to be isomorphic, and the notation is $R \simeq S$.

4.4. EXERCISE. Prove that ring isomorphism is an equivalence relation.

As it happens in the case of groups, to understand quotient rings, one has the first isomorphism theorem.

4.5. THEOREM (First isomorphism theorem). *If $f\colon R \to S$ is a ring homomorphism, then $R/\ker f \simeq f(R)$.*

This is somewhat similar to the result one knows from group theory. One needs to show that, if $I = \ker f$, then the map $R/I \to f(R)$, $x + I \mapsto f(x)$, is a well-defined bijective ring homomorphism.

4.6. EXERCISE. Prove Theorem 4.5.

4.7. EXAMPLE. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}$$

with the usual matrix operations. A direct calculation shows that the map $R \to \mathbb{Q}$, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a$, is a surjective ring homomorphism with

$$\ker f = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Q} \right\}.$$

Thus $R/\ker f \simeq \mathbb{Q}$.

4.8. EXAMPLE. We will prove that

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

But before going into the technical proof, let us show how this isomorphism works. Let $f(X) \in \mathbb{R}[X]$. The division algorithm on $\mathbb{R}[X]$ allows us to write

$$f(X) = (X^2 + 1)q(X) + r(X)$$

for some $q(X), r(X) \in \mathbb{R}[X]$, where $r(X) = 0$ or $\deg r(X) < 2$. Thus $r(X) = aX + b$ for some $a, b \in \mathbb{R}$. This implies that

$$f(X) \equiv aX + b \bmod (X^2 + 1).$$

It is quite easy to describe the ring operation of $\mathbb{R}[X]/(X^2 + 1)$. Clearly

$$(aX + b) + (cX + d) \equiv (a + c)X + (b + d) \bmod (X^2 + 1),$$

Since $X^2 \equiv -1 \bmod (X^2 + 1)$,

$$(aX + b)(cX + d) \equiv X(ad + bc) + (bd - ac),$$

which reminds us of the usual multiplication rule of the field of complex numbers. This means that, in practice, this quotient ring looks pretty much like the ring of complex numbers.

Now is time to prove that

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

Let $\varphi \colon \mathbb{R}[X] \to \mathbb{C}$, $f(X) \mapsto f(i)$, be the evaluation map. Then φ is a ring homomorphism. Moreover, φ is surjective, as $\varphi(a + bX) = a + bi$ for all $a, b \in \mathbb{R}$.

We claim that $\ker \varphi = (X^2 + 1)$, the ideal of $\mathbb{R}[X]$ generated by the polynomial $X^2 + 1$. Clearly, every multiple of $X^2 + 1$, that is every polynomial of the form $(X^2 + 1)g(X)$ for some $g(X) \in \mathbb{R}[X]$, belongs to the kernel of φ. Thus $(X^2 + 1) \subseteq \ker \varphi$. Conversely, if $f(X) \in \ker \varphi$, then $f(i) = 0$. Thus

$$f(X) = (X - i)g(X)$$

for some $g(X) \in \mathbb{R}[X]$. Since $f(X) \in \mathbb{R}[X]$, $f(-i) = 0$ and hence $g(-i) = 0$. Thus $X + i$ divides $g(X)$. Therefore

$$f(X) = (X - i)(X + i)h(X) = (X^2 + 1)h(X)$$

for some $h(X) \in \mathbb{R}[X]$. Therefore $f(X) \in (X^2 + 1)$.

By the first isomorphism theorem,

$$\mathbb{R}[X]/\ker \varphi = \mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}.$$

4.9. EXERCISE. Prove that $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[X]/(X^2 + 5)$.

Similarly, if N is a square-free integer, then

$$\mathbb{Z}[\sqrt{N}] \simeq \mathbb{Z}[X]/(X^2 - N).$$

4.10. EXERCISE. Prove the following isomorphisms:
  1) $\mathbb{Z}[X]/(7) \simeq (\mathbb{Z}/7)[X]$.
  2) $\mathbb{Q}[\sqrt{2}] \simeq \mathbb{Q}[X]/(X^2 - 2)$.
  3) $\mathbb{R}[X]/(X^2 - 1) \simeq \mathbb{R} \times \mathbb{R}$.
  4) $\mathbb{Q}[X]/(X - 2) \simeq \mathbb{Q}$.
  5) $\mathbb{R}[X, Y]/(X) \simeq \mathbb{R}[Y]$.

4.11. EXERCISE. Are the rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ isomorphic?

4.12. EXERCISE. Let R be the ring of continuous maps $[0, 2] \to \mathbb{R}$, where the operations are given by

$$(f + g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x)g(x).$$

Prove that the set $I = \{f \in R : f(1) = 0\}$ is an ideal of R and that $R/I \simeq \mathbb{R}$.

4.13. EXERCISE. Let $n \geq 1$. Let R be a ring and I be an ideal of R. Prove that $M_n(I)$ is an ideal of $M_n(R)$ and that

$$M_n(R)/M_n(I) \simeq M_n(R/I).$$

4.14. EXERCISE. Let $R = \mathbb{Z}[\sqrt{10}]$ and $I = (2, \sqrt{10})$. Prove that $R/I \simeq \mathbb{Z}/2$.

Hint: Use the ring homomorphism $\mathbb{Z}[\sqrt{10}] \to \mathbb{Z}/2$, $a + b\sqrt{10} \mapsto a \bmod 2$.

4.15. EXERCISE. Prove that $\mathbb{Z}[i]/(1 + 3i) \simeq \mathbb{Z}/10$.

Hint: Use the ring homomorphism

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[i] \xrightarrow{\pi} \mathbb{Z}[i]/(1 + 3i),$$

where π is the canonical map.

4.16. EXERCISE. Prove that there is no ideal I of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

4.17. EXERCISE. Let $R = (\mathbb{Z}/2)[X]/(X^2 + X + 1)$.
  1) How many elements does R have?
  2) Can you recognize the additive group of R?
  3) Prove that R is a field.

§ 5. The correspondence theorem

Recall that if $f\colon X \to Y$ is a map and $A \subseteq X$ and $B \subseteq Y$ are subsets, then

$$f(A) = \{f(a) : a \in A\}, \quad f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

The following statements are easily proved:

1) $A \subseteq f^{-1}(f(A))$.
2) $A = f^{-1}(f(A))$ if f is injective.
3) $f(f^{-1}(B)) \subseteq B$.
4) $f(f^{-1}(B)) = B$ if f is surjective.

5.1. THEOREM (Correspondence theorem). *Let $f\colon R \to S$ be a surjective ring homomorphism. There exists a bijective correspondence between the set of ideals of R containing $\ker f$ and the set of ideals of S. Moreover, if $f(I) = J$, then $R/I \simeq S/J$.*

SKETCH OF THE PROOF. Let I be an ideal of R containing $\ker f$ and let J be an ideal of S. We need to prove the following facts:

1) $f(I)$ is an ideal of S.
2) $f^{-1}(J)$ is an ideal of R containing $\ker f$.
3) $f(f^{-1}(J)) = J$ and $f^{-1}(f(I)) = I$.
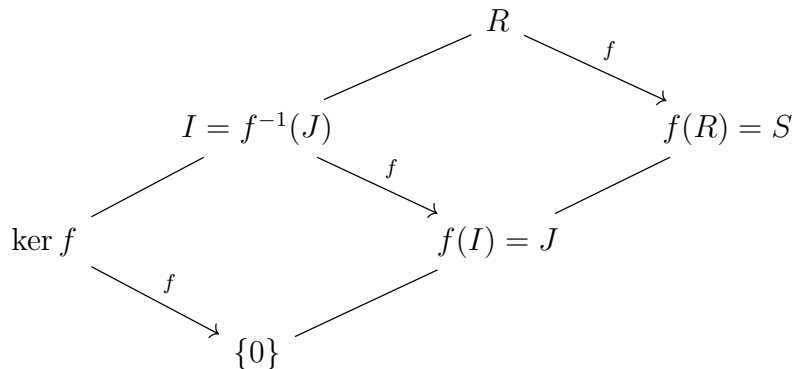**4)** If $f(I) = J$, then $R/I \simeq S/J$.

We only prove the fourth statement, the others are left as exercises. Note that the third claim implies that $f(I) = J$ if and only if $I = f^{-1}(J)$. Let $\pi\colon S \to S/J$ be the canonical map. The composition $g = \pi \circ f\colon R \to S/J$ is a surjective ring homomorphism and

$$\ker g = \{x \in R : g(x) = 0\} = \{x \in R : f(x) \in J\} = \{x \in R : x \in f^{-1}(J) = I\} = I.$$

Then the first isomorphism theorem implies that $R/I \simeq S/J$. $\qquad\square$

5.2. EXERCISE. Prove Theorem 5.1.

As we did for groups, for the correspondence theorem, it helps to have in mind the following diagram:

§ 6. Direct products and direct sums

In Example 1.10, we defined the **direct product** of rings. There is another similar, yet important, construction.

6.1. DEFINITION. Let R be a ring and I and J be ideals of R. We say that $R = I \oplus J$ (that is, R is a **direct sum** of ideals) if $R = I + J$ and $I \cap J = \{0\}$.

6.2. EXERCISE. Let R be a ring and I and J be ideals of R. Prove that $R = I \oplus J$ as a direct sum of ideals if and only if every element $r \in R$ can be written uniquely as $r = u + v$ for $u \in I$ and $v \in J$.

The following exercise illustrates the relationship between decomposing a ring as a direct product of two rings and as a direct sum of two ideals:

6.3. EXERCISE. Let R be a ring. Prove that R admits a decomposition $R = S \times T$ as a direct product of rings if and only if R admits a decomposition $R = I \oplus J$ as a direct sum of ideals.

The constructions in Example 1.10 and Definition 6.1 can be generalized to a finite number of objects. If R is a ring and $I_1, \ldots, I_n$ are ideals of R, we say R is the **direct sum** of the ideals $I_1, \ldots, I_n$, that is

$$R = I_1 \oplus \cdots \oplus I_n,$$

if $R = I_1 + \cdots + I_n$ and for every $i \in \{1, \ldots, n\}$

$$I_i \cap (I_1 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n) = \{0\}.$$

The notation

$$I_1 + \cdots + \widehat{I_i} + \cdots + I_n = I_1 + \cdots + I_{i-1} + I_{i+1} + \cdots + I_n$$

is typically used.

As we did in Exercise 6.2, one can prove that $R = I_1 \oplus \cdots \oplus I_n$ as a direct sum of ideals if and only if every $r \in R$ can be written uniquely as $r = e_1 + \cdots + e_n$ for $e_1 \in I_1, \ldots, e_n \in I_n$. Moreover, R admits a decomposition $R = R_1 \times \cdots \times R_n$ as a direct product of rings if and only if R admits a decomposition $R = I_1 \oplus \cdots \oplus I_n$ as a direct sum of ideals.

§ 7. The Chinese remainder theorem

We now work with commutative rings. If R is a commutative ring and I and J are ideals of R, then

$$I + J = \{u + v : u \in I, \, v \in J\}$$

is an ideal of R. The sum of ideals makes sense also in non-commutative rings.

7.1. DEFINITION. Let R be a commutative ring. The ideals I and J of R are said to be **coprime** if $R = I + J$.

The terminology is motivated by the following example. If I and J are ideals of $\mathbb{Z}$, then $I = (a)$ and $J = (b)$ for some $a, b \in \mathbb{Z}$. Then Bezout's theorem states that

$$a \text{ and } b \text{ are coprime} \iff 1 = ra + sb \text{ for some } r, s \in \mathbb{Z}$$

$$\iff I \text{ and } J \text{ are coprime.}$$

In some books, coprime ideals are called **comaximal** ideals.

If I and J are ideals of R, then

$$IJ = \left\{ \sum_{i=1}^{m} u_i v_i : m \in \mathbb{Z}_{\geq 0}, \, u_1, \ldots, u_m \in I, \, v_1, \ldots, v_m \in J \right\}$$

is an ideal of R. Note that IJ is the set of all finite sum of elements of the form uv for $u \in I$ and $v \in J$. For example, if $I = (u)$ and $J = (v)$, then $IJ = (uv)$. Why we need to consider finite sums of elements of the form uv for $u \in I$ and $v \in J$?

7.2. EXERCISE. Let $R = \mathbb{R}[X, Y]$ and $I = J = (X, Y)$. Prove that the set
$$\{uv : u \in I, \ v \in J\}$$
is not an ideal of R.

Note that $IJ \subseteq I \cap J$. Equality does not hold in general. Take for example $R = \mathbb{Z}$ and $I = J = (2)$. Then $IJ = (4) \subsetneq (2) = I \cap J$.

7.3. PROPOSITION. *Let R be a commutative ring. If I and J are coprime ideals, then $IJ = I \cap J$.*

PROOF. Let $x \in I \cap J$. Since I and J are coprime, $1 = u + v$ for some $u \in I$ and $v \in J$,
$$x = x1 = x(u + v) = xu + xv \in IJ \qquad \square.$$

7.4. BONUS EXERCISE. Let R be a commutative ring. Prove that $I \cap J = IJ$ for all ideals I and J of R if and only if R is **strongly regular**, that is for each $a \in R$ there exists $x \in R$ such that $a = xa^2$.

One can also prove that if R is a ring, $I \cap J = IJ$ holds for all left ideals I and J of R if and only if R is strongly regular.

7.5. THEOREM (Chinese remainder theorem). *Let R be a commutative ring and I and J be coprime ideals of R. If $u, v \in R$, then there exists $x \in R$ such that*
$$\begin{cases} x \equiv u \ \mathrm{mod} \ I, \\ x \equiv v \ \mathrm{mod} \ J. \end{cases}$$

PROOF. Since the ideals I and J are coprime, $1 = a + b$ for some $a \in I$ and $b \in J$. Let $x = av + bu$. Then
$$x - u = av + (b - 1)u = av - au = a(v - u) \in I,$$
that is $x \equiv u \ \mathrm{mod} \ I$. Similarly, $x - v \in J$ and $x \equiv v \ \mathrm{mod} \ J$. $\qquad \square$

For the following result, we need to use the direct product of rings. See Example 1.10.

7.6. COROLLARY. *Let R be a commutative ring. If I and J are coprime ideals of R, then $R/(I \cap J) \simeq R/I \times R/J$.*

PROOF. Let $\pi_I \colon R \to R/I$ and $\pi_J \colon R \to R/J$ be the canonical maps. A direct calculation shows that the map $\varphi \colon R \to R/I \times R/J$, $x \mapsto (\pi_I(x), \pi_J(x))$, is a ring homomorphism with $\ker \varphi = I \cap J$. For example, to prove that
$$\varphi(xy) = \varphi(x)\varphi(y)$$

we proceed as follows: if $x, y \in R$, then

$$\begin{aligned}
\varphi(xy) &= (\pi_I(xy), \pi_J(xy)) \\
&= (\pi_I(x)\pi_I(y), \pi_J(x)\pi_J(y)) \\
&= (\pi_I(x), \pi_J(x))(\pi_I(y), \pi_J(y)) \\
&= \varphi(x)\varphi(y).
\end{aligned}$$

We now claim that the map φ is surjective. To prove this, we will use the Chinese remainder theorem. If $(u + I, v + J) \in R/I \times R/J$, then there exists $x \in R$ such that $x - u \in I$ and $x - v \in J$. This translates into the surjectivity of φ, as

$$\varphi(x) = (\pi_I(x), \pi_J(x)) = (x + I, x + J) = (u + I, v + J).$$

Now $R/(I \cap J) \simeq R/I \times R/J$ by the first isomorphism theorem. $\qquad\square$

7.7. EXAMPLE. If n and m are coprime integers, then

$$\mathbb{Z}/(nm) \simeq \mathbb{Z}/n \times \mathbb{Z}/m$$

as rings. This follows from Corollary 7.6 with $R = \mathbb{Z}$, $I = (n)$ and $J = (m)$.

Let R be a commutative ring and $I_1, \ldots, I_n$ be ideals of R. Then $I_1 \cdots I_n$, defined as the set of all finite sums of the form $x_1 \cdots x_n$ such that $x_j \in I_j$ for all $j \in \{1, \ldots, n\}$, is an ideal of R. For example, if $I_j = (x_j)$ for all $j \in \{1, \ldots, n\}$, then $I_1 \cdots I_j = (x_1 \ldots x_j)$.

If I_1 and I_j are coprime for all $j \in \{2, \ldots, n\}$, then I_1 and $I_2 \cdots I_n$ are coprime. If I_i and I_j are coprime whenever $i \neq j$, then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ and

$$R/(I_1 \cap \cdots \cap I_n) \simeq R/I_1 \times \cdots \times R/I_n.$$

Applying the previous observations in the case of the ring of integers, we get the following result: If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the factorization of n into powers of distinct primes, then

$$\mathbb{Z}/n \simeq \mathbb{Z}/(p_1^{\alpha_1}) \times \cdots \times \mathbb{Z}/(p_k^{\alpha_k})$$

as rings.

7.8. BONUS EXERCISE. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the factorization of n into powers of distinct primes. Prove that $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$, where φ is the Euler φ-function.

The story says that, instead of counting troops, the Chinese generals would order them to assemble in rows of different depths (hence obtaining the remainder of the number of soldiers modulo different integers) and then they would use the theorem to compute the size of the army.

7.9. BONUS EXERCISE. Let us gather people in the following way. When I count by three, there are two people left. When I count by four, there is one person left over and when I count by five there is one missing. How many people are there?

7.10. BONUS EXERCISE. Prove that

$$\begin{cases} x \equiv 29 \bmod 52, \\ x \equiv 19 \bmod 72, \end{cases}$$

does not have a solution.

7.11. BONUS EXERCISE. Find three consecutive integers such that the first one is divisible by a square, the second one is divisible by a cube and the third one is divisible by a fourth power.

7.12. BONUS EXERCISE. Prove that for each $n > 0$ there are n consecutive integers such that each integer is divisible by a perfect square $\neq 1$.

A special application of the Chinese remainder theorem leads to the construction of the Lagrange interpolation polynomial.

7.13. BONUS EXERCISE (Lagrange's interpolation theorem). The Chinese remainder theorem proves the following well-known result. Let $x_1, \ldots, x_k \in \mathbb{R}$ be such that $x_i \neq x_j$ whenever $i \neq j$ and $y_1, \ldots, y_k \in \mathbb{R}$. Then there exists $f(X) \in \mathbb{R}[X]$ such that
$$\begin{cases} f(X) \equiv y_1 \bmod (X - x_1), \\ f(X) \equiv y_2 \bmod (X - x_2), \\ \quad\vdots \\ f(X) \equiv y_k \bmod (X - x_k). \end{cases}$$
The solution $f(X)$ is unique modulo $(X - x_1)(X - x_2)\cdots(X - x_n)$.

With small changes, the Chinese remainder theorem can be proved in arbitrary non-commutative rings, see for example [**4**, Chapter III, Theorem 2.25].

§ 8. Noetherian rings

8.1. DEFINITION. A ring R is said to be **noetherian** if every (increasing) sequence
$$I_1 \subseteq I_2 \subseteq \cdots$$
of ideals of R stabilizes, that is $I_n = I_m$ for some $m \in \mathbb{Z}_{>0}$ and all $n \geq m$.

Finite rings are noetherian. The ring $\mathbb{Z}$ of integers is noetherian. Why?

8.2. EXERCISE. Let $R = \{f \colon [0,1] \to \mathbb{R}\}$ with
$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad f, g \in R,\ x \in [0,1].$$
For $n \in \mathbb{Z}_{>0}$ let $I_n = \{f \in R : f|_{[0,1/n]} = 0\}$. Then each I_n is an ideal of R and the sequence $I_1 \subsetneq I_2 \subsetneq \cdots$ does not stabilize. Thus R is not noetherian.

8.3. DEFINITION. Let R be a ring. An ideal I of R is said to be **finitely generated** if $I = (X)$ for some finite subset X of R.

If R is a ring, $\{0\}$ and R are finitely generated. Why?
If $X = \{x_1, \ldots, x_n\}$ is a subset of a ring R, we write $(x_1, \ldots, x_n)$ to denote the ideal of R generated by the set $\{x_1, \ldots, x_n\}$.

8.4. PROPOSITION. *Let R be a ring. Then R is noetherian if and only if every ideal of R is finitely generated.*

PROOF. Assume first that R is noetherian. Let I be an ideal of R that is not finitely generated. Thus $I \neq \{0\}$. Let $x_1 \in I \setminus \{0\}$ and let $I_1 = (x_1)$. Since I is not finitely generated, $I \neq I_1$ and hence $\{0\} \subsetneq I_1 \subsetneq I$. Let $x_2 \in I \setminus I_1$. Then $I_2 = (x_1, x_2)$ is a finitely generated ideal such that $I_1 \subsetneq I_2 \subsetneq I$. We continue with this procedure. Once I have the ideals $I_1, \ldots, I_{k-1}$, let $x_k \in I \setminus I_{k-1}$ (such an element exists because I_{k-1} is finitely generated and I is not) and $I_k = (I_{k-1}, x_k)$. The sequence $\{0\} \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ does not stabilize.

Assume now that every ideal of R is finitely generated and let $I_1 \subseteq I_2 \subseteq \cdots$ be a sequence of ideals of R. Then $I = \cup_{i \geq 1} I_i$ is an ideal of R, so it is finitely generated, say $I = (x_1, \ldots, x_n)$. We may assume that $x_j \in I_{i_j}$ for all j. Let $N = \max\{j_1, \ldots, j_n\}$. Then $x_j \in I_N$ for all $j \in \{1, \ldots, n\}$ and hence $I \subseteq I_N$. This implies that $I_m = I_N$ for all $m \geq N$. $\qquad\square$

8.5. EXERCISE. Let $R = \mathbb{C}[X_1, X_2, \cdots]$ be the ring of polynomial in an infinite number of commuting variables. Every element of R is a finite sum of the form

$$\sum a_{i_1 i_2 \cdots i_k} X_{i_1}^{n_1} X_{i_2}^{n_2} \cdots X_{i_k}^{n_k}$$

for some non-zero complex numbers $a_{i_1 i_2 \cdots i_k}$. Prove that the ideal $I = (X_1, X_2, \ldots)$ of polynomials with zero constant term is not finitely generated.

The correspondence theorem and the previous proposition allow us to prove easily the following result.

8.6. PROPOSITION. *Let I be an ideal of R. If R is noetherian, then R/I is noetherian.*

PROOF. Let $\pi \colon R \to R/I$ be the canonical surjection and let J be an ideal of R/I. Then $\pi^{-1}(J)$ is an ideal of R containing I. Since R is noetherian, $\pi^{-1}(J)$ is finitely generated, say $\pi^{-1}(J) = (x_1, \ldots, x_k)$ for $x_1, \ldots, x_k \in R$. Thus

$$J = \pi(\pi^{-1}(J)) = (\pi(x_1), \ldots, \pi(x_k)),$$

because π is surjective and hence J is finitely generated. $\qquad\square$

Since $\mathbb{Z}$ is noetherian, $\mathbb{Z}/n$ is noetherian for all $n \geq 2$.

8.7. EXERCISE. Prove that $\mathbb{R}[X]$ is noetherian.

Hint: Use the fact that $\mathbb{R}[X]$ is a principal domain (Exercise 2.11).

8.8. THEOREM (Hilbert). *Let R be a commutative ring. If R is a noetherian ring, then $R[X]$ is noetherian.*

PROOF. We must show that every ideal of $R[X]$ is finitely generated. Assume that there is an ideal I of $R[X]$ that is not finitely generated. In particular, $I \neq \{0\}$. Let $f_1(X) \in I \setminus \{0\}$ be of minimal degree n_1. Since I is not finitely generated, it follows that $I \neq (f_1(X))$. Let $f_2(X) \in I \setminus (f_1(X))$ be of minimal degree n_2. In particular, the minimality of the degree of $f_1(X)$ implies that $n_2 \geq n_1$. We continue with this procedure. For $i > 1$ let $f_i(X) \in I$ be a polynomial of minimal degree n_i such that $f_i(X) \notin (f_1(X), \ldots, f_{i-1}(X))$ (note that such an $f_i(X)$ exists because I is not finitely generated). Moreover, $n_i \geq n_{i-1}$. This happens because if $n_i < n_{i-1}$, then $f_i(X) \notin (f_1(X), \ldots, f_{i-1}(X))$, which contradicts the minimality of $n_{i-1} = \deg f_{i-1}(X)$. For each $i \geq 1$ let a_i be the leading coefficient of $f_i(X)$, that is

$$f_i(X) = a_i X^{n_i} + \cdots,$$

where the dots denote a polynomial of degree $< n_i$. Note that $a_i \neq 0$ for all $i \geq 1$.

Let $J = (a_1, a_2, \dots)$. Since R is noetherian, the sequence

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots (a_1, a_2, \dots, a_k) \subseteq \cdots$$

stabilizes, so we may assume that $J = (a_1, \dots, a_m)$ for some $m \in \mathbb{Z}_{>0}$. In particular, there exist $u_1, \dots, u_m \in R$ such that

$$a_{m+1} = \sum_{i=1}^{m} u_i a_i.$$

Let

$$g(X) = \sum_{i=1}^{m} u_i f_i(X) X^{n_{m+1} - n_i} \in (f_1(X), \dots, f_m(X)) \subseteq I.$$

The leading coefficient of $g(X)$ is $\sum_{i=1}^{m} u_i a_i = a_{m+1}$ and, moreover, the degree of $g(X)$ is n_{m+1}. Thus $\deg(g(X) - f_{m+1}(X)) < n_{m+1}$.

Since $f_{m+1}(X) \notin (f_1(X) \dots, f_m(X))$,

$$g(X) - f_{m+1}(X) \notin (f_1(X), \dots, f_m(X)),$$

a contradiction to the minimality of the degree of f_{m+1}. $\qquad\square$

Since $R[X_1, \dots, X_n] = (R[X_1, \dots, X_{n-1}])[X_n]$, by induction one proves that if R is a commutative noetherian ring, then $R[X_1, \dots, X_n]$ is noetherian.

8.9. EXAMPLE. Let $N > 0$ be a square-free integer. Since $\mathbb{Z}$ is noetherian, so is $\mathbb{Z}[X]$ by Hilbert's theorem. Now $\mathbb{Z}[\sqrt{N}]$ is noetherian, as

$$\mathbb{Z}[\sqrt{N}] \simeq \mathbb{Z}[X]/(X^2 - N)$$

and quotients of noetherian rings are noetherian.

8.10. EXAMPLE. The ring $\mathbb{Z}[X, X^{-1}]$ is noetherian, as

$$\mathbb{Z}[X, X^{-1}] \simeq \mathbb{Z}[X, Y]/(XY - 1).$$

8.11. EXERCISE. Let R be a commutative ring and $R[\![X]\!]$ be the ring of formal power series with the usual operations. Prove that $R[\![X]\!]$ is noetherian if R is noetherian.

8.12. EXERCISE. Let $f \colon R \to R$ be a surjective ring homomorphism. Prove that f is an isomorphism if R is noetherian.

§ 9. Factorization

9.1. DEFINITION. A **domain** is a ring $R \neq \{0\}$ such that $xy = 0$ implies $x = 0$ or $y = 0$. An **integral domain** is a commutative ring that is also a domain.

The rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ are both integral domains. More generally, if N is a square-free integer, then the ring $\mathbb{Z}[\sqrt{N}]$ is an integral domain. The ring $\mathbb{Z}/4$ of integers modulo 4 is not an integral domain.

9.2. EXAMPLE. The ring $\mathbb{Z}/12$ is not a domain. Weird things can happen when we work over these rings. For example, the degree-two $f(X) = X^2 - 4 \in (\mathbb{Z}/12)[X]$ has more than two roots, as $f(2) = f(8) = f(10) = 0$. In fact,

$$f(X) = (X - 2)(X - 10) = (X - 8)(X - 10).$$

The previous example shows why it might be better to work over integral domains.

9.3. DEFINITION. Let R be an integral domain and $x, y \in R$. Then x **divides** y if $y = xz$ for some $z \in R$. Notation: $x \mid y$ if and only if x divides y. If x does not divide y one writes $x \nmid y$.

Note that $x \mid y$ if and only if $(y) \subseteq (x)$.

9.4. DEFINITION. Let R be an integral domain and $x, y \in R$. Then x and y are **associate** in R if $x = yu$ for some $u \in \mathcal{U}(R)$.

Note that x and y are associate if and only if $(x) = (y)$.

9.5. EXAMPLE. The integers 2 and -2 are associate in $\mathbb{Z}$.

9.6. EXAMPLE. Let $R = \mathbb{Z}[i]$.
   1) Let $d \in \mathbb{Z}$ and $a + ib \in R$. Then $d \mid a + ib$ in R if and only if $d \mid a$ and $d \mid b$ in $\mathbb{Z}$.
   2) 2 and $-2i$ are associate in R.

9.7. EXAMPLE. Let $R = \mathbb{R}[X]$ and $f(X) \in R$. Then $f(X)$ and $\lambda f(X)$ are associate in R for all $\lambda \in \mathbb{R}^{\times}$.

9.8. DEFINITION. Let R be an integral domain and $x \in R \setminus \{0\}$. Then x is **irreducible** if and only if $x \notin \mathcal{U}(R)$ and $x = ab$ with $a, b \in R$ implies that $a \in \mathcal{U}(R)$ or $b \in \mathcal{U}(R)$.

Note that $x \in R$ is irreducible if and only if $(x) \neq R$ and there is no principal ideal (y) such that $(x) \subsetneq (y) \subsetneq R$.

9.9. EXAMPLE. Let $R = \mathbb{R}[X]$ and $f(X) \in R \setminus \{0\}$. Then the polynomial $f(X)$ is irreducible if $\lambda \in \mathbb{R}^{\times}$ or $\lambda f(X)$ for $\lambda \in \mathbb{R}^{\times}$ are the only divisors of $f(X)$.

The irreducibles of $\mathbb{Z}$ are the prime numbers. Note that $p \in \mathbb{Z}$ is prime if and only if $p \mid xy$ then $p \mid x$ or $p \mid y$.

9.10. EXAMPLE. The polynomial $X^4 + 1 \in \mathbb{Z}[X]$ is irreducible. If not, since $X^4 + 1$ has no integer roots, there are $a, b, c, d \in \mathbb{Z}$ such that
$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d).$$
This implies that

(9.1)
$$\begin{cases} bd = 1, \\ cb + ad = 0, \\ b + d + ac = 0, \\ a + c = 0. \end{cases}$$

This is a contradiction, as (9.1) has no integer solutions.

If p is a prime number, one can prove that $X^4 + 1 \in (\mathbb{Z}/p)[X]$ is never irreducible. For example $X^4 + 1 = (X^2 + 1)^2$ in $(\mathbb{Z}/2)[X]$.

9.11. DEFINITION. Let R be an integral domain and $p \in R \setminus \{0\}$. Then p is **prime** if $p \notin \mathcal{U}(R)$ and $p \mid xy$ implies that $p \mid x$ or $p \mid y$.

Note that a non-zero element $p \in R$ is prime if and only if $p \neq 0$, $(p) \neq R$ and $xy \in (p)$ implies that $x \in (p)$ or $y \in (p)$.

9.12. PROPOSITION. *Let R be an integral domain and $p \in R$. If p is prime, then p is irreducible.*

PROOF. Let p be a prime. Then $p \neq 0$ and $p \notin \mathcal{U}(R)$. Let x be such that $x \mid p$. Then $p = xy$ for some $y \in R$. In particular, $p \mid xy$. Since p is prime, $p \mid x$ or $p \mid y$. If $p \mid x$, then p and x are associate, that is $p = xu$ for some $u \in \mathcal{U}(R)$. This implies that $xu = p = xy$, so $x(u - y) = 0$. Since $x \neq 0$, $y = u \in \mathcal{U}(R)$. If $p \mid y$, then $y = pz$ for some $z \in R$. Then $y = pz = (xy)z$ and hence $y(1 - xz) = 0$. Since $y \neq 0$, $xz = 1$ and hence $x \in \mathcal{U}(R)$. $\qquad\square$

In $\mathbb{Z}$ primes and irreducible coincide. This does not happen in full generality. To show that there are rings where some irreducibles are not prime, we need the following lemma.

9.13. LEMMA. *Let $N \in \mathbb{Z}$ be a non-zero square-free integer and $R = \mathbb{Z}[\sqrt{N}]$. Then the map*

$$\mathrm{norm} \colon R \to \mathbb{Z}_{\geq 0}, \quad a + b\sqrt{N} \mapsto |a^2 - Nb^2|,$$

satisfies the following properties:
1) $\mathrm{norm}(\alpha) = 0$ *if and only if* $\alpha = 0$.
2) $\mathrm{norm}(\alpha\beta) = \mathrm{norm}(\alpha)\,\mathrm{norm}(\beta)$ *for all* $\alpha, \beta \in R$.
3) $\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{N}])$ *if and only if* $\mathrm{norm}(\alpha) = 1$.
4) *If* $\mathrm{norm}(\alpha)$ *is prime in* $\mathbb{Z}$, *then* α *is irreducible in* R.

PROOF. The first three items are left as exercises. Let us prove 4). If $\alpha = \beta\gamma$ for some $\beta, \gamma \in R$, then $\mathrm{norm}(\alpha) = \mathrm{norm}(\beta)\,\mathrm{norm}(\gamma)$. Since $\mathrm{norm}(\alpha) \in \mathbb{Z}$ is a prime number, it follows that $\mathrm{norm}(\beta) = 1$ or $\mathrm{norm}(\gamma) = 1$. Thus $\beta \in \mathcal{U}(R)$ or $\gamma \in \mathcal{U}(R)$. $\qquad\square$

9.14. EXERCISE. Prove Lemma 9.13.

9.15. BONUS EXERCISE. Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

Hint: You can prove, for example, that $(1 + \sqrt{2})^n \in \mathcal{U}(\mathbb{Z}[\sqrt{2}])$ for all $n \geq 1$.

9.16. EXAMPLE. Let $R = \mathbb{Z}[i]$.
1) $\mathcal{U}(R) = \{-1, 1, i, -i\}$.
2) 3 is irreducible in R. In fact, if $3 = \alpha\beta$, then

$$9 = \mathrm{norm}(\alpha)\,\mathrm{norm}(\beta).$$

Thus $\mathrm{norm}(\alpha) \in \{1, 3, 9\}$. Write $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. If $\mathrm{norm}(\alpha) = 1$, then $\alpha \in \mathcal{U}(R)$ by Lemma 9.13. If $\mathrm{norm}(\alpha) = 9$, then $\mathrm{norm}(\beta) = 1$ and hence $\beta \in \mathcal{U}(R)$ by the lemma. Finally, if $\mathrm{norm}(\alpha) = 3$, then $a^2 + b^2 = 3$, which is a contradiction since $a, b \in \mathbb{Z}$.
3) 2 is not irreducible in R. In fact, $2 = (1 + i)(1 - i)$ and since

$$\mathrm{norm}(1 + i) = \mathrm{norm}(1 - i) = 2,$$

it follows that $1 + i \notin \mathcal{U}(R)$ and $1 - i \notin \mathcal{U}(R)$.

9.17. EXAMPLE. Let $R = \mathbb{Z}[\sqrt{-3}]$ and $x = 1 + \sqrt{-3}$.
1) x is irreducible. If $x = \alpha\beta$ for some $\alpha, \beta \in R$, then

$$4 = \mathrm{norm}(x) = \mathrm{norm}(\alpha)\,\mathrm{norm}(\beta).$$

Thus $\mathrm{norm}(\alpha) \in \{1, 2, 4\}$. Write $\alpha = a + b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$. If $\mathrm{norm}(\alpha) = 1$, then $\alpha \in \mathcal{U}(R)$. If $\mathrm{norm}(\alpha) = a^2 + 3b^2 = 2$, then $b = 0$ and hence $a^2 = 2$, a contradiction. If $\mathrm{norm}(\alpha) = 4$, then $\mathrm{norm}(\beta) = 1$ and $\beta \in \mathcal{U}(R)$.

2) x is not prime. Note that

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 4,$$

then x divides $4 = 2 \cdot 2$. But $1 + \sqrt{-3} \nmid 2$, as

$$(a - 3b) + (a + b)\sqrt{-3} = (1 + \sqrt{-3})(a + b\sqrt{-3}) = 2$$

implies that $a - 3b = 2$ and $a + b = 0$, which yields $a = 1/2 \notin \mathbb{Z}$, a contradiction.

9.18. EXERCISE. Let $R = \mathbb{Z}[\sqrt{-5}]$.
  1) Prove that $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in R.
  2) Prove that $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are not associate in R.

9.19. EXERCISE. Let $R = \mathbb{Z}[\sqrt{5}]$. Prove that $1 + \sqrt{5}$ is irreducible and not prime in R.

9.20. DEFINITION. Let R be an integral domain. Then R is **principal** (or a principal ideal domain) if every ideal I of R is of the form $I = (x)$ for some $x \in R$.

An ideal I of the form $I = (x)$ for some x is called a **principal ideal**.

The rings $\mathbb{Z}$ and $\mathbb{R}[X]$ are both principal.

9.21. EXAMPLE. The ring $\mathbb{Z}[X]$ is not principal. For example, the ideal $I = (2, X)$ is not principal.

First note that $I \neq \mathbb{Z}[X]$. In fact, if $I = \mathbb{Z}[X]$, then $1 = 2f(X) + Xg(X)$ for some polynomials $f(X), g(X) \in \mathbb{Z}[X]$. Then $1 = 2f(0)$, which implies that $-1/2 = f(0) \in \mathbb{Z}$, a contradiction.

If $I = (h(X))$ for some $h(X) \in \mathbb{Z}[X]$, then $2 = h(X)g(X)$ for some $g(X) \in \mathbb{Z}[X]$. This implies that $\deg(h(X)) = 0$, so $h(X) = h(1) \in \mathbb{Z}$. In particular, $2 = h(1)g(1)$ and hence $h(1) \in \{-1, 1, 2, 2\}$. Since $I \neq \mathbb{Z}[X]$, it follows that $h(X) = h(1) \notin \{-1, 1\}$. Now $X = h(X)f(X)$ for some $f(X) \in \mathbb{Z}[X]$. In particular, $\deg(f(X)) = 1$, so we may assume that $f(X) = a_0 + a_1 X$ for $a_0, a_1 \in \mathbb{Z}$ and $a_1 \neq 0$. It follows that

$$X = \pm 2 f(X) = \pm 2(a_0 + a_1 X)$$

and therefore $\pm 1/2 = a_1 \in \mathbb{Z}$, a contradiction.

9.22. EXERCISE. Let R be a principal domain. Prove that R is noetherian.

9.23. EXAMPLE. Let $R = \mathbb{Z}[\sqrt{-5}]$. The ideal $I = (2, 1 + \sqrt{-5})$ is not principal, so R is not principal.

We first note that $I \neq R$. If not, there exist $x, y, u, v \in \mathbb{Z}$ such that

$$1 = 2(x + y\sqrt{-5}) + (1 + \sqrt{-5})(u + v\sqrt{-5}) = (2x + u - 5v) + \sqrt{-5}(2y + u + v).$$

This implies that $1 = 2x + u - 5v$ and $0 = 2y + u + v$. These formulas imply that

$$1 = 2(x + y + u - 2v),$$

a contradiction because $x + y + u - 2v \in \mathbb{Z}$.

Now assume that $I = (\alpha)$ for some α. Then $\alpha \mid 2$ and $\alpha \mid 1 + \sqrt{-5}$. Then $\text{norm}(\alpha) \mid 4$ and $\text{norm}(\alpha) \mid 6$, because $\text{norm}(2) = 4$ and $\text{norm}(1 + \sqrt{-5}) = 6$. Thus $\text{norm}(\alpha) \in \{1, 2\}$. If we write $\alpha = a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$, then it follows that $a^2 + 5b^2 = \text{norm}(\alpha)$. Clearly, $\text{norm}(\alpha) \neq 2$, as $a^2 = 2$ has no solution in $\mathbb{Z}$. Now $\text{norm}(\alpha) = 1$ implies that $\alpha \in \mathcal{U}(R)$ and hence $I = R$, a contradiction.

Sometimes primes and irreducibles coincide.

9.24. PROPOSITION. *Let R be a principal domain and $x \in R$. Then x is irreducible if and only if x is prime.*

PROOF. We only need to prove that if x is irreducible, then x is prime. Let us assume that $x \mid yz$. Let $I = (x, y)$. Since R is principal, $I = (a)$ for some $a \in R$. In particular, $x = ab$ for some $b \in R$. Since x is irreducible, $a \in \mathcal{U}(R)$ or $b \in \mathcal{U}(R)$. If $a \in \mathcal{U}(R)$, then $I = R$ and hence $1 = xr + ys$ for some $r, s \in R$. Thus

$$z = z1 = z(xr + ys) = zxr + zys$$

and therefore $x \mid z$. If $b \in \mathcal{U}(R)$, then x and a are associate in R. Thus $I = (x) = (a)$ and hence $xt = y$ for some $t \in R$, that is $x \mid y$. $\qquad\square$

In the integers primes and irreducible coincide. This happens because $\mathbb{Z}$ is a principal domain.

9.25. EXAMPLE. Since $\mathbb{Z}[\sqrt{-3}]$ have irreducible elements that are not prime, $\mathbb{Z}[\sqrt{-3}]$ is not a principal domain.

9.26. DEFINITION. Let R be an integral domain. We say that R is an **euclidean domain** if there exists a map $\varphi \colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for every $x, y \in R$ with $y \neq 0$ there exist $q, r \in R$ such that $x = qy + r$, where $r = 0$ or $\varphi(r) < \varphi(y)$.

Note that in the definition of euclidean domains, we do not ask for the uniqueness of the quotient and the remainder. In fact, we will meet important examples of euclidean domains where uniqueness in the division algorithm is not achieved.

9.27. EXAMPLE. $\mathbb{Z}$ is a euclidean domain with $\varphi(x) = |x|$.

Do we have uniqueness in the previous example?

9.28. EXAMPLE. $\mathbb{R}[X]$ is a euclidean domain with $\varphi(f(X)) = \deg(f(X))$.

The previous examples suggest why for the definition of a euclidean domain one needs to consider a map $\varphi \colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$.

9.29. EXAMPLE. Let $R = \mathbb{Z}[i]$. Then R is a euclidean domain with $\varphi(a + bi) = a^2 + b^2$. Note that in this case, φ is a multiplicative function in $\mathbb{C}$, that is

$$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$$
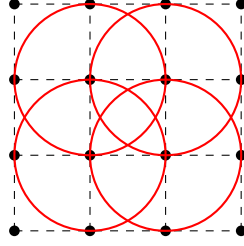
for all $\alpha, \beta \in \mathbb{C}$.

Let $\alpha, \beta \in \mathbb{Z}[i]$ and assume that $\beta \neq 0$. We want to find $\gamma, \delta \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\delta + \gamma, \quad \varphi(\gamma) < \varphi(\beta).$$

So we need to find $\delta \in R$ and $\gamma \in R$ such that

$$\frac{\alpha}{\beta} = \delta + \frac{\gamma}{\beta}, \quad \varphi(\gamma/\beta) < 1.$$

Note that every complex number $z \in \mathbb{C}$ can be written[1] as $z = \xi + \eta$, where $\xi \in \mathbb{Z}[i]$ and $\varphi(\eta) < 1$. In fact, this follows from the fact that $\mathbb{C}$ is covered by open unit disks of radius one and centers $\mathbb{Z}[i]$, see the following figure:

Now let $\alpha = a + ib$ and $\beta = c + id$, where $a, b, c, d \in \mathbb{Z}$. Write

$$\frac{\alpha}{\beta} = \frac{a + ib}{c + id} = r + is$$

for some $r, s \in \mathbb{Q}$. We don't need to compute r and s explicitly! Let $m, n \in \mathbb{Z}$ be such that $|r - m| \leq 1/2$ and $|s - n| \leq 1/2$. If $\delta = m + in$ and $\gamma = \alpha - \beta\delta$, then $\gamma \in R$, $\delta \in R$ and $\alpha = \beta\delta + \gamma$. If $\gamma \neq 0$, then

$$\begin{aligned}
\varphi(\gamma) = \varphi\left(\beta\left(\frac{\alpha}{\beta} - \delta\right)\right) &= \varphi(\beta)\varphi\left(\frac{\alpha}{\beta} - \delta\right) \\
&= \varphi(\beta)\varphi((r - m) + i(s - n)) \\
&= \varphi(\beta)((r - m)^2 + (s - n)^2) \\
&\leq \varphi(\beta)(1/4 + 1/4) \\
&< \varphi(\beta).
\end{aligned}$$

In $\mathbb{Z}[i]$ the division algorithm does not have uniqueness. In fact, if $\alpha, \beta \in \mathbb{Z}[i]$ and $\alpha = \beta\delta + \gamma$ for some $\delta, \gamma \in \mathbb{Z}[i]$, then there are up to four possibilities for the remainder γ.

9.30. EXAMPLE. Let $R = \mathbb{Z}[i]$ and $\alpha = -1 + i$ and $\beta = 1 + 2i$. Let $I = (\beta)$ be the ideal of R generated by β. First, note that

$$I = (\beta) = (1 + 2i)R = (1 + 2i)\mathbb{Z} + (1 + 2i)\mathbb{Z}i = (1 + 2i)\mathbb{Z} + (-2 + i)\mathbb{Z}.$$

This allows us to draw the lattice of elements of I, that is the lattice formed by the multiples of β, see Figure 9.1. Since $\alpha - \gamma \in I = (\beta)$, there are at most four possibilities for writing the division algorithm. In our particular example, we find three possible cases:

1) If $\alpha - \gamma = \beta_0$, where $0 = \beta_0 = \beta 0$, then $\gamma = \alpha = -1 + i$ and

$$-1 + i = (1 + 2i)0 + (-1 + i)$$

with $\text{norm}(-1 + i) = 2 < \text{norm}(\beta) = 5$.
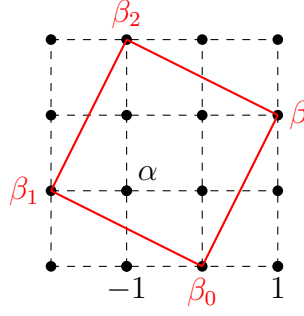
---

[1]For example, the complex number

$$z = \sqrt{2} + \frac{i}{3}$$

can be written as $z = \xi + \eta$, where

$$\xi = 1 + i \in \mathbb{Z}[i], \quad \eta = (\sqrt{2} - 1) + \left(\frac{1}{3} - 1\right)i = (\sqrt{2} - 1) - \frac{2}{3}i.$$

A direct calculation shows that $\varphi(\eta) < 1$.

FIGURE 9.1. Division algorithm in $\mathbb{Z}[i]$.

2) If $\alpha - \gamma = \beta_1$, where $-2 + i = \beta_1 = \beta i$, then $\gamma = 1$ and

$$-1 + i = (1 + 2i)i + 1$$

with $\text{norm}(-1) = 1 < \text{norm}(\beta) = 5$.

3) If $\alpha - \gamma = \beta_2$, where $-1 + 3i = \beta_2 = \beta(1 + i)$, then $\gamma = -2i$ and

$$-1 + i = (1 + 2i)(1 + i) + (-2i)$$

and $\text{norm}(-2i) = 4 < \text{norm}(\beta) = 5$.

We know that $\mathbb{Z}$ and $\mathbb{R}[X]$ are both principal. The proofs are very similar, as both use the division algorithm essentially in the same way. The following result takes advantage of this fact.

9.31. PROPOSITION. *Let R be a euclidean domain. Then R is principal.*

PROOF. Let I be an ideal of R. If $I = \{0\}$, then $I = (0)$ and hence it is principal. So we may assume that $I \neq \{0\}$. Let $y \in I \setminus \{0\}$ be such that $\varphi(y)$ is minimal. We claim that $I = (y)$. If $z \in I$, then $z = yq + r$, where $r = 0$ or $\varphi(r) < \varphi(y)$. The minimality of $\varphi(y)$ implies that $r = 0$. Thus $z = yq \in (y)$ and it follows that $I = (y)$. $\qquad\square$

9.32. EXAMPLE. Since $\mathbb{Z}[i]$ is euclidean, it is principal.

9.33. EXAMPLE. The rings $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-3}]$ are not euclidean. Why?

The ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is an example of a ring that is principal and not euclidean. We will not prove this fact in these notes. For a proof see [**2**], [**11**] or [**10**].

9.34. DEFINITION. Let R be an integral domain. Then R is a **unique factorization domain** if the following statements hold:

1) Each $x \in R \setminus \{0\}$ that is not a unit can be written as $x = c_1 \cdots c_n$ for irreducibles $c_1, \dots, c_n$.
2) If $x = c_1 \cdots c_n = d_1 \cdots d_m$ for irreducibles $c_1, \dots, c_n$ and $d_1, \dots, d_m$, then $n = m$ and there exists $\sigma \in \mathbb{S}_n$ such that c_i and $d_{\sigma(i)}$ are associate for all $i \in \{1, \dots, n\}$.

It is important to remark that some rings have factorizations and this factorization is not unique. In fact, if N is a square-free integer, $\mathbb{Z}[\sqrt{N}]$ is noetherian and hence it has factorization. However, not all these rings admit are unique factorization domains.

25

9.35. EXAMPLE. The ring $R = \mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain. In fact,

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Note that $\operatorname{norm}(a + b\sqrt{-6}) = a^2 + 6b^2 \neq 2$. This implies that 2 is irreducible, as if $2 = \alpha\beta$, then $4 = \operatorname{norm}(2) = \operatorname{norm}(\alpha)\operatorname{norm}(\beta)$. Similarly, 5 is irreducible. It is an exercise to prove that $2 + \sqrt{-6}$ and $2 - \sqrt{-6}$ are both irreducible.

9.36. THEOREM. *Let R be a principal domain. Then R is a unique factorization domain.*

PROOF. We divide the proof into three steps.

CLAIM. R is noetherian.

This is trivial, as every ideal is, in particular, finitely generated by assumption.

CLAIM. R admits factorizations.

Let $x \in R \setminus \{0\}$ be such that $x \notin \mathcal{U}(R)$. If x is irreducible, there is nothing to prove. If not, $x = x_1 x_2$ with $x_1 \notin \mathcal{U}(R)$ and $x_2 \notin \mathcal{U}(R)$. If x_1 and x_2 are both irreducibles, we are done. If not, say x_1 can be written as $x_1 = x_{11} x_{12}$ with $x_{11} \notin \mathcal{U}(R)$ and $x_{12} \notin \mathcal{U}(R)$. If this process does not terminate, it means that there is a sequence of ideals

$$(x) \subsetneq (x_1) \subsetneq (x_{11}) \subsetneq \cdots$$

that does not stabilize, which contradicts the fact that R is noetherian.

CLAIM. R admits unique factorization.

Let $x \in R$ be such that x factorizes into irreducibles as $x = c_1 \cdots c_n = d_1 \cdots d_m$. Note that since R is a principal domain, irreducibles and primes coincide by Proposition 9.24. We may assume that $n \leq m$. We proceed by induction on m. If $m = 1$, then $n = 1$ and $c_1 = d_1$. If $m > 1$, then, since c_1 is prime and $c_1 \mid d_1 \cdots d_m$, it follows that $c_1 \mid d_j$ for some j, say $c_1 \mid d_1$ (here is precisely where the permutation σ appears). Since d_1 is irreducible, c_1 and d_1 are associate, that is $c_1 = u d_1$ for some $u \in \mathcal{U}(R)$. Then

$$c_1 c_2 \cdots c_n = (u d_1) c_2 \cdots c_n = d_1 d_2 \cdots d_m.$$

Since $d_1 \neq 0$,

$$d_1(u c_2 \cdots c_n - d_2 \cdots d_m) = 0,$$

which implies that $(u c_2) \cdots c_n = d_2 \cdots d_m$ because R is an integral domain. Note that $u c_2$ is irreducible and hence the claim follows from the inductive hypothesis. $\square$

It is interesting to remark that the proof of the previous theorem is exactly the proof one does for $\mathbb{Z}$.

9.37. EXAMPLE. The ring $\mathbb{Z}[i]$ is a unique factorization domain.

Let us show that the converse of Theorem 9.36 does not hold.

9.38. EXERCISE. A polynomial $f \in \mathbb{Z}[X]$ is **primitive** if the greatest common divisor of its coefficients is equal to one. Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial. If $f = a f_1$ for some $a \in \mathbb{Z}$ and some primitive polynomial f_1, then $|a|$ is the greatest common divisor of the coefficients of f.

9.39. EXERCISE. Prove the following statements:

1) Let $f, g \in \mathbb{Z}[X]$ be primitive polynomials. Prove that fg is primitive.
2) Let $f \in \mathbb{Z}[X]$ be non-constant. Then f is irreducible in $\mathbb{Z}[X]$ if and only if f is primitive and f is irreducible in $\mathbb{Q}[X]$.

The first item of Exercise 9.39 is known as Gauss' lemma. The second one is Gauss' theorem. These results should be used to prove the following result:

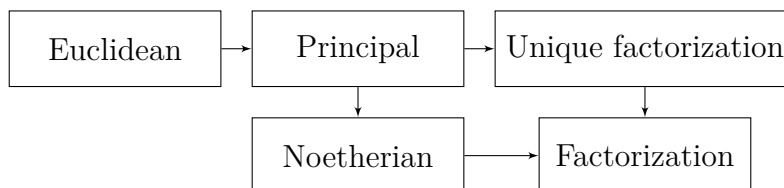9.40. EXERCISE. Prove that $\mathbb{Z}[X]$ is a unique factorization domain.

Finally, the example.

9.41. EXAMPLE. The ring $\mathbb{Z}[X]$ is a unique factorization domain that is not a principal domain.

The same technique could be used to prove that if R is a unique factorization domain, then $R[X]$ is a unique factorization domain, see for example, [**4**, Chapter III, Theorem 6.14].

9.42. EXERCISE. Prove that $\mathbb{R}[X, Y]$ is a unique factorization domain and the ideal $I = (X, Y)$ is not principal.

The following picture shows the relationships between different classes of commutative domains:

We also know that the reverse implications do not hold.

§ 10. Fermat's Christmas theorem

It is time to give a very nice number-theoretical application.

10.1. THEOREM (Fermat). *Let $p \in \mathbb{Z}_{>0}$ be a prime number. The following statements are equivalent:*

1) $p = 2$ *or* $p \equiv 1 \bmod 4$.
2) *There exists $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod p$.*
3) *p is not irreducible in $\mathbb{Z}[i]$.*
4) *$p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.*

PROOF. We first prove that 1) $\implies$ 2). If $p = 2$, take $a = 1$. If $p = 4k + 1$ for some $k \in \mathbb{Z}$, then by Fermat's little theorem, the polynomial $X^{p-1} - 1 \in (\mathbb{Z}/p)[X]$ has roots $1, 2, \ldots, p - 1$. Write

$$(X - 1)(X - 2) \cdots (X - (p - 1)) = X^{p-1} - 1 = X^{4k} - 1 = (X^{2k} + 1)(X^{2k} - 1)$$

in $(\mathbb{Z}/p)[X]$. Since p is prime, $\mathbb{Z}/p$ is a field, and hence $(\mathbb{Z}/p)[X]$ is a unique factorization domain (because it is euclidean). Thus there exists $\alpha \in \mathbb{Z}/p$ such that $\alpha^{2k} + 1 = 0$. To finish the proof take $a = \alpha^k$.

We now prove that 2) $\implies$ 3). If $a^2 \equiv -1 \bmod p$, then $a^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Since $(a - i)(a + i) = a^2 + 1 = kp$, then p divides $(a - i)(a + i)$. Let us prove that p is not prime in $\mathbb{Z}[i]$. We claim that p does not divide $a - i$ in $\mathbb{Z}[i]$. Indeed, if $p \mid a - i$, then $a - i = p(e + fi)$ for some $e, f \in \mathbb{Z}$ and this implies that $1 = pf$, a contradiction. Similarly, p does not divide $a + i$. Thus p is not prime in $\mathbb{Z}[i]$ and hence it is not irreducible in $\mathbb{Z}[i]$ (because in $\mathbb{Z}[i]$ primes and irreducible coincide).

We now prove that 3) $\implies$ 4). If $p = (a + bi)(c + di)$ with $a + bi \notin \mathcal{U}(\mathbb{Z}[i])$ and $c + di \notin \mathcal{U}(\mathbb{Z}[i])$, then

$$p^2 = \text{norm}(p) = \text{norm}(a + bi) \, \text{norm}(c + di) = (a^2 + b^2)(c^2 + d^2)$$

in $\mathbb{Z}$. Since $\mathbb{Z}$ has unique factorization, it follows that $p = a^2 + b^2$.

Finally, we prove that 4) $\implies$ 1). The only possible remainders after division by four are $0, 1, 2$ and 3. For all a, either $a^2 \equiv 0 \bmod 4$ or $a^2 \equiv 1 \bmod 4$. If $p \equiv 3 \bmod 4$, then p is never a sum of two squares, as $a^2 + b^2 \equiv 0 \bmod 4$, $a^2 + b^2 \equiv 1 \bmod 4$ or $a^2 + b^2 \equiv 2 \bmod 4$. $\qquad\square$

An alternative proof of the implication 1) $\implies$ 2) goes as follows: if $p = 4k + 1$ is prime, then $x = (2k)!$ is such that $x^2 \equiv -1 \bmod p$. By Wilson's theorem,

$$(p - 1)! = (4k)! \equiv \bmod p.$$

Moreover,

$$
\begin{aligned}
(4k)! &\equiv (4k)(4k - 1) \cdots (2k + 2)(2k + 1)(2k)(2k - 1) \cdots 1 \bmod p \\
&\equiv -1(-2) \cdots (-2k + 1)(-2k)(2k)(2k - 1) \cdots 1 \bmod p \\
&\equiv (-1)^{2k}(2k)!(2k)! \bmod p.
\end{aligned}
$$

Hence $x = (2k)!$ is such that $x^2 \equiv -1 \bmod p$.

10.2. EXERCISE. Decompose the prime 41 as a sum of two squares.

In 1625, Girard stated without proof a result characterizing which integers can be expressed as the sum of two squares. Later, in a letter to Mersenne dated December 25, Fermat presented several improvements and claimed to have proved the result (this is the "Christmas Letter"). Euler later published the first rigorous proof, explicitly acknowledging Fermat's earlier work.

The previous exercise can be solved by using computers and a beautiful formula of Gauss that uses binomial coefficients. Let $p = 4k + 1$ be a prime number. If

$$a = \left\langle \frac{1}{2}\binom{2k}{k} \right\rangle, \quad b = \langle (2k)! a \rangle,$$

where $\langle x \rangle$ denotes the residue of x modulo p of absolute value smaller than $p/2$, then it follows that $p = a^2 + b^2$. Simple and beautiful as it is, Gauss' formula does not seem to be of any real computational value.

In [9], the author employs the Euclidean algorithm to determine efficiently the decomposition of a prime number $p = 4k + 1$ as the sum of two squares.

10.3. EXERCISE. Let $\alpha \in \mathbb{Z}[i]$ be such that $\text{norm}(\alpha) = p^2$ for some prime number $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$. Prove that α is irreducible.

10.4. EXERCISE. Let $p \in \mathbb{Z}$ be a prime number such that $p \equiv 1 \bmod 4$. Then $p = \alpha\overline{\alpha}$ for some $\alpha \in \mathbb{Z}[i]$ irreducible.

10.5. EXERCISE. Find the irreducible elements of $\mathbb{Z}[i]$.

As a consequence of Theorem 10.1 one can prove the following result: An integer ≥ 2 can be written as a sum of two squares if and only if its prime decomposition contains no factor p^k, where $p \equiv 3 \bmod 4$ and k is odd.

The numbers that can be represented as the sums of two squares form the integer sequence A001481:

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, \dots$$

They form the set of all norms of Gaussian integers.

10.6. BONUS EXERCISE (Eisenstein integers). Let $\omega = e^{2\pi i/3} \in \mathbb{C}$ and

$$R = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}.$$

Prove the following statements:

1) The map

$$N\colon R \to \mathbb{Z}_{\geq 0}, \quad \text{norm}(a + b\omega) = a^2 - ab + b^2,$$

is multiplicative and satisfies $\text{norm}(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in R$.
2) $\mathcal{U}(R) = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.
3) R is a euclidean domain.
4) If $\text{norm}(\alpha)$ is a prime number, then α is irreducible.
5) If $\text{norm}(\alpha) = p^2$ for some prime number p with $p \equiv 2 \bmod 3$, then α is irreducible.
6) If $p \equiv 1 \bmod 3$, then $p = \gamma\overline{\gamma}$ for some irreducible $\gamma \in R$.
7) Up to multiplication by units, the irreducible elements of R are $1 - 2\omega$, $a + b\omega$ with $a^2 - ab + b^2 = p$ and $p \equiv 1 \bmod 3$, and prime numbers $p \in \mathbb{Z}$ with $p \equiv 2 \bmod 3$.

§ 11. Zorn's lemma

11.1. DEFINITION. A non-empty set R is said to be a **partially ordered set** (or **poset**, for short) if there is a subset $X \subseteq R \times R$ such that

1) $(r, r) \in X$ for all $r \in R$,
2) if $(r, s) \in X$ and $(s, t) \in X$, then $(r, t) \in X$, and
3) if $(r, s) \in X$ and $(s, r) \in X$, then $r = s$.

The set X is a partial order relation on R. We will use the following notation: $(r, s) \in X$ if and only if $r \leq s$. Moreover, $r < s$ if and only if $r \leq s$ and $r \neq s$. When we say that R is a poset, we implicitly denote the partial order relation on R by the symbol $\leq$. With this notation, the conditions needed to define a poset are the following:
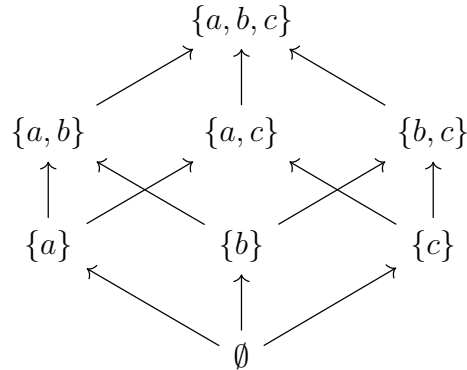
1) $r \leq r$ for all $r \in R$,

2) if $r \leq s$ and $s \leq t$, then $r \leq t$, and
3) if $r \leq s$ and $s \leq r$, then $r = s$.

11.2. DEFINITION. Let R be a poset and $r, s \in R$. Then r and s are **comparable** if either $r \leq s$ or $s \leq r$.

11.3. EXAMPLE. Let $U = \{1, 2, 3, 4, 5\}$ and T be the set of subsets of U. Then T is a poset with the usual inclusion, that is $C \leq D$ if and only if $C \subseteq D$. The subsets $\{1, 2\}$ and $\{3, 4\}$ of U are elements of T that are not comparable.

Is there a good pictorial representation of a poset? A **Hasse diagram** is a common way to represent one. It is a graph in which the vertices represent the elements of the poset. Elements connected by an arrow are comparable, while elements not connected are incomparable. Specifically, if x and y are elements of a poset, we draw an arrow from x to y if and only if $x \neq y$ and there is no element z such that $x < z < y$.

11.4. EXAMPLE. The **Hasse diagram** of the set of all subsets of $\{a, b, c\}$, ordered by inclusion, is the following:

11.5. DEFINITION. Let R be a poset and $r \in R$. Then r is **maximal** in R if $r \leq t$ implies $r = t$.

11.6. EXAMPLE. $\mathbb{Z}$ with the poset structure given by the usual ordering, has no maximal elements.

11.7. EXAMPLE. Let $R = \{(x, y) \in \mathbb{R}^2 : y \leq 0\}$ with $(x_1, y_1) \leq (x_2, y_2)$ if and only if $x_1 = x_2$ and $y_1 \leq y_2$. Then R is a poset and each $(x, 0)$ is maximal. Thus R has infinitely many maximal elements.

11.8. DEFINITION. Let R be a poset and S be a non-empty subset of R. An **upper bound** for S is an element $u \in R$ such that $s \leq u$ for all $s \in S$.

An upper bound for S might not be an element of S.

11.9. EXAMPLE. Let $S = \{6\mathbb{Z}, 12\mathbb{Z}, 24\mathbb{Z}\}$ be a subset of the set X of subgroups of $\mathbb{Z}$ partially ordered by the inclusion. Then $6\mathbb{Z} = 6\mathbb{Z} \cup 12\mathbb{Z} \cup 24\mathbb{Z}$ is an upper bound of the subset S that is not maximal in X.

11.10. EXAMPLE. Let $R = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}\}$ partially ordered with the inclusion, where R is considered as a subset of the power set of $X = \{1, 2, 3\}$. Then $\{3\}$ and $\{1, 2\}$ are maximal elements of R. Moreover, X is an upper bound for R.

11.11. DEFINITION. Let R be a poset. A **chain** is a non-empty subset S of R such that any two elements of S are comparable.

We now state **Zorn's lemma**:

> *Let R be a poset such that every chain in R admits an upper bound in R. Then R contains a maximal element.*

It may not be intuitive[2], but it is logically equivalent to a more intuitive statement in set theory: the **Axiom of Choice**, which states that the Cartesian product of a collection of non-empty sets is non-empty. Zorn's lemma is an axiom, not a lemma. The reason it is called a lemma, rather than an axiom, is purely historical.

11.12. DEFINITION. Let R be a ring. An ideal I of R is said to be **maximal** if $I \neq R$ and if J is an ideal of R such that $I \subseteq J$, then either $I = J$ or $J = R$.

If p is a prime number, then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

11.13. EXERCISE. Let R be a commutative ring. Prove that R is a field if and only if $\{0\}$ is a maximal ideal of R.

11.14. EXERCISE. Let R be a commutative ring and I be an ideal of R. Prove that I is maximal if and only if R/I is a field.

An ideal I of a ring R is said to be **proper** if $I \neq R$.

11.15. THEOREM (Krull). *Let R be a ring. Each proper ideal I of R is contained in a maximal ideal. In particular, all rings have maximal ideals.*

PROOF. Let $X = \{J : J \text{ is an ideal of } R \text{ such that } I \subseteq J \subsetneq R\}$. Since $I \in X$, it follows that X is non-empty. Moreover, X is a poset with respect to inclusion. If C is a chain in X (for example, C could be an increasing sequence

$$I_1 \subseteq I_2 \subseteq \cdots$$

of proper ideals of R containing I), then $\cup_{J \in C} J$ is an upper bound for C, as $\cup_{J \in C} J$ is an ideal and $\cup_{J \in C} J \neq R$ because $1 \notin \cup_{J \in C} J$. Zorn's lemma implies that there exists a maximal element $M \in X$. We claim that M is a maximal ideal of R. The definition of X implies that M is a proper ideal of R that contains I. If M_1 is a proper ideal of R such that $M \subseteq M_1$, it follows that $I \subseteq M_1$ and hence $M_1 \in X$. The maximality of M implies that $M = M_1$. $\square$

In the proof of the previous theorem, we see that it is crucial to consider rings with identity.

11.16. EXERCISE. Compute the maximal ideals of $\mathbb{R}[X]$ and $\mathbb{C}[X]$.

One can also compute the maximal ideals of $K[X]$ for any field K.

11.17. EXERCISE. Let R be a principal domain and $p \in R \setminus \{0\}$. Then p is irreducible if and only if (p) is maximal.

---

[2]The mathematician Jerry L. Bona has a nice joke about Zorn's lemma: *The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?*

11.18. DEFINITION. Let R be a commutative ring. A proper ideal I of R is said to be **prime** if $xy \in I$ implies that $x \in I$ or $y \in I$.

If p is a prime number, then $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

11.19. EXERCISE. Let R be a commutative ring. Prove that an ideal I of R is prime if and only if R/I is a domain.

11.20. EXERCISE. Let R be a commutative ring.

1) Prove that maximal ideals are prime.
2) Let $R = \mathbb{Z}[X]$. Prove that (X) is a prime ideal that is not maximal.
3) Let R be a principal domain. Prove that non-zero prime ideals are maximal.

11.21. EXAMPLE. The ideal $(X^2 + 2X + 2)$ is maximal in $\mathbb{Q}[X]$ because
$$X^2 + 2X + 2 = (X + 1)^2 + 1$$
has degree two and no rational roots. Hence $X^2 + 2X + 2$ is irreducible in $\mathbb{Q}[X]$ and it generates a maximal ideal.

11.22. EXAMPLE. Let $R = (\mathbb{Z}/2)[X]$ and $f(X) = X^2 + X + 1$. Since $f(X)$ is irreducible (because $\deg f(X) = 2$ and $f(X)$ has no roots in $\mathbb{Z}/2$, it follows that $(f(X))$ is a maximal ideal. Thus R/I is a field.

11.23. EXERCISE. Compute the maximal ideals of $\mathbb{Z}/n$.

11.24. EXERCISE. Let R be a commutative ring and $J(R)$ be the intersection of all maximal ideals of R. Prove that $x \in J(R)$ if and only if $1 - xy \in \mathcal{U}(R)$ for all $y \in R$. The ideal $J(R)$ is known as the **Jacobson's radical** of R. Note that $J(R) \neq R$.

We conclude the lecture with a different application of Zorn's lemma.

11.25. BONUS EXERCISE. Prove that every non-zero vector space has a basis.

The previous exercise can be used to solve the following exercises:

11.26. BONUS EXERCISE. Every linearly independent subset of a non-zero vector space V can be extended to a basis of V.

Hint: If X is a linearly independent set, a basis of V that contains X will be found as a maximal linearly independent set containing X.

11.27. BONUS EXERCISE. Let V be a vector space. Prove that every subspace U of V is a direct summand of V, that is $V = U \oplus W$ for some subspace W of V.

11.28. BONUS EXERCISE. Prove that every spanning set of a non-zero vector space contains a basis.

11.29. BONUS EXERCISE. Prove that there exists a group homomorphism $f \colon \mathbb{R} \to \mathbb{R}$ that is not of the form $f(x) = \lambda x$ for some $\lambda \in \mathbb{R}$.

11.30. BONUS EXERCISE. Prove that the abelian groups $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic.

11.31. BONUS EXERCISE. Let G be a group such that $|G| > 2$. Prove that $|\operatorname{Aut}(G)| > 1$.

§ 12. The characteristic of a ring

12.1. DEFINITION. Let R be a ring. If there is a least positive integer n such that $nx = 0$ for all $x \in R$, then R has **characteristic** n, i.e. $\operatorname{char} R = n$. If no such n exists, then R is of characteristic zero.

Easy examples: $\operatorname{char} \mathbb{Z} = 0$ and $\operatorname{char} \mathbb{Z}/n = n$.

12.2. PROPOSITION. *Let R be a ring such that* $\operatorname{char} R = n > 0$,

1) *The map $f \colon \mathbb{Z} \to R$, $m \mapsto m1$, is a ring homomorphism and $\ker f = n\mathbb{Z}$.*
2) *$n = \min\{k \in \mathbb{Z}_{>0} : k1 = 0\}$.*
3) *If R is a domain, then n is a prime number.*

PROOF. We leave 1) as an exercise.
Let us prove 2). Let $n_1 = \min\{k \in \mathbb{Z}_{>0} : k1 = 0\}$. Clearly $n \geq n_1$. For $x \in R$,

$$n_1 x = n_1(1x) = (n_1 1)x = 0x = 0$$

and hence $n_1 \geq n$.
Finally, we prove 3). If n is not prime, say $n = rs$ with $1 < r, s < n$. Then

$$0 = n1 = (rs)1 = (r1)(s1)$$

and hence $r1 = 0$ or $s1 = 0$, a contradiction. $\qquad\square$

12.3. EXERCISE. Let p be a prime number and $R = \mathbb{Z}/p \times \mathbb{Z}/p$ be a ring with the usual point-wise operations. Prove that $\operatorname{char} R = p$ and that R has zero divisors.

12.4. EXERCISE (binomial theorem). Let R be a commutative ring and $n \geq 1$. Prove that if $a, b \in R$, then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

12.5. EXERCISE. Let R be a commutative ring of prime characteristic p.
1) If $x, y \in R$, then $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for all $n \geq 0$.
2) The map $R \to R$, $x \mapsto x^{p^n}$, is a ring homomorphism for all $n \geq 0$.

Hint: Proceed by induction on n and use the fact that the prime number p divides $\binom{p}{k}$ for all $k \in \{1, 2, \ldots, p-1\}$. Alternatively, one could use that the prime number p divides $\binom{p^n}{k}$ for all $k \in \{1, 2, \ldots, p^n - 1\}$.

12.6. BONUS EXERCISE. Let R be a ring and $n \geq 1$. For $a, b \in R$, let $A(x) = (a+b)x - xb$. Prove that if $a, b \in R$, then

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} A^k(1) b^{n-k}.$$

We will dedicate three lectures to the development of the character theory for complex representations of finite groups. Our approach will remain entirely elementary, relying solely on fundamental linear algebra principles over complex numbers.

§ 13. Group algebras

Fix a field K (for example, $K = \mathbb{C}$). For a finite group G, let $K[G]$ be the vector space (over K) with basis $\{g : g \in G\}$. Thus $K[G]$ is a vector space of dimension $\dim K[G] = |G|$. Moreover, $K[G]$ is a ring with

$$\left(\sum_{g \in G} \lambda_g g \right) \left(\sum_{h \in G} \mu_h h \right) = \sum_{g,h \in G} \lambda_g \mu_h (gh).$$

Note that $K[G]$ is commutative if and only if G is abelian.

13.1. EXAMPLE. Let

$$\mathbb{S}_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$$

the symmetric group in three letters. Every element of $\mathbb{C}[\mathbb{S}_3]$ is of the form

$$a\,\mathrm{id} + b(12) + c(13) + d(23) + e(123) + f(132)$$

for some $a, b, c, d, e, f \in \mathbb{C}$. For example,

$$\alpha = 5\,\mathrm{id} + 3(123) \quad \text{and} \quad \beta = -4\,\mathrm{id} + (132)$$

are elements of $\mathbb{C}[\mathbb{S}_3]$. We compute

$$\alpha + \beta = 1\,\mathrm{id} + 3(123) + (132)$$

and

$$\begin{aligned}
\alpha\beta &= (5\,\mathrm{id} + 3(123))(-4\,\mathrm{id} + (132)) \\
&= -20\,\mathrm{id} + 5(132) - 12(123) + 3(123)(132) \\
&= -20\,\mathrm{id} + 5(132) - 12(123) + 3\,\mathrm{id} \\
&= -17\,\mathrm{id} + 5(132) - 12(123).
\end{aligned}$$

Another example:

$$\begin{aligned}
(\mathrm{id} + 5(13))(2\,\mathrm{id} - (12)) &= 2\,\mathrm{id} - (12) + 10(13) - 5(13)(12) \\
&= 2\,\mathrm{id} - (12) + 10(13) - 5(123),
\end{aligned}$$

as $(13)(12) = (123)$.

Note that $K[G]$ is a ring and also a vector space (over K) and these structures are somewhat compatible, as the formulas

$$(\lambda a + \mu b)c = \lambda(ac) + \mu(bc), \quad a(\lambda b + \mu c) = \lambda(ab) + \mu(ac)$$

hold for all $\lambda, \mu \in K$ and $a, b, c \in K[G]$.

13.2. DEFINITION. Let A be a ring and K be a field. Then A is a K-**algebra** (or an **algebra** over the field K) if A is a vector space (over K) such that $\lambda(ab) = (\lambda a)b = a(\lambda b)$ for all $\lambda \in K$ and $a, b \in A$.

The fields $\mathbb{R}$ and $\mathbb{C}$ are examples of $\mathbb{R}$-algebras. Other examples of $\mathbb{R}$-algebras are the polynomial rings $\mathbb{R}[X]$ and $\mathbb{R}[X, Y]$ and the matrix rings $M_n(\mathbb{R})$.

13.3. EXAMPLE. If A is an algebra, then $M_n(A)$ is an algebra.

13.4. EXAMPLE. Let G be a finite group and K be a field. Then $K[G]$ is a K-algebra.

13.5. EXAMPLE. Let $G = \langle g : g^3 = 1 \rangle = \{1, g, g^2\} \simeq C_3$ be the cyclic group of order three. If $\alpha = a_1 1 +_2 g + a_3 g^2$ and $\beta = b_1 1 + b_2 g + b_3 g^2$, then

$$\alpha\beta = (a_1 b_1 + a_2 b_3 + a_3 b_2)1 + (a_1 b_2 + a_2 b_1 + a_3 b_3)g + a_1 b_3 + a_2 b_2 + a_3 b_1)g^2.$$

One can check that $\mathbb{C}[G] \simeq \mathbb{C}[X]/(X^3 - 1)$.

In general, one proves that the group algebra of C_n, the cyclic group of order $n \geq 2$, is isomorphic to $\mathbb{C}[X]/(X^n - 1)$.

13.6. EXERCISE. Prove that $\mathbb{R}[C_3] \simeq \mathbb{R} \times \mathbb{C}$.

13.7. EXERCISE. Let $G = \{1, g\} \simeq C_2$ be the cyclic group of order two. The product of $\mathbb{C}[G]$ is

$$(a1 + bg)(c1 + gd) = (ac + bd)1 + (ad + bc)g.$$

Prove that the map

$$\mathbb{C}[G] \to \mathbb{C} \times \mathbb{C}, \quad a1 + bg \mapsto (a + b, a - b),$$

is a linear isomorphism of rings.

13.8. EXERCISE. Let $K = \mathbb{Z}/2$ and $G = \{1, g\} \simeq C_2$ be the cyclic group of order two. Prove that the map

$$K[G] \to \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}, \quad a1 + bg \mapsto \begin{pmatrix} a+b & b \\ 0 & a+b \end{pmatrix},$$

is a linear isomorphism of rings.

The group ring has the following property, which is left as an exercise. Let A be an algebra and G be a finite group. If $f \colon G \to \mathcal{U}(A)$ is a group homomorphism, then there exists a unique algebra homomorphism $\varphi \colon K[G] \to A$ such that $\varphi|_G = f$.

13.9. EXAMPLE. Let $\mathbb{D}_3 = \langle r, s : r^3 = s^2 = 1, srs^{-1} = r^{-1} \rangle$ be the dihedral group of six elements. We claim that

$$\mathbb{C}[\mathbb{D}_3] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}).$$

Let ω be a primitive cubic root of one. Let

$$R = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

One easily checks that $SRS^{-1} = R^{-1}$ and $R^3 = S^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. It follows that there exists a group homomorphism $G \to \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$ such that $r \mapsto (1, 1, R)$ and $s \mapsto (1, -1, S)$. This group homomorphism is a ring isomorphism.

§ 14. Group representations

14.1. DEFINITION. A **representation** (over the field K) of a group G is a group homomorphism $\rho \colon G \to \mathbf{GL}(V)$, $g \mapsto \rho_g$, for some non-zero finite-dimensional vector space V (over K).

The **degree** of the representation $\rho \colon G \to \mathbf{GL}(V)$ will be the dimension of V.

Note that a representation $\rho \colon G \to \mathbf{GL}(V)$ satisfies the following properties:

1) $\rho_{1_G} = \mathrm{id}$.
2) $\rho_{gh} = \rho_g \rho_h$ for all $g, h \in G$.
3) $\rho_g(v + w) = \rho_g(v) + \rho_g(w)$ for all $v, w \in V$.
4) $\rho_g(\lambda v) = \lambda \rho_g(v)$ for all $v \in V$ and $\lambda \in K$.

Since by assumption V is finite-dimensional, say $\dim V = n$, after fixing a basis of V we get a **matrix representation** $\rho \colon G \to \mathbf{GL}(V) \simeq \mathbf{GL}_n(K)$ of G. Depending on the context, we will use either representations on vector spaces or matrix representations.

14.2. EXAMPLE. We use group representations to show that the group

$$G = \langle x, y : x^2 = y^2 = 1 \rangle$$

is infinite. Note that

$$\rho \colon G \to \mathbf{GL}_2(\mathbb{C}), \quad x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},$$

is a group homomorphism, as $\rho_x^2 = \rho_y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We claim that the elements of the form $(xy)^n$ are different for all n. It is enough to show that $(xy)^n = (xy)^m$, then $n = m$. Note that

$$\rho_{xy} = \rho_x \rho_y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus $\rho_{xy}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ and $\rho_{xy}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. Then

$$(xy)^n = (xy)^m \implies \rho_{xy}^n = \rho_{xy}^m \implies n = m.$$

The previous example demonstrates the power of group representations, even for infinite groups. However, in this course, we will focus on complex finite-dimensional representations of finite groups.

14.3. CONVENTION. When studying representations of groups, we will focus on complex representations of finite groups, unless stated otherwise.

14.4. EXAMPLE. If G is a group, then $\rho \colon G \to \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$, $g \mapsto 1$, is a representation. This representation is known as the **trivial (complex) representation** of G.

14.5. EXAMPLE. The sign of permutations yields a representation of $\mathbb{S}_n$. It is the group homomorphism $\mathbb{S}_n \to \mathbb{C}^\times$, $\sigma \mapsto \mathrm{sign}(\sigma)$.

14.6. EXAMPLE. Let $G = \langle g : g^6 = 1 \rangle$ be the cyclic group of order six. Then

$$\rho\colon G \to \mathbf{GL}_2(\mathbb{C}), \quad g \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

is a group representation of degree two.

14.7. DEFINITION. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations. A linear map $T\colon V \to W$ is said to be **invariant** if the diagram

$$\begin{array}{ccc} V & \xrightarrow{\rho_g} & V \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ W & \xrightarrow[\psi_g]{} & W \end{array}$$

commutes for all $g \in G$, this means that $\psi_g T = T \rho_g$ for all $g \in G$.

It is convenient to introduce an alternative notation for group representations. Let

$$\rho\colon G \to \mathbf{GL}(V), \quad g \mapsto \rho_g,$$

be a representation. For $g \in G$ and $v \in V$ write $g \cdot v = \rho_g(v)$. Then the following properties hold:

1) $1 \cdot v = v$ for all $v \in V$,
2) $g \cdot (h \cdot v) = (gh) \cdot v$ for all $g, h \in G$ and $v \in V$,
3) $g \cdot (v + w) = g \cdot v + g \cdot w$ for all $g \in G$ and $v, w \in V$, and
4) $g \cdot (\lambda v) = \lambda(g \cdot v)$ for all $g \in G$, $\lambda \in \mathbb{C}$ and $v \in V$.

Using this notation for the representations $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$, a linear map $T\colon V \to W$ is invariant if and only if

$$T(g \cdot v) = g \cdot T(v)$$

for all $v \in V$ and $g \in G$.

14.8. DEFINITION. The representations $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are **equivalent** if there exists a bijective linear map $T\colon V \to W$ invariant.

If the representations ρ and ψ are equivalent, we write $\rho \simeq \psi$.

14.9. EXAMPLE. Let $G = \mathbb{Z}/n$. The representations

$$\rho\colon G \to \mathbf{GL}_2(\mathbb{C}), \quad m \mapsto \begin{pmatrix} \cos(2\pi m/n) & -\sin(2\pi m/n) \\ \sin(2\pi m/n) & \cos(2\pi m/n) \end{pmatrix},$$

and

$$\psi\colon G \to \mathbf{GL}_2(\mathbb{C}), \quad m \mapsto \begin{pmatrix} e^{2\pi i m/n} & 0 \\ 0 & e^{-2\pi i m/n} \end{pmatrix},$$

are equivalent, as $\rho_m T = T \psi_m$ for all $m \in G$ if $T = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$.

The following example explains why we can alternatively use representations or matrix representations.

14.10. EXAMPLE. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation, say, of degree $n = \dim V$. Choose a basis $B = \{v_1, \ldots, v_n\}$ of V and let

$$T\colon V \to \mathbb{C}^n, \quad \sum_{i=1}^{n} \lambda_i v_i \mapsto (\lambda_1, \ldots, \lambda_n),$$

be the isomorphism that takes coordinates for the basis B. For each $g \in G$, the composition of linear maps

$$\mathbb{C}^n \xrightarrow{\ T^{-1}\ } V \xrightarrow{\ \rho_g\ } V \xrightarrow{\ T\ } \mathbb{C}^n$$

produces a representation $\psi\colon G \to \mathbf{GL}(C^n)$ of G equivalent to ρ.

14.11. DEFINITION. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. A subspace W of V is said to be **invariant** (with respect to ρ) if $\rho_g(W) \subseteq W$ for all $g \in G$.

Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. Then $\{0\}$ and V are always invariant subspaces of V. Moreover, if $W \subseteq V$ is invariant, then the map $\rho|_W\colon G \to \mathbf{GL}(W)$, $g \mapsto (\rho_g)|_W$, is a representation. The map $\rho|_W$ is the **restriction** of ρ to W.

14.12. EXERCISE. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations of a given group G and $T\colon V \to W$ be an invariant map. Prove that the **kernel**

$$\ker T = \{v \in V : T(v) = 0\}$$

is an invariant subspace of V and that the **image**

$$T(V) = \{T(v) : v \in V\}$$

is an invariant subspace of W.

14.13. DEFINITION. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. A **subrepresentation** of ρ is a restricted representation of the form $\rho|_W\colon G \to \mathbf{GL}(W)$ for some invariant subspace W of V.

14.14. DEFINITION. A non-zero representation $\rho\colon G \to \mathbf{GL}(V)$ is **irreducible** if $\{0\}$ and V are the only invariant subspaces of V.

Degree-one representations are irreducible.

The irreducibility of a representation, of course, depends on the base field. In the following example, it is crucial using real representations.

14.15. EXAMPLE. Let $G = \langle g : g^3 = 1 \rangle$ be the cyclic group of order three and

$$\rho\colon G \to \mathbf{GL}_3(\mathbb{R}), \quad g \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Note that in this example we work with a real representation! It is a routine calculation to prove that

$$W = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 : x + y + z = 0 \right\}$$

is an invariant subspace of $\mathbb{R}^3$. We claim that W is irreducible. Let S be a non-zero invariant subspace of W and let $s = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \in S$ be a non-zero element. Then

$$t = \begin{pmatrix} y_0 \\ z_0 \\ x_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \in S.$$

We claim that $\{s, t\}$ is linearly independent. If not, there exists $\lambda \in \mathbb{R}$ such that $\lambda s = t$. Thus $\lambda x_0 = y_0$, $\lambda y_0 = z_0$ and $\lambda z_0 = x_0$. This implies that $\lambda^3 x_0 = x_0$. Since $x_0 \neq 0$ (because if $x_0 = 0$, then $y_0 = z_0 = 0$, a contradiction), it follows that $\lambda = 1$ and hence $x_0 = y_0 = z_0$, a contradiction because $x_0 + y_0 + z_0 = 0$. Therefore $\dim S = 2$ and hence $S = W$.

What happens in the previous example if we work over complex numbers?

14.16. EXERCISE. Let $\rho\colon G \to \mathbf{GL}(V)$ be a degree-two representation. Prove that ρ is irreducible if and only if there is no common eigenvector for the ρ_g, $g \in G$.

The previous exercise can be used to show that the representation $\mathbb{S}_3 \to \mathbf{GL}_2(\mathbb{C})$ of the symmetric group $\mathbb{S}_3$ given by

$$(12) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$

is irreducible.

14.17. EXAMPLE. Let $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ and $\psi\colon G \to \mathbf{GL}_m(\mathbb{C})$ be representations. One defines the **direct sum** $\rho \oplus \psi$ of ρ and ψ as

$$\rho \oplus \psi\colon G \to \mathbf{GL}_{n+m}(\mathbb{C}), \quad g \mapsto \begin{pmatrix} \rho_g & 0 \\ 0 & \psi_g \end{pmatrix}.$$

Let us describe the previous example without using matrix representations. If V and W are complex vector spaces, the (external) direct sum of V and W is defined as the set $V \times W$ with the complex vector space structure given by

$$(v, w) + (v_1, w_1) = (v + v_1, w + w_1), \quad \lambda(v, w) = (\lambda v, \lambda w)$$

for all $v, v_1 \in V$, $w, w_1 \in W$ and $\lambda \in \mathbb{C}$. If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations, the **direct sum** $\rho \oplus \psi$ of ρ and ψ is then

$$\rho \oplus \psi\colon G \to \mathbf{GL}(V \oplus W), \quad g \mapsto (\rho \oplus \psi)_g,$$

where $(\rho \oplus \psi)_g\colon V \oplus W \to V \oplus W$, $(v, w) \mapsto (\rho_g(v), \psi_g(w))$. Note that both $V \simeq V \oplus \{0\}$ and $W \simeq \{0\} \oplus W$ are invariant subspaces of $V \oplus W$.

14.18. DEFINITION. A representation $\rho\colon G \to \mathbf{GL}(V)$ is said to be **completely reducible** if ρ can be decomposed as $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations $\rho_1, \ldots, \rho_n$ of G.

Note that if $\rho\colon G \to \mathbf{GL}(V)$ is completely reducible and $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations $\rho_i\colon G \to \mathbf{GL}(V_i)$, $i \in \{1, \ldots, n\}$, then each V_i is an invariant

subspace of V and $V = V_1 \oplus \cdots \oplus V_n$. Moreover, on some basis of V, the matrix ρ_g can be written as

$$\rho_g = \begin{pmatrix} (\rho_1)_g & & & \\ & (\rho_2)_g & & \\ & & \ddots & \\ & & & (\rho_n)_g \end{pmatrix}.$$

14.19. DEFINITION. A representation $\rho\colon G \to \mathbf{GL}(V)$ is **decomposable** if V can be decomposed as $V = S \oplus T$ where S and T are non-zero invariant subspaces of V.

A representation is **indecomposable** if it is not decomposable.

14.20. EXERCISE. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be equivalent representations. Prove the following facts:
   1) If ρ is irreducible, then ψ is irreducible.
   2) If ρ is decomposable, then ψ is decomposable.
   3) If ρ is completely reducible, then ψ is completely reducible.

§ 15. Tensor product of representations

Let V be a vector space with basis $\{v_1, \ldots, v_k\}$ and W be a vector space with basis $\{w_1, \ldots, w_l\}$. A **tensor product** of V and W is a vector space X with together with a bilinear map

$$V \times W \to X, \quad (v, w) \mapsto v \otimes w,$$

such that $\{v_i \otimes w_j : 1 \leq i \leq k, \, 1 \leq j \leq l\}$ is a basis of X. The tensor product of V and W is unique up to isomorphism and is denoted by $V \otimes W$. Note that

$$\dim(V \otimes W) = (\dim V)(\dim W).$$

Moreover, every element of $V \otimes W$ is a finite sum of the form

$$\sum_{i,j} \lambda_{ij} v_i \otimes v_j$$

for some scalars $\lambda_{ij} \in \mathbb{C}$. It is important to remark that elements of $V \otimes W$ are not always of the form $v \otimes w$ for $v \in V$ and $w \in W$.

The bilinearity of tensor products is crucial. For example,

$$\begin{aligned}
(v_1 + v_3) \otimes (3w_1 + w_2) &= v_1 \otimes (3w_1 + w_2) + v_3 \otimes (3w_1 + w_2) \\
&= v_1 \otimes (3w_1) + v_1 \otimes w_2 + v_3 \otimes (3w_1) + v_3 \otimes w_2 \\
&= 3v_1 \otimes w_1 + v_1 \otimes w_2 + 3v_3 \otimes w_1 + v_3 \otimes w_2.
\end{aligned}$$

15.1. DEFINITION. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations, and let $\{v_1, \ldots, v_n\}$ be a basis of V and $\{w_1, \ldots, w_m\}$ a basis of W. The **tensor product** of ρ and ψ is the representation of G given by

$$\rho \otimes \psi \colon G \to \mathbf{GL}(V \otimes W), \quad g \mapsto (\rho \otimes \psi)_g,$$

where

$$(\rho \otimes \psi)_g \left(\sum_{i,j} \lambda_{ij} v_i \otimes w_j \right) = \sum_{i,j} \lambda_{ij} \rho_g(v_i) \otimes \psi_g(w_j), \quad i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}.$$

15.2. EXERCISE. Prove that the tensor product of representations is a representation.

§ 16. Unitary representations

Since we are considering finite-dimensional vector spaces, our vector spaces admit an **inner product**, that is a map $V \times V \to \mathbb{C}$, $(v, w) \mapsto \langle v, w \rangle$, that satisfies the following properties:

1) $\langle y, x \rangle = \overline{\langle x, y \rangle}$ for all $x, y \in V$, where $\overline{a + bi} = a - bi$ denotes the complex conjugate.
2) $\langle ax + by, z \rangle = a\langle x, z \rangle + b\langle y, z \rangle$ for all $x, y, z \in V$ and $a, b \in \mathbb{C}$.
3) $\langle x, x \rangle > 0$ for all $x \in V$ and $\langle x, x \rangle = 0$ if $x = 0$.

For example, if $V = \mathbb{C}^n$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in V$ and $w = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \in V$, then the **usual inner product** between v and w is given by

(16.1) $$V \times V \to \mathbb{C}, \quad (v, w) \mapsto v_1\overline{w_1} + \cdots + v_n\overline{w_n} = v^T\overline{w},$$

where

$$v^T = (v_1, \ldots, v_n), \quad \overline{w} = \begin{pmatrix} \overline{w_1} \\ \vdots \\ \overline{w_n} \end{pmatrix}.$$

16.1. DEFINITION. Let V be a finite-dimensional complex vector space with inner product $(v, w) \mapsto \langle v, w \rangle$. A representation $\rho \colon G \to \mathbf{GL}(V)$ is **unitary** if $\langle \rho_g v, \rho_g w \rangle = \langle v, w \rangle$ for all $g \in G$ and $v, w \in V$.

16.2. EXERCISE. Let G be a finite group and $V = \mathbb{C}[G]$ be the complex vector space with basis $\{g : g \in G\}$. The **left regular representation** of G is the representation

$$L \colon G \to \mathbf{GL}(V), \quad g \mapsto L_g,$$

where $L_g(h) = gh$. With respect to the inner product

$$\left\langle \sum_{g \in G} \lambda_g g, \sum_{g \in G} \mu_g g \right\rangle = \sum_{g \in G} \lambda_g \overline{\mu_g},$$

the representation L is unitary. Prove it!

If V is a vector space and W is a subspace of V,

$$W^\perp = \{v \in V : \langle v, w \rangle = 0 \text{ for all } w \in W\},$$

is called the **orthogonal complement** of W. The following result is extremely important:

16.3. PROPOSITION. *Let $\rho \colon G \to \mathbf{GL}(V)$ be a unitary representation. Then ρ is either irreducible or decomposable.*

PROOF. If ρ is not irreducible, there exists an invariant subspace W of V such that $\{0\} \subsetneq W \subsetneq V$. Can we find an invariant complement? Yes, and this is because our representation is unitary. We know that $V = W \oplus W^\perp$ as complex vector spaces, where

$W^\perp \neq \{0\}$. So ρ will be decomposable if we can prove that $W^\perp$ is an invariant subspace of V. Let $v \in W^\perp$, $w \in W$ and $g \in G$. Then

$$\langle \rho_g(v), w \rangle = \langle v, \rho_g^{-1}(w) \rangle = 0$$

since $\rho_g^{-1}(w) \in W$, as W is an invariant subspace of V. This means that $\rho_g(v) \in W^\perp$ and hence $V = W \oplus W^\perp$ is decomposable. $\qquad\square$

§ 17. Weyl's trick

The following theorem is known as the **Weyl trick**.

17.1. THEOREM (Weyl). *Every representation* $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ *of a finite group is unitary.*

PROOF. Let $V = \mathbb{C}^n$ and $V \times V \to \mathbb{C}$, $(v,w) \mapsto v \cdot w$, be an[3] inner product on V. A straightforward calculation shows that

$$\langle v, w \rangle = \sum_{g \in G} (\rho_g v) \cdot (\rho_g w)$$

is an inner product of V. For example,

$$\langle v, w + w_1 \rangle = \sum_{g \in G} \rho_g v \cdot \rho_g(w + w_1)$$

$$= \sum_{g \in G} \rho_g v \cdot (\rho_g w + \rho_g w_1)$$

$$= \sum_{g \in G} \rho_g v \cdot \rho_g w + \rho_g v \cdot \rho_g w_1$$

$$= \sum_{g \in G} \rho_g v \cdot \rho_g w + \sum_{g \in G} \rho_g v \cdot \rho_g w_1$$

$$= \langle v, w \rangle + \langle v, w_1 \rangle$$

holds for all $v, w, w_1 \in V$.

Since

$$\langle \rho_g v, \rho_g w \rangle = \sum_{h \in G} (\rho_h \rho_g v) \cdot (\rho_h \rho_g w)$$

$$= \sum_{h \in G} (\rho_{hg} v) \cdot (\rho_{hg} w) = \sum_{x \in G} (\rho_x v) \cdot (\rho_x w) = \langle v, w \rangle,$$

the representation ρ is unitary. $\qquad\square$

17.2. EXAMPLE. Let $A = \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}$. Since $A^3 = I$, we can use this matrix to represent the (multiplicative) cyclic group

$$C_3 = \langle g : g^3 = 1 \rangle$$

of order three. Note that the map $1 \mapsto g$ yields an isomorphism $C_3 \simeq \mathbb{Z}/3$.

---

[3]It does not matter which inner product we have chosen, we can safely use, for example, the usual inner product of (16.1).

The map $C_3 \to \mathbf{GL}_2(\mathbb{C})$, $g \mapsto A$, is a group homomorphism. In particular, we have a representation $\rho\colon C_3 \to \mathbf{GL}(V)$, where $V = \mathbb{C}^2$ with the usual inner product given by (16.1), that is

$$v \cdot w = v^T \overline{w}$$

for $v, w \in V$. For example, the inner product between the vectors $\begin{pmatrix} 1 \\ i \end{pmatrix}$ and $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is

$$(1, i) \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 1 + 2i.$$

Since $A \in M_2(\mathbb{R})$, we compute

$$\langle v, w \rangle = v^T \overline{w} + (Av)^T \overline{(Aw)} + (A^2 v)^T \overline{(A^2 w)} = v^T \left(I + A^T A + (A^2)^T A^2 \right) \overline{w}$$

and this is an invariant inner product on V. Note that

$$B = I + A^T A + (A^2)^T A^2 = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}.$$

Weyl's trick has several interesting consequences:

17.3. COROLLARY. *Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation of a finite group G. The following properties hold:*

1) *ρ is equivalent to a unitary representation.*
2) *ρ is either irreducible or decomposable.*
3) *Each ρ_g is diagonalizable.*

PROOF. The first claim follows from Example 14.10 and Weyl's trick. The second claim, from 1) and Proposition 16.3. Finally, 3) follows from Weyl's trick immediately, as unitary matrices are diagonalizable. □

17.4. EXERCISE. If G is an infinite group, it is no longer true that every non-zero representation is either irreducible or decomposable. Find an example.

For the previous exercise. consider the representation $\mathbb{Z} \to \mathbf{GL}_2(\mathbb{C})$, $1 \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

§ 18. Maschke's theorem

Recall that, by convention, we only consider complex finite-dimensional representations of finite groups.

18.1. THEOREM (Maschke). *Every representation of a finite group is completely reducible.*

PROOF. Let G be a finite group and $\rho\colon G \to \mathbf{GL}(V)$ be a representation of G. We proceed by induction on $\dim V$. If $\dim V = 1$, the result is trivial, as degree-one representations are irreducible. Assume that the result holds for representations of degree $\leq n$. Suppose that ρ has degree $n + 1$. If ρ is irreducible, we are done. If not, use Proposition 16.3 to write $V = S \oplus T$, where S and T are non-zero invariant subspaces of V. Since $\dim S < \dim V$ and $\dim T < \dim V$, it follows from the inductive hypothesis that both S and T are spaces of completely reducible representations. Thus ρ is completely reducible. □

18.2. EXAMPLE. Let $G = \mathbb{S}_3$ and $\rho \colon G \to \mathbf{GL}_3(\mathbb{C})$ be the representation given by

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then ρ_g is unitary for all $g \in G$ (because $\rho_{(12)}$ and $\rho_{(123)}$ are both unitary). Moreover,

$$S = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \quad T = S^\perp = \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\rangle,$$

are irreducible invariant subspaces of $V = \mathbb{C}^3$. A direct calculation shows that in the orthogonal basis $\left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\}$ the matrices $\rho_{(12)}$ and $\rho_{(123)}$ can be written as

$$\rho_{(12)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_{(123)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}.$$

The **commutator subgroup** of a group G is defined as the subgroup $[G, G]$ generated by the commutators $[x, y] = xyx^{-1}y^{-1}$, that is

$$[G, G] = \langle [x, y] : x, y \in G \rangle.$$

Routine calculations show that $[G, G]$ is always a normal subgroup of G. For example, the commutator subgroup of $\mathbb{Z}$ is the trivial subgroup $\{0\}$, as

$$[x, y] = x + y - x - y = 0$$

for all $x, y \in \mathbb{Z}$. As an exercise, one can also prove that $[\mathbb{S}_3, \mathbb{S}_3] = \{\mathrm{id}, (123), (132)\}$.

18.3. EXERCISE. Let H be a normal subgroup of G. Prove that G/H is abelian if and only if $[G, G] \subseteq H$.

The previous exercise demonstrates, in particular, that for any group G, the quotient $G/[G, G]$ is always an abelian group. This quotient is known as the **abelianization** of G.

18.4. EXERCISE. Let G be a finite group. Prove that there is a bijection between degree-one representations of G and degree-one representations of $G/[G, G]$.

The following result is simple and crucial.

18.5. LEMMA (Schur). *Let $\rho \colon G \to \mathbf{GL}(V)$ and $\psi \colon G \to \mathbf{GL}(W)$ be irreducible representations. If $T \colon V \to W$ is a non-zero invariant map, then T is bijective.*

PROOF. Since T is non-zero and $\ker T$ is an invariant subspace of V, it follows that $\ker T = \{0\}$, as ρ is irreducible. Thus T is injective. Since $T(V)$ is a non-zero invariant subspace of W and ψ is irreducible, it follows that T is surjective. Therefore T is bijective. $\square$

Two applications:

18.6. PROPOSITION. *If G is finite, $\rho \colon G \to \mathbf{GL}(V)$ is an irreducible representation, and $T \colon V \to V$ is invariant, then $T = \lambda \, \mathrm{id}$ for some $\lambda \in \mathbb{C}$.*

PROOF. Let λ be an eigenvalue of T. Then $T - \lambda\,\mathrm{id}$ is invariant, as

$$(T - \lambda\,\mathrm{id})\rho_g = T\rho_g - \lambda\rho_g = \rho_g(T - \lambda\,\mathrm{id})$$

for all $g \in G$ since T is invariant. By definition, $T - \lambda\,\mathrm{id}$ is not bijective. Thus $T - \lambda\,\mathrm{id} = 0$ by Schur's lemma. $\square$

18.7. PROPOSITION. *Let G be a finite abelian group. If $\rho\colon G \to \mathbf{GL}(V)$ is an irreducible representation, then* $\dim V = 1$.

PROOF. Let $h \in G$. Note that since G is abelian, $T = \rho_h$ is invariant:

$$T\rho_g = \rho_h\rho_g = \rho_{hg} = \rho_{gh} = \rho_g\rho_h = \rho_g T.$$

By the previous proposition, there exists $\lambda_h \in \mathbb{C}$ such that $\rho_h = \lambda_h\,\mathrm{id}$. If $v \in V \setminus \{0\}$, then $V = \langle v \rangle$. In fact, since $\langle v \rangle$ is a non-zero invariant subspace of V and ρ is irreducible, it follows that $V = \langle v \rangle$. $\square$

§ 19. Modules

The rest of the course will be devoted to studying modules over rings. We first start with the main definitions and basic examples.

19.1. DEFINITION. Let R be a ring. A **module** (over R) is an abelian group (written additively) M with a map $R \times M \to M$, $(r, m) \mapsto r \cdot m$, such that the following conditions hold:

1) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$ for all $r_1, r_2 \in R$ and $m \in M$.
2) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for all $r \in R$ and $m_1, m_2 \in M$.
3) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ for all $r_1, r_2 \in R$ and $m \in M$.
4) $1 \cdot m = m$ for all $m \in M$.

Our definition is that of left module. Similarly, one defines right modules. We will always consider left modules (over R) so that they will be referred to simply as R-modules (or just modules).

19.2. EXAMPLE. A module over a field is a vector space.

19.3. EXAMPLE. Every abelian group is a module over $\mathbb{Z}$.

19.4. EXAMPLE. Let R be a ring. Then R is a module (over R) with $x \cdot m = xm$. This is the **(left) regular module** over R, and it usually is denoted by $_RR$.

The module $_RR$ is also known as the (left) regular representation of R.

19.5. EXAMPLE. Let G be a finite group. If $\rho\colon G \to \mathbf{GL}(V)$ is a representation, then V is a $\mathbb{C}[G]$-module with

$$g \cdot v = \rho_g(v)$$

for $g \in G$ and $v \in V$.
Conversely, if V is a $\mathbb{C}[G]$-module and V is a complex finite-dimensional vector space, then the map

$$\rho\colon G \to \mathbf{GL}(V), \quad g \mapsto \rho_g,$$

where $\rho_g(v) = g \cdot v$ for $v \in V$, is a representation of G.

19.6. EXAMPLE. If R is a ring, then $R^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in R\}$ is a module (over R) with $r \cdot (x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$.

19.7. EXAMPLE. If R is a ring, then $M_{m,n}(R)$ is a module (over R) with usual matrix operations.

Students usually ask why in the definition of a ring homomorphism, one needs the condition $1 \mapsto 1$. The following example provides a good explanation.

19.8. EXAMPLE. If $f\colon R \to S$ is a ring homomorphism and M is a module (over S) with $(s,m) \mapsto sm$, then M is also a module (over R) with $r \cdot m = f(r)m$ for all $r \in R$ and $m \in M$. In fact,

$$1 \cdot m = f(1)m = 1m = m,$$
$$r_1 \cdot (r_2 \cdot m) = f(r_1)(r_2 \cdot m) = f(r_1)(f(r_2)m) = (f(r_1)f(r_2))m = f(r_1 r_2)m$$

for all $r_1, r_2 \in R$ and $m \in M$.

19.9. EXAMPLE. Let V be a finite-dimensional real vector space and $T\colon V \to V$ be a linear map. Let $R = \mathbb{R}[X]$. Then $M = V$ with

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v)$$

is a module (over R), where we use the following notation: for $v \in V$, we write

$$T^0(v) = v, \quad T^1(v) = T(v), \quad T^2(v) = T(T(v)) \ldots$$

19.10. EXAMPLE. If $\{M_i : i \in I\}$ is a family of R-modules, then

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \text{ for all } i \in I\}$$

is an R-module with $x \cdot (m_i)_{i \in I} = (x \cdot m_i)_{i \in I}$, where $(m_i)_{i \in I}$ denotes the map $I \to \bigcup_{i \in I} M_i$, $i \mapsto m_i \in M_i$. This module is the **direct product** of the family $\{M_i : i \in I\}$.

19.11. EXAMPLE. If $\{M_i : i \in I\}$ is family of R-modules, then

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i \text{ for all } i \in I \text{ and } m_i = 0 \text{ except finitely many } i \in I\}$$

is an R-module with $x \cdot (m_i)_{i \in I} = (x \cdot m_i)_{i \in I}$. This module is the **direct sum** of the family $\{M_i : i \in I\}$.

If M is a module, then $0 \cdot m = 0$ and $-m = (-1) \cdot m$ for all $m \in M$ and $x \cdot 0 = 0$ for all $x \in R$.

19.12. EXAMPLE. Let $M = \mathbb{Z}/6$ as a module (over $\mathbb{Z}$). Note that $3 \cdot 2 = 0$ but $3 \neq 0$ (in $\mathbb{Z}$) and $2 \neq 0$ (in $\mathbb{Z}/6$).

19.13. EXERCISE. Prove that $\mathbb{Z}/4$ is not a module over $\mathbb{Z}/2$.

19.14. DEFINITION. Let M be a module. A subset N of M is a **submodule** of M if N is a subgroup of M and $R \cdot N \subseteq N$, that is $x \cdot n \in N$ for all $x \in R$ and $n \in N$.

Clearly, if M is a module, then $\{0\}$ and M are submodules of M.

19.15. EXAMPLE. Let R be a field and M be a module over R. Then N is a submodule of M if and only if N is a subspace of M.

19.16. EXAMPLE. Let $R = \mathbb{Z}$ and M be a module (over R). Then N is a submodule of M if and only if N is a subgroup of M

19.17. EXAMPLE. If $M = {}_R R$, then a subset $N \subseteq M$ is a submodule of M if and only if N is a left ideal of R.

19.18. EXAMPLE. If V is a finite-dimensional real vector space and $T : V \to V$ is a linear map, then V is a module (over $\mathbb{R}[X]$) with

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

A submodule is a subspace W of V such that $T(W) \subseteq W$.

Clearly, a subset N of M is a submodule if and only if $r_1 n_1 + r_2 n_2 \in N$ for all $r_1, r_2 \in R$ and $n_1, n_2 \in N$.

19.19. EXERCISE. If N and N_1 are submodules of M, then
$$N + N_1 = \{n + n_1 : n \in N, n_1 \in N_1\}$$
is a submodule of M.

19.20. DEFINITION. Let M and N be modules over R. A map $f : M \to N$ is a **module homomorphism** if $f(x+y) = f(x)+f(y)$ and $f(r \cdot x) = r \cdot f(x)$ for all $x, y \in M$ and $r \in R$.

We denote by $\operatorname{Hom}_R(M, N)$ the set of module homomorphisms $M \to N$.

19.21. EXERCISE. Let $f \in \operatorname{Hom}_R(M, N)$.
1) If V is a submodule of M, then $f(V)$ is a submodule of N.
2) If W is a submodule of N, then $f^{-1}(W)$ is a submodule of M.

If $f \in \operatorname{Hom}_R(M, N)$, the **kernel** of f is the submodule
$$\ker f = f^{-1}(\{0\}) = \{m \in M : f(m) = 0\}$$
of M. We say that f is a **monomorphism** (resp. **epimorphism**) if f is injective (resp. surjective). Moreover, f is an **isomorphism** if f is bijective.

19.22. EXERCISE. Let $f \in \operatorname{Hom}_R(M, N)$. Prove that the following statements are equivalent:
1) f is a monomorphism.
2) $\ker f = \{0\}$.
3) For every module V and every $g, h \in \operatorname{Hom}_R(V, M)$, $fg = fh \implies g = h$.
4) For every module V and every $g \in \operatorname{Hom}(V, M)$, $fg = 0 \implies g = 0$.

Later we will see a similar exercise for surjective module homomorphisms.

19.23. EXAMPLE. Let $R = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}$. We claim that $\begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix} \not\cong \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix}$ as modules over R, where the module structure is given by the usual matrix multiplication. Assume that they

are isomorphic. Let $f \colon \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix} \to \begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix}$ be an isomorphism of modules and let $x_0 \in \mathbb{R} \setminus \{0\}$ be such that $f \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_0 \\ 0 \end{pmatrix}$. Thus

$$f \begin{pmatrix} 0 \\ 1 \end{pmatrix} = f \left(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot f \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

a contradiction, as f is injective.

If N and N_1 are submodules of M, we say that M is the **direct sum** of N and N_1 if $M = N + N_1$ and $N \cap N_1 = \{0\}$. In this case, we write $M = N \oplus N_1$. Note that if $M = N \oplus N_1$, then each $m \in M$ can be written uniquely as $m = n + n_1$ for some $n \in N$ and $n_1 \in N_1$. Such a decomposition exists because $M = N + N_1$. If $m \in M$ can be written as $m = n + n_1 = n' + n_1'$ for some $n, n' \in N$ and $n_1, n_1' \in N_1$, then $-n' + n = n_1' - n_1 \in N \cap N_1 = \{0\}$ and hence $n = n'$ and $n_1 = n_1'$. If $M = N \oplus N_1$, the submodule N (resp. N_1) is a **direct summand** of M and the submodule N_1 (resp N) is a **complement** of N in M.

19.24. EXAMPLE. If $M = \mathbb{R}^2$ is a vector space, then every subspace of M is a direct summand of M.

Clearly, the submodules $\{0\}$ and M are direct summands of M.

19.25. EXAMPLE. If $M = \mathbb{Z}$ as a module over $\mathbb{Z}$, then $m\mathbb{Z}$ is a direct summand of M if and only if $m \in \{0, 1\}$, as $n\mathbb{Z} \cap m\mathbb{Z} = \{0\}$ if and only if $nm = 0$.

19.26. EXERCISE. Let M be a module. A module N is isomorphic to a direct summand of M if and only if there are module homomorphisms $i \colon N \to M$ and $p \colon M \to N$ such that $pi = \mathrm{id}_N$. In this case, $M = \ker p \oplus i(N)$.

The **direct sum** of submodules can be defined for finitely many summands. If $V_1, \ldots, V_n$ are submodules of M, we say that $M = V_1 \oplus \cdots \oplus V_n$ if every $m \in M$ can be written uniquely as $m = v_1 + \cdots + v_n$ for some $v_1 \in V_1, \ldots, v_n \in V_n$.

19.27. EXERCISE. Prove that $M = V_1 \oplus \cdots \oplus V_n$ if and only if $M = V_1 + \cdots + V_n$ and

$$V_i \cap \left(\sum_{j \neq i} V_j \right) = \{0\}$$

for all $i \in \{1, \ldots, n\}$.

If $\{N_i : i \in I\}$ is a family of submodules of a module M, then the intersection $\cap_{i \in I} N_i$ is also a submodule of M.

19.28. EXERCISE. Let $T\colon \mathbb{R}^2 \to \mathbb{R}^2$ be a linear map and $M = \mathbb{R}^2$ with the module structure over $\mathbb{R}[X]$ given by

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot (x, y) = \sum_{i=0}^{n} a_i T^i(x, y).$$

Find the submodules of M in the following cases:

1) $T(x, y) = (0, y)$.
2) $T(x, y) = (y, x)$.

19.29. EXERCISE. Let V be a finite-dimensional real vector space and $T\colon V \to V$ be a linear map. Then V is a module over $\mathbb{R}[X]$ with

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot v = \sum_{i=0}^{n} a_i T^i(v).$$

Prove that any module homomorphism $g\colon V \to V$ commutes with T.

19.30. EXERCISE. Prove that $\operatorname{Hom}_R(M, N)$ is a module over $Z(R)$ with the following action: If $r \in R$ and $f \in \operatorname{Hom}_R(M, N)$, then $r \cdot f\colon M \to N$, $m \mapsto f(r \cdot m)$.

Let M be a module, and N be a submodule of M. In particular, M/N is an abelian group, and the map $\pi\colon M \to M/N$, $m \mapsto m + N$, is a surjective group homomorphism with kernel equal to N. We claim that the **quotient** M/N is a module with

$$r \cdot (m + N) = (r \cdot m) + N, \quad r \in R,\ m \in M.$$

Let us check that this operation on M/N is well-defined. If $x + N = y + N$, then $x - y \in N$ implies that

$$r \cdot x - r \cdot y = r \cdot (x - y) \in N,$$

that is $r \cdot (x + N) = r \cdot (y + N)$. It is an exercise to show that the map $\pi\colon M \to M/N$, $x \mapsto x + N$, is a surjective module homomorphism.

19.31. EXAMPLE. If $R = M = \mathbb{Z}$ and $N = 2\mathbb{Z}$, then $M/N \simeq \mathbb{Z}/2$.

19.32. EXAMPLE. Let R be a commutative ring and M be an R-module. We claim that

$$M \simeq \operatorname{Hom}_R({}_RR, M).$$

Since R is commutative, it follows that $\operatorname{Hom}_R({}_RR, M)$ is a module, see Exercise 19.30.

Let $\varphi\colon M \to \operatorname{Hom}_R({}_RR, M)$, $m \mapsto f_m$, where $f_m\colon R \to M$, $r \mapsto r \cdot m$. To show that φ is well-defined it is enough to see that $\varphi(m) \in \operatorname{Hom}_R({}_RR, M)$, that is

$$f_m(r + s) = (r + s) \cdot m = r \cdot m + s \cdot m, \quad f_m(rs) = (rs) \cdot m = r \cdot (s \cdot m) = r \cdot f_m(s).$$

Let us show that φ is a module homomorphism. We first note that

$$\varphi(m + n) = \varphi(m) + \varphi(n)$$

for all $m, n \in M$, as

$$\varphi(m + n)(r) = f_{m+n}(r) = r \cdot (m + n)$$
$$= r \cdot m + r \cdot n = f_m(r) + f_n(r) = \varphi(m)(r) + \varphi(n)(r).$$

49

Moreover,

$$\varphi(r \cdot m) = r \cdot \varphi(m)$$

for all $r \in R$ and $m \in M$, as

$$\varphi(r \cdot m)(s) = f_{r \cdot m}(s) = s \cdot (r \cdot m) = (sr) \cdot m$$
$$= (rs) \cdot m = f_m(rs) = \varphi(m)(rs) = (r \cdot \varphi(m))(s).$$

It remains to show that φ is bijective. We first prove that φ is injective. If $\varphi(m) = 0$, then $r \cdot m = \varphi(m)(r) = 0$ for all $r \in R$. In particular, $m = 1 \cdot m = 0$. We now prove that φ is surjective. If $f \in \text{Hom}_R({}_R R, M)$, let $m = f(1)$. Then $\varphi(m) = f$, as

$$\varphi(m)(r) = r \cdot m = r \cdot f(1) = f(r).$$

As one does for groups, it is possible to show that if M is a module and N is a submodule of M, the pair $(M/N, \pi\colon M \to M/N)$ has the following properties:

1) $N \subseteq \ker \pi$.
2) If $f\colon M \to T$ is a homomorphism such that $N \subseteq \ker f$, then there exists a unique module homomorphism $\varphi\colon M/N \to T$ such that the diagram

$$
\begin{array}{ccc}
M & \xrightarrow{\ f\ } & T \\
{\scriptstyle \pi}\downarrow & \nearrow_{\varphi} & \\
M/N & &
\end{array}
$$

is commutative, that is $\varphi\pi = f$.

Recall that if S and T are submodules of a module M, then both $S \cap T$ and

$$S + T = \{s + t : s \in S,\, t \in T\}$$

are submodules of M. The **isomorphism theorems** hold:

1) If $f \in \text{Hom}_R(M, N)$, then $M/\ker f \simeq f(M)$.
2) If $T \subseteq N \subseteq M$ are submodules, then

$$\frac{M/T}{N/T} \simeq M/N$$

3) If S and T are submodules of M, then

$$(S + T)/S \simeq T/(S \cap T).$$

19.33. EXAMPLE. If K is a field and V is a module over K, then V is, by definition, a vector space over K. If S and T are subspaces of V, then they are submodules of V. By the isomorphism theorem, $(S + T)/S \simeq T/(S \cap T)$ as vector spaces. By applying dimension,

$$\dim(S + T) - \dim S = \dim T - \dim(S \cap T).$$

19.34. EXAMPLE. If N is a direct summand of M and X is a complement for N, then $X \simeq M/N$, as

$$M/N = (N \oplus X)/N \simeq X/(N \cap X) = X/\{0\} \simeq X$$

by the second isomorphism theorem. So all complements of N in M are isomorphic.

It is also possible to prove that there exists a bijective correspondence between submodules of M/N and submodules of M containing N. The correspondence is given by $\pi^{-1}(Y) \leftrightarrow Y$ and $X \mapsto \pi(X)$.

19.35. EXERCISE. Let $f \in \operatorname{Hom}_R(M, N)$. Prove that the following statements are equivalent:

1) f is an epimorphism.
2) $N/f(M) \simeq \{0\}$.
3) For every module T and every $g, h \in \operatorname{Hom}_R(N, T)$, $gf = hf \implies g = h$.
4) For every module T and every $g \in \operatorname{Hom}_R(N, T)$, $gf = 0 \implies g = 0$.

19.36. EXERCISE. Let R be a ring and M_1 and M_2 be maximal ideals of R. Prove that $R/M_1 \simeq R/M_2$ as modules over R if and only if there exists $r \in R \setminus M_2$ such that $rM_1 \subseteq M_2$.

§ 20. Noetherian modules

We first start with a very easy exercise.

20.1. EXERCISE. Let M be a module. Prove that the intersection of submodules of M is a submodule of M.

20.2. DEFINITION. Let M be a module and X be a subset of M. The submodule of M generated by X is defined as

$$(X) = \bigcap \{N : N \text{ is a submodule of } M \text{ that contains } X\},$$

the smallest submodule of M containing X.

One can prove that

$$(X) = \left\{ \sum_{i=1}^{m} r_i \cdot x_i : m \in \mathbb{Z}_{\geq 0}, \ r_1, \ldots, r_m \in R, \ x_1, \ldots, x_m \in X \right\}.$$

20.3. DEFINITION. A module M is **finitely generated** if $M = (X)$ for some finite subset X of M.

If $X = \{x_1, \ldots, x_m\}$ one writes $(X) = (x_1, \ldots, x_n)$. For example, $\mathbb{Z} = (1) = (2, 3)$ and $\mathbb{Z} \neq (2)$.

20.4. EXERCISE. Let R be the ring of continuous maps $[0, 1] \to \mathbb{R}$ with point-wise operations and $M = {}_R R$. Prove that

$$N = \{f \in R : f(x) \neq 0 \text{ for finitely many } x\}$$

is not finitely generated.

20.5. EXERCISE. Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Prove that if $M = \mathbb{C}[G]$ is finitely generated, then M is a finite-dimensional complex vector space.

20.6. EXAMPLE. Let R be a ring. The R-module R^3 is finitely generated by $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$.

If $f \in \mathrm{Hom}_R(M, N)$ and M is finitely generated, then $f(M)$ is finitely generated. To prove this and other similar results, we introduce exact sequences (of modules and module homomorphisms). A sequence

(20.1) $$0 \longrightarrow M \stackrel{f}{\longrightarrow} N \stackrel{g}{\longrightarrow} T \longrightarrow 0$$

of modules and homomorphism is said to be **exact** if f is injective, g is surjective and $f(M) = \ker g$. For example, the sequence

$$0 \longrightarrow M \stackrel{f}{\longrightarrow} M \oplus N \stackrel{g}{\longrightarrow} N \longrightarrow 0,$$

where $f(m) = (m, 0)$ and $g(m, n) = n$, is exact.

20.7. EXERCISE. Let

$$0 \longrightarrow M \stackrel{f}{\longrightarrow} N \stackrel{g}{\longrightarrow} T \longrightarrow 0$$

be an exact sequence. Prove the following statements:

1) If N if finitely generated, then T is finitely generated.
2) If M and T are finitely generated, then N is finitely generated.

20.8. EXERCISE. Find a finitely generated module that contains a submodule that is not finitely generated.

20.9. PROPOSITION. *Let R be a ring and M be a module over R. Then M is finitely generated if and only if M is isomorphic to a quotient of R^k for some k.*

PROOF. Assume first that $M = (m_1, \ldots, m_k)$ is finitely generated. A routine calculation shows that the map

$$\varphi \colon R^k \to M, \quad (r_1, \ldots, r_k) \mapsto \sum_{j=1}^{k} r_j \cdot m_j,$$

is a surjective module homomorphism. The first isomorphism theorem implies that

$$R^k / \ker \varphi \simeq \varphi(R^k) = M.$$

Conversely, assume that there exists a surjective module homomorphism $\varphi \colon R^k \to M$. Since $R^k = (e_1, \ldots, e_k)$, where

$$(e_i)_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

it follows that $\{\varphi(e_1), \ldots, \varphi(e_k)\}$ generates $\varphi(R^k) = M$. To prove this, note that if $m \in M$, by the surjectivity of φ, we write $m = \varphi(r_1, \ldots, r_k)$ for some $(r_1, \ldots, r_k) \in R^k$. Hence

$$m = \varphi(r_1, \ldots, r_k) = \varphi \left(\sum_{i=1}^{k} r_i \cdot e_i \right) = \sum_{i=1}^{k} r_i \cdot \varphi(e_i). \qquad \square$$

20.10. DEFINITION. A module M is **noetherian** if every sequence $M_1 \subseteq M_2 \subseteq \cdots$ of submodules of M stabilizes, that is there exists an integer n such that $M_n = M_{n+k}$ for all k.

Let M be a module and X be a non-empty family of submodules of M. We say that $S \in X$ is a **maximal element** (with respect to the inclusion) if $S \subseteq T$ for some $T \in X$ implies $S = T$.

20.11. PROPOSITION. *Let M be a module. The following statements are equivalent:*

1) *M is noetherian.*
2) *All submodules of M are finitely generated.*
3) *Every non-empty family of submodules of M has a maximal element.*

PROOF. We first prove 2) $\implies$ 1). If $S_1 \subseteq S_2 \subseteq \cdots$ is an increasing sequence of submodules of M, it follows that $S = \cup_{i \geq 1} S_i$ is a submodule[4] of M. Since S is finitely generated, $S = (x_1, \ldots, x_n)$ for some $x_1, \ldots, x_n \in M$. It follows that $x_1, \ldots, x_n \in S_N$ for some positive integer N. Thus $S \subseteq S_N$ and hence $S_N = S_{N+k}$ for all k.

We now prove 1) $\implies$ 3). Let F be a non-empty family of submodules of M with no maximal elements. Let $S_1 \in F$. Since S_1 is not maximal in F, there exists $S_2 \in F$ such that $S_1 \subsetneq S_2$. Having constructed with this method the submodules $S_1 \subsetneq \cdots \subsetneq S_k$, since S_k is not maximal in F, there exists $S_{k+1} \in F$ such that $S_k \subsetneq S_{k+1}$. This means that the sequence $S_1 \subsetneq S_2 \subsetneq \cdots$ does not stabilize.

We finally prove 3) $\implies$ 2). Let S be a submodule of M and let

$$F = \{T \subseteq S : T \text{ finitely generated submodule of } M\}.$$

Note that $F \neq \emptyset$, as $\{0\} \in F$. Then F has a maximal element N. Thus N is a finitely generated submodule of M such that $N \subseteq S$. We may assume that $N = (n_1, \ldots, n_k)$. If $N = S$, then, in particular, S is finitely generated. Suppose that $N \neq S$ and let $x \in S \setminus N$. It follows that $N \subseteq (n_1, \ldots, n_k, x) \subseteq S$. Since $(n_1, \ldots, n_k, x) \in F$ and N is maximal, it follows that $N = (n_1, \ldots, n_k, x)$, a contradiction to $x \notin N$. $\qquad\square$

The previous theorem shows that every noetherian module is finitely generated.

20.12. EXERCISE. Find a non-noetherian module such that every proper submodule is finitely generated.

20.13. EXERCISE. Let

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

be an exact sequence. Prove the following statements:
1) If N is noetherian, then M and T are noetherian.
2) If M and T are noetherian, then N is noetherian.

20.14. EXERCISE. A commutative ring R is noetherian if and only if $_R R$ is noetherian.

20.15. EXERCISE. If $M_1, \ldots, M_n$ are noetherian, then $M_1 \oplus \cdots \oplus M_n$ is noetherian.

The previous exercise cannot be extended to infinitely many modules. Why?

20.16. PROPOSITION. *If R is noetherian and M is a finitely generated module, then M is noetherian.*

---

[4]In general, the union of submodules is not a submodule. Here $\cup_j S_j$ is a submodule because we have an increasing sequence $S_1 \subseteq S_2 \subseteq \cdots$ of submodules.

PROOF. Assume that $M = (m_1, \ldots, m_k)$. There exists a surjective homomorphism

$$R^k \to M, \quad (r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot m_i,$$

where $R^k = \bigoplus_{i=1}^{k} R$. Since R is noetherian, R^k is noetherian. Thus M is noetherian. □

§ 21. Free modules

21.1. DEFINITION. Let R be a ring, M be a module over R and X be a subset of M. We say that X is **linearly independent** if for each $k \in \mathbb{Z}_{>0}$, $r_1, \ldots, r_k \in R$ and $m_1, \ldots, m_k \in X$ such that $\sum_{i=1}^{k} r_i \cdot m_i = 0$, then $r_1 = \cdots = r_k = 0$.

In any ring, the set $\{1\}$ is linearly independent.

21.2. EXERCISE. Let R be a ring, M a module over R and X a subset of M. Prove that X is linearly independent if every finite subset of X is linearly independent.

21.3. EXERCISE. Let R be a ring, M a module over R and $m_1, \ldots, m_k \in M$. Prove that $\{m_1, \ldots, m_k\}$ is linearly independent if for each $m \in (m_1, \ldots, m_k)$ there are unique coefficients $r_1, \ldots, r_k \in R$ such that $m = r_1 \cdot m_1 + \cdots + r_k \cdot m_n$.

The previous exercise also holds for infinite sets of linearly independent elements.

21.4. BONUS EXERCISE. Let R be a ring, M a module over R and X a subset of M. Prove that X is linearly independent if for each $m \in (X)$ there are unique coefficients $\{r_x : x \in X\}$ with $r_x = 0$ except finitely many x, such that $m = \sum r_x \cdot x$.

A set is said to be **linearly dependent** if it is not linearly independent.

21.5. EXAMPLE.
1) $\{2, 3\}$ is a linearly dependent subset of $\mathbb{Z}$.
2) $\{2\}$ is a linearly dependent subset of $\mathbb{Z}/4$.
3) Let $R = \mathbb{Z}$, $M = \mathbb{Q}$ and $x \in M \setminus \{0\}$. Then $\{x\}$ is a linearly independent subset of M. If $y \in M \setminus \{x\}$, then $\{x, y\}$ is linearly dependent.

A generating set X for a module M is **minimal** if $X \setminus \{x\}$ is no longer a generating set of M for all $x \in X$. In vector spaces, a subset of the vector space is a basis if and only if it is a minimal generating set. This is no longer true for arbitrary modules.

21.6. EXAMPLE. Let $R = M_2(\mathbb{R})$ and $M = \begin{pmatrix} 0 & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$. Then $\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$ is a minimal generating set and it is not linearly independent.

However, one can prove that each module's basis is a minimal generating set.

21.7. EXERCISE. Let $f \in \mathrm{Hom}_R(M, N)$ and X be a subset of M.
1) If X is linearly dependent, then $f(X)$ is linearly dependent.
2) If X is linearly independent and f is injective, then $f(X)$ is linearly independent.
3) If $M = (X)$ and f is surjective, then $N = (f(X))$.

21.8. DEFINITION. Let M be a module and B be a subset of M. Then B is a **basis** of M if B is linearly independent and $M = (B)$. A module M is said to be **free** if it admits a basis.

21.9. EXERCISE. Let M be a module. Prove that M is free if and only if there is a subset B of M such that every element $m \in M$ can be written uniquely as finite sum of the form $m = \sum_{i=1}^{k} r_i \cdot b_i$ with $r_1, \ldots, r_k \in R$ and $b_1, \ldots, b_k \in B$.

As a consequence of Zorn's lemma, vector spaces are free.

21.10. EXAMPLE.

1) If R is a ring, then $\{1\}$ is a basis of $_R R$, so $_R R$ is free.
2) If R is a ring, then R^n is free as a module over R.

21.11. EXERCISE. Prove that $\mathbb{Z}/4$ is free as a $\mathbb{Z}/4$ module and that the submodule $\{0, 2\} \subseteq \mathbb{Z}/4$ is not free as a $\mathbb{Z}/4$-module.

21.12. EXERCISE. Prove that $\mathbb{Q}$ is not free as a module over $\mathbb{Z}$.

21.13. EXERCISE. Let R be a division ring and M be a non-zero and finitely generated module over R. Prove the following facts:

1) Every finite set of generators contains a basis.
2) Every linearly independent set can be extended into a basis.
3) Any two bases contain the same number of elements.

The previous exercise states that modules over division rings are like vector spaces over fields. In particular, such modules have dimensions.

21.14. EXAMPLE. $\mathbb{R}[X]$ is a free module (over $\mathbb{R}$) with basis $\{1, X, X^2, \ldots\}$.

21.15. EXERCISE. Prove that $\{(a, b), (c, d)\}$ is a basis of $\mathbb{Z} \times \mathbb{Z}$ (as a module over $\mathbb{Z}$) if and only if $ad - bc \in \{-1, 1\}$.

21.16. EXAMPLE. If $u \in \mathcal{U}(R)$, then $\{u\}$ is a basis of $_R R$. Conversely, if R is a (not necessarily commutative) domain and $\{z\}$ is a basis of $_R R$, then $z \in \mathcal{U}(R)$. Since $1 = yz$ for some $y \in R$, then it follows that $zy = 1$, as

$$(zy - 1)z = z(yz) - z = z1 - z = z - z = 0.$$

If R is a ring and I is a set,

$$R^{(I)} = \{f \colon I \to R : f(x) = 0 \text{ for all but finitely many } x \in I\}$$

is a module (over R) with $(f + g)(x) = f(x) + g(x)$ and $(rf)(x) = rf(x)$ for all $f, g \in R^{(I)}$, $x \in I$ and $r \in R$. Note that every element of $R^{(I)}$ can be written uniquely as a finite sum of the form

$$\sum_{i \in I} r_i \delta_i,$$

where the r_i are elements of R and only finitely many of them are non-zero, and

$$\delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

One proves that

$$R^{(I)} \simeq \bigoplus_{i \in I} R.$$

21.17. EXAMPLE. If I is a non-empty set, the module $R^{(I)}$ is free with basis $\{\delta_i : i \in I\}$, where

$$\delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

21.18. EXAMPLE. If $R = M_2(\mathbb{Z})$, then $M = {}_R R$ is free with basis $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. The submodule $N = \begin{pmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & 0 \end{pmatrix}$ does not admits a basis as a module over R.

In modules, the size of a basis is not an invariant of the module.

21.19. EXAMPLE. Let V be the complex vector space with infinite basis $e_0, e_1, e_2, \ldots$ and let $R = \text{End}(V)$ with the ring structure given by

$$(f + g)(v) = f(v) + g(v), \quad (fg)(v) = f(g(v))$$

for $f, g \in R$ and $v \in V$.

Let $M = {}_R R$. The set $\{\text{id}\}$ is a basis for R. We claim that M admits a basis with two elements. If $r, s \in R$ are such that

$$\begin{aligned} r(e_{2n}) &= e_n, & r(e_{2n+1}) &= 0, \\ s(e_{2n}) &= 0, & s(e_{2n+1}) &= e_{2n}, \end{aligned}$$

then $\{r, s\}$ is a basis of M. If $f \in R$, then $f = \alpha r + \beta s$, where $\alpha \colon V \to V$, $e_n \mapsto f(e_{2n})$ for all n, and $\beta \in V \to V$, $e_n \mapsto f(e_{2n+1})$ for all n. In fact,

$$\begin{aligned} (\alpha r + \beta s)(e_{2n}) &= \alpha(r(e_{2n})) + \beta(s(e_{2n})) = f(e_{2n}), \\ (\alpha r + \beta s)(e_{2n+1}) &= \alpha(r(e_{2n+1})) + \beta(s(e_{2n+1})) = f(e_{2n+1}). \end{aligned}$$

Moreover, $\{r, s\}$ is linearly independent. Indeed, if $\alpha r + \beta s = 0$ for some $\alpha, \beta \in R$, Evaluation on e_{2n} yields $\alpha = 0$ and evaluation on e_{2n+1} yields $\beta = 0$.

21.20. EXAMPLE. If M is a free module with basis X and N is a free module with basis Y, then $M \oplus N$ is a free module with basis

$$\{(x, 0) : x \in X\} \cup \{(0, y) : y \in Y\}.$$

21.21. EXERCISE. Let R be a commutative ring. If M and N are free and finitely generated, then $\text{Hom}_R(M, N)$ is free and finitely generated.

Some properties of free modules:

21.22. PROPOSITION. *If M is free, then there exists a subset $\{m_i : i \in I\}$ of M such that for each $m \in M$ there exist unique $r_i \in R$, $i \in I$, where $r_i = 0$ except for finitely many $i \in I$ such that $m = \sum r_i \cdot m_i$.*

PROOF. Since M is free, there exists a basis $\{m_i : i \in I\}$ of M. If $m \in M$, $m = \sum r_i \cdot m_i$ (finite sum) for some $r_i \in I$. We claim that the r_i's are unique. If $m = \sum s_i \cdot m_i$, then $\sum (r_i - s_i) \cdot m_i = 0$. Since $\{m_i : i \in I\}$ is linearly independent, $r_i = s_i$ for all $i \in I$. $\qquad\square$

21.23. PROPOSITION. *Let M be a free module over R with basis $\{m_i : i \in I\}$ and let N be a module over R. If $\{n_i : i \in I\} \subseteq N$, then there exists a unique $f \in \operatorname{Hom}_R(M, N)$ such that $f(m_i) = n_i$ for all $i \in I$.*

SKETCH OF THE PROOF. Note that the unique homomorphism $f \colon M \to N$ is defined as

$$f\left(\sum r_i \cdot m_i\right) = \sum r_i \cdot n_i. \qquad\qquad\square$$

Another application:

21.24. EXAMPLE. There is no surjective homomorphism $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ (of modules over $\mathbb{Z}$). If $f \colon \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is a surjective homomorphism, let $\{u, v\}$ a basis of $\mathbb{Z} \times \mathbb{Z}$. Then $f(k) = u$ and $f(l) = v$ for some $k, l \in \mathbb{Z}$. Proposition 21.23 implies that there exists a homomorphism $g \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $g(u) = k$ and $g(v) = l$. In particular, $fg = \operatorname{id}_{\mathbb{Z} \times \mathbb{Z}}$ and hence g is injective. Since

$$g(lu - kv) = lg(u) - kg(v) = lk - kl = 0,$$

it follows that $lu - kv = 0$ and thus $k = l = 0$, as $\{u, v\}$ is linearly independent, a contradiction

Another important property:

21.25. PROPOSITION. *If M is a free R-module, then $M \simeq R^{(I)}$ for some set I.*

PROOF. Suppose that M has basis $\{m_i : i \in I\}$. Then there exists a unique homomorphism $f \in \operatorname{Hom}_R(M, R^{(I)})$ such that $f(m_i) = \delta_i$ for all $i \in I$, where

$$\delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

We claim that f is an isomorphism. We first prove that the map f is surjective: if $(r_i)_{i \in I} \in R^{(I)}$, then $f(\sum r_i \cdot m_i) = (r_i)_{i \in I}$. Let us prove that f is injective:

$$0 = f\left(\sum r_i \cdot m_i\right) = \sum r_i \cdot f(m_i) = \sum r_i \cdot \delta_i \implies r_i = 0 \text{ for all } i \in I. \qquad\square$$

21.26. COROLLARY. *Every module is (isomorphic to) a quotient of a free module.*

PROOF. Let M be a module. We claim that there exists a free module L and a surjective homomorphism $f \in \operatorname{Hom}_R(L, M)$. Then $L/\ker f \simeq M$. Let $\{m_i : i \in I\}$ be a generating set of M (note that such a generating set always exists, as one could take, for example, the set $\{m : m \in M\}$) and let $L = R^{(I)}$. Then L is free and $f \colon R^{(I)} \to M$, $\delta_i \mapsto m_i$, is a surjective homomorphism. $\qquad\square$

§ 22. Projective modules

22.1. DEFINITION. Let R be a ring and P an R-module. We say that P is **projective** if for every surjective module homomorphism $f\colon N \to T$ and every module homomorphism $f\colon P \to T$, there exists a module homomorphism $\varphi\colon P \to N$ such that the diagram

$$
\begin{array}{ccc}
 & & P \\
 & \swarrow^{\varphi} & \downarrow^{h} \\
N & \xrightarrow{\ f\ } T & \longrightarrow 0
\end{array}
$$

commutes.

22.2. PROPOSITION. *Let*

$$
0 \longrightarrow A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C \longrightarrow 0
$$

be an exact sequence of R-modules. If C is projective, then $A \oplus C \simeq B$.

PROOF. By considering the diagram

$$
\begin{array}{ccc}
 & & C \\
 & \swarrow^{h} & \| \\
B & \xrightarrow{\ g\ } C & \longrightarrow 0
\end{array}
$$

we get a homomorphism $h\colon C \to B$ such that $gh = \mathrm{id}_C$.

Let $\varphi\colon A \oplus C \to B$, $(a,c) \mapsto f(a) + h(c)$. A simple calculation shows that φ is a module homomorphism.

We prove that φ is injective. If $\varphi(a,c) = 0$, then $f(a) + h(c) = 0$. By applying g we get that $0 = g(f(a)) + g(h(c)) = c$ and hence, since f is injective and $f(a) = 0$, it follows that $(a,c) = (0,0)$.

Now we prove that φ is surjective. Let $b \in B$. We need to find $(a,c) \in A \oplus C$ such that $\varphi(a,c) = b$. Let $c = g(b) \in C$. Since

$$
g(b - h(c)) = g(b) - gh(c) = g(b) - c,
$$

it follows that $b - h(c) \in \ker g = f(A)$. This means that $b - h(c) = f(a)$ for some $a \in A$. Now $b \in \varphi(A \oplus C)$, as

$$
\varphi(a,c) = f(a) + h(c) = b - h(c) + h(c) = b. \qquad \square
$$

22.3. PROPOSITION. *Let R be a ring and M a free R-module. Then M is projective.*

PROOF. We will prove that there exists a homomorphism φ that makes the diagram

$$
\begin{array}{ccc}
 & & M \\
 & \swarrow^{\varphi} & \downarrow^{h} \\
N & \xrightarrow{\ f\ } T & \longrightarrow 0
\end{array}
$$

commutative. Let $\{m_i : i \in I\}$ be a basis of M. Since f is surjective, for each $i \in I$ there exists $n_i \in N$ such that $f(n_i) = h(m_i)$. Since M is free, there exists a unique homomorphism $\varphi\colon M \to N$ such that $\varphi(m_i) = n_i$ for all $i \in I$. Thus homomorphism is such that $f\varphi = h$. $\quad\square$

§ 23. Quotient fields

Let R be an integral domain and $S = R \setminus \{0\}$. On $R \times S$ we define the following relation:

$$(r, s) \sim (r_1, s_1) \iff rs_1 - r_1 s = 0.$$

23.1. EXERCISE. Prove that $\sim$ is an equivalence relation.

The equivalence class of (r, s) will be denoted by r/s or $\frac{r}{s}$.

It is possible to prove that the set $K(R) = (R \times S)/\sim$ of equivalence classes is a field with the operations

(23.1) $$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1}, \quad \frac{r}{s}\frac{r_1}{s_1} = \frac{rr_1}{ss_1}.$$

23.2. DEFINITION. $K(R)$ is known as the **quotient field** of R.

Simple example: $K(\mathbb{Z}) = \mathbb{Q}$.

23.3. EXERCISE. Let R be an integral domain. Prove that $K(R)$ is a field.

To prove that $K(R)$ is a field, one first needs to prove that the operations (23.1) are well-defined. For example, let us check the addition is well-defined. If $r/s \sim r'/s'$ and $r_1/s_1 \sim r_1'/s_1'$, then $r/s + r_1/s_1 \sim r'/s' + r_1'/s_1'$. In fact, since $r/s \sim r'/s'$, it follows that $rs' - r's = 0$. Similarly, $r_1 s_1' - r_1' s_1 = 0$, as $r_1/s_1 \sim r_1'/s_1'$. Thus

$$\frac{rs_1 + r_1 s}{ss_1} = \frac{r's_1' + r_1' s'}{s's_1'}$$

as

$$(rs_1 + r_1 s)s's_1' = rs_1 s's_1' + r_1 ss's_1' = r'ss_1 s_1' + r_1' s_1 ss' = (r's_1' + r_1' s)ss_1.$$

/

§ 24. Rank of a module

What can we say about the number of elements of a basis? If M has a finite basis, then every basis of M will be finite. To prove this, let M be a module and $E = \{e_i : i \in I\}$ be a basis of M. If M is finitely generated, say $M = (m_1, \ldots, m_k)$, write each m_j as a (finite) linear combination of elements of E. Then there exists a finite set $\{e_1, \ldots, e_m\}$ that generates M. Since E is a basis, it follows that $\{e_1, \ldots, e_m\} = E$ and hence E is finite.

24.1. EXERCISE. Let M be a free module with an infinite basis E. Prove that every basis of M has cardinality $|E|$.

Under additional assumptions the previous exercise also holds for finite bases.

24.2. THEOREM. *Let R be an integral domain. If M is free with a finite basis, then any two bases of M have the same number of elements.*

PROOF. Let $K = K(R)$ be the field of fractions of R. Note that $V = \mathrm{Hom}_R(M, K)$ is an abelian group and hence it is a vector space (over K) with

$$(\lambda f)(m) = \lambda f(m),$$

where $\lambda \in K$, $f \in V$ and $m \in M$.

The vector space V has a well-defined dimension. Let us compute $\dim V$. Let $\{e_1, \ldots, e_n\}$ be a basis of M. For each $i \in \{1, \ldots, n\}$ let

$$f_i \colon M \to K, \quad e_j \mapsto \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

We claim that $\{f_1, \ldots, f_n\}$ is basis of V. It generates V, as if $f \in V$, then

$$f = \sum_{i=1}^{n} f(e_i) f_i,$$

as these homomorphisms coincide in the elements of a basis of M, that is

$$f(e_j) = \left(\sum_{i=1}^{n} f(e_i) f_i \right)(e_j)$$

for all $j \in \{1, \ldots, n\}$. Moreover, $\{f_1, \ldots, f_n\}$ is linearly independent, as if $0 = \sum_{i=1}^{n} \lambda_i f_i$, then, evaluating on each e_j, it follows that

$$0 = \left(\sum_{i=1}^{n} \lambda_i f_i \right)(e_j) = \lambda_j$$

for all $j \in \{1, \ldots, n\}$. Thus $n = \dim V$. $\qquad \square$

The previous result can be proved for commutative rings.

24.3. DEFINITION. Let R be an integral domain. If M is a free finitely generated module, we define the **rank** of M as the size of a basis of M. If M is not finitely generated, we say that the rank of M is infinite.

The rank of a module M will be denoted by $\operatorname{rank}(M)$.

24.4. EXERCISE. Prove that a finitely-generated free modules have a finite basis.

§ 25. Modules over principal domains

Recall that a principal domain is a commutative ring where every ideal is principal, i.e. generated by one element and such that $xy = 0$ implies $x = 0$ or $y = 0$.

25.1. THEOREM. *Let R be a principal domain. If F is a finitely generated free R-module and N is a submodule of F, then N is free and $\operatorname{rank}(N) \leq \operatorname{rank}(F)$. In particular, N is finitely generated.*

PROOF. Recall that finitely-generated free modules have a finite basis (Exercise 24.4). We proceed by induction on $n = \operatorname{rank}(F)$. If $n = 1$, then $F \simeq {}_R R$ and since R is commutative the submodules of F are exactly the ideals of R. In particular, $N = (r)$ for some $r \in R$. If $r = 0$, then $N = \{0\}$ and the result holds. If $r \neq 0$, then $\{r\}$ is basis of N (since R is a domain) and the result holds.

Assume now that the result holds for all free modules of rank $< n$. Let F be a free module of rank n and $\{f_1, \ldots, f_n\}$ be basis of F. Let $F_n = (f_1, \ldots, f_{n-1})$. By the inductive

hypothesis, $U = N \cap F_n$ is free of rank $\leq n - 1$. Let $\{n_1, \ldots, n_k\}$ be a basis of U (by convention, if $U = \{0\}$, then $k = 0$). If $f \in F$, there exist unique $r_1, \ldots, r_n \in R$ such that

$$f = \sum_{i=1}^{n} r_i \cdot f_i.$$

There exists a well-defined surjective homomorphism

$$\varphi \colon F \to R, \quad \sum_{i=1}^{n} r_i \cdot f_i \mapsto r_n.$$

If $\varphi(N) = \{0\}$, then $N \subseteq (f_1, \ldots, f_{n-1})$ and thus $N = U$. If $\varphi(N) \neq \{0\}$, then $\varphi(N)$ is an ideal of R, say $\varphi(N) = (x)$ for some $x \in R \setminus \{0\}$. Let $n_{k+1} \in N$ be such that $\varphi(n_{k+1}) = x$. We claim that $\{n_1, \ldots, n_k, n_{k+1}\}$ is basis of N. We first prove that this is a generating set. If $n \in N$, then $\varphi(n) = rx$ for some $r \in R$. Thus $n - r \cdot n_{k+1} \in N \cap \ker \varphi = N \cap F_n = U$, as $\varphi(n - r \cdot n_{k+1}) = 0$. In particular,

$$n - r \cdot n_{k+1} \in (n_1, \ldots, n_k) \implies n \in (n_1, \ldots, n_k, n_{k+1}).$$

We claim that $\{n_1, \ldots, n_k, n_{k+1}\}$ is linearly independent. If

$$0 = \sum_{i=1}^{k+1} r_i \cdot n_i,$$

for some $r_1, \ldots, r_{k+1} \in R$, then, since $\varphi(n_i) = 0$ for all $i \in \{1, \ldots, k\}$,

$$0 = \varphi(r_{k+1} \cdot n_{k+1}) = r_{k+1} x.$$

This implies that $r_{k+1} = 0$. Thus $\sum_{i=1}^{k} r_i \cdot n_i = 0$. Since $\{n_1, \ldots, n_k\}$ is basis of U, we conclude that $r_1 = \cdots = r_k = 0$. $\qquad\square$

The previous theorem also holds for infinite bases. However, the proof requires the use of Zorn's lemma.

25.2. COROLLARY. *Let R be a principal domain. If M is a finitely generated R-module and N is a submodule of M, then N is finitely generated.*

PROOF. There exists a free module F of finite rank and a surjective homomorphism $\varphi \colon F \to M$. Since $N_1 = \varphi^{-1}(N)$ is a submodule of F, the previous theorem implies that $\mathrm{rank}(N_1) \leq \mathrm{rank}\, F < \infty$. If $\{x_1, \ldots, x_k\}$ is basis of N_1, then $\{\varphi(x_1), \ldots, \varphi(x_k)\}$ is a generating set of $\varphi(N_1) = \varphi(\varphi^{-1}(N)) = N$, as φ is surjective. N is generated by $\leq k = \mathrm{rank}(N_1) \leq \mathrm{rank}(F) < \infty$ elements. $\qquad\square$

Some exercises:

25.3. EXERCISE. Let R be a principal domain and let M be a free R-module. If S is a submodule of M such that M/S is free, then $M \simeq S \oplus (M/S)$. Moreover, S is free and

$$\mathrm{rank}(M) = \mathrm{rank}(S) + \mathrm{rank}(M/S).$$

25.4. EXERCISE. Let R be a principal domain. If M is a free R-module of rank n, then every linearly independent subset of M contains at most n elements.

25.5. EXERCISE. Let R be a principal domain. and M and N be free R-modules. Prove that $M \simeq N$ if and only if $\operatorname{rank}(M) = \operatorname{rank}(N)$.

25.6. EXERCISE. Let R be a principal domain. If M is a free R-module of finite rank n and $\{s_1, \dots, s_n\}$ is a generating set, then $\{s_1, \dots, s_n\}$ is a basis of M.

Let R be an integral domain, the **torsion** of an R-module M is defined as the subset

$$T(M) = \{m \in M : r \cdot m = 0 \text{ for some non-zero } r \in R\}.$$

It is an exercise to show that $T(M)$ is a submodule of M. A module M **is torsion-free** if $T(M) = \{0\}$ and it is a **torsion** module if $T(M) = M$. We also say that M **has torsion** if $T(M) \neq \{0\}$.

25.7. EXERCISE. If $M \simeq N$, then $T(M) \simeq T(N)$.

25.8. EXERCISE. Prove that $T(\bigoplus_{i \in I} M_i) \simeq \bigoplus_{i \in I} T(M_i)$.

25.9. EXERCISE. Let R be a principal domain and M be an R-module. Prove that if M is finitely generated and $S \subseteq M$ is a free submodule such that M/S is torsion-free, then M is free.

The torsion generalizes the concept of elements of finite order in abelian groups. For example, $T(\mathbb{Z}/n) = \mathbb{Z}/n$, $T(\mathbb{Q}) = \{0\}$ and

$$T(\mathbb{Z} \times \mathbb{Z}/3) \simeq T(\mathbb{Z}) \times T(\mathbb{Z}/3) \simeq \{0\} \times \mathbb{Z}/3 \simeq \mathbb{Z}/3.$$

25.10. EXAMPLE. Let R be a ring, viewed as an R-module with left multiplication. Then $T(R) = \{r \in R : rs = 0 \text{ for some non-zero } s \in R\}$.

25.11. EXAMPLE. Let M be the module (over $\mathbb{Z}$) of integer sequences, that is $M = \mathbb{Z}^I$, where $I = \{1, 2, 3, \dots\}$. Then $T(M) = \{0\}$.

25.12. EXAMPLE. If V is a real finite-dimensional vector space and $f \colon V \to V$ is a linear transformation, V is a module (over $\mathbb{R}[X]$) with

$$\left(\sum_{i=0}^{m} a_i X^i\right) \cdot v = \sum_{i=0}^{m} a_i f^i(v).$$

We claim that V is a torsion module, that is $V = T(V)$. Let $n = \dim V$. If $v \in V$, then $\{v, f(v), \dots, f^n(v)\}$ is linearly dependent, as it has $n+1$ elements. In particular, there exist $a_0, \dots, a_n \in \mathbb{R}$ not all zero such that

$$0 = \sum_{i=0}^{n} a_i f^i(v) = \left(\sum_{i=0}^{n} a_i X^i\right) \cdot v.$$

Thus $v \in T(V)$.

25.13. THEOREM. *Let R be a principal domain and M be a finitely generated R-module. If $T(M) = \{0\}$, then M is free.*

PROOF. Without loss of generality, we may assume that M is non-zero. By assumption, $M = (X)$ for some finite set X. Without loss of generality, we may assume that $0 \notin X$. If $x \in X$, then $r \cdot x = 0 \iff r = 0$, as $T(M) = \{0\}$. Let $S = \{x_1, \ldots, x_k\} \subseteq X$ be maximal with respect to the following property:

$$r_1 \cdot x_1 + \cdots + r_k \cdot x_k = 0 \text{ for } r_1, \ldots, r_k \in R \implies r_1 = \cdots = r_k = 0.$$

Let $F = (S)$ be the free module with basis S. If $X = S$, we are done. If $y \in X \setminus S$, then there exist $r_y, r_1, \ldots, r_k \in R$ not all zero such that

$$r_y \cdot y + \sum_{i=1}^{k} r_i \cdot x_i = 0.$$

Since $r_y \cdot y = -\sum_{i=1}^{k} r_i \cdot x_i \in F$, it follows that $r_y \neq 0$, as $r_y = 0$ implies $r_1 = \cdots = r_k = 0$. Since X is finite,

$$r = \prod_{y \in X \setminus S} r_y$$

is well-defined, as R is commutative and $r \cdot X \subseteq F$. If $f \colon M \to M$, $x \mapsto r \cdot x$, then f is a homomorphism such that $f(M) = r \cdot M$.

Since $T(M) = \{0\}$, it follows that $\ker f = \{0\}$. Thus

$$r \cdot M = f(M) \simeq M.$$

To finish the proof, we show that $r \cdot M \subseteq F$. Let $m \in M$. Since $M = (X)$, there exist $s_{i_1}, \ldots, s_{i_m} \in R$ such that $m = \sum s_j \cdot x_{i_j}$. Then

$$r \cdot m = \sum (r s_j) \cdot x_{i_j} = \sum s_j \cdot (r \cdot x_{i_j}) \in F,$$

as each $r \cdot x_{i_j} \in r \cdot X \subseteq F$. In particular, since R is commutative, $r \cdot M$ is a submodule of F and hence $r \cdot M$ is a free module. $\qquad\square$

25.14. THEOREM. *Let R be a principal domain. If M is a finitely generated R-module, then $M = T(M) \oplus F$, where $F \simeq M/T(M)$ is finitely generated and free. The torsion submodule is unique and F is unique up to isomorphism.*

PROOF. We first prove that $T(M/T(M)) \simeq \{0\}$. If $x + T(M) \in T(M/T(M))$, then there exists $r \in R \setminus \{0\}$ such that $r \cdot (x + T(M)) = T(M)$. Then $r \cdot x \in T(M)$, that is, there exists $s \in R \setminus \{0\}$ such that $s \cdot (r \cdot x) = (sr) \cdot x = 0$. Since $sr \neq 0$, it follows that $x \in T(M)$.

Since M is finitely generated, $M/T(M)$ is finitely generated. Moreover, $M/T(M)$ is torsion-free. It follows that $M/T(M)$ is free. Consider the exact sequence

$$0 \longrightarrow T(M) \overset{\iota}{\longrightarrow} M \overset{\pi}{\longrightarrow} M/T(M) \longrightarrow 0$$

where ι is the inclusion map and π is the canonical map. Since $M/T(M)$ is free, there exists an R-module homomorphism $h \colon M/T(M) \to M$ such that $\pi h = \mathrm{id}$, see Proposition 22.3. This homomorphism is needed to prove that $M \simeq T(M) \oplus M/T(M)$, see Proposition 22.2.

Let us prove uniqueness. Suppose that $M = T \oplus L$, where T is a torsion module and L is free. We first prove that $T = T(M)$. On the one hand, $T \subseteq T(M)$. On the other hand, if $m \in T(M)$, then $m = t + l$ for some $t \in T$ and $l \in L$. In particular, $r \cdot m = 0$ and $s \cdot t = 0$ for some non-zero $r, s \in R$. Since R is commutative,

$$0 = (rs) \cdot m = (rs) \cdot (t + l) = (rs) \cdot t + (rs) \cdot l = (rs) \cdot l.$$

and thus $l \in T(L)$. Since L is free, $T(L) = \{0\}$ (because $T(L)$ is free and hence every basis element x of $T(L)$ is such that $\{x\}$ is linearly independent, a contradiction). Thus $l = 0$ and hence $m = t \in T$. The free part is unique up to isomorphism because it is isomorphic to $M/T(M)$. $\qquad\square$

§ 26. The Smith normal form

We finish the course with an algorithm that allows us to understand the structure of certain finitely generated modules. We will discuss the case of modules over euclidean domains, as in this case the algorithm is constructive.

Let M be a finitely generated module and $\{m_1, \ldots, m_k\}$ be a set of generators. There exists a surjective module homomorphism

$$\varphi \colon R^k \to M, \quad (r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot m_i,$$

and hence $M \simeq R^k / \ker \varphi$. The submodule $\ker \varphi$ of R^k is the **relations module** of M. Since R is an euclidean domain, R is a principal domain. Since M is finitely generated, then so is the submodule $\ker \varphi$ of R^k. Let $\{e_1, \ldots, e_l\}$ be a generating set of $\ker \varphi$, say

$$e_1 = (a_{11}, a_{12}, \ldots, a_{1k}),$$
$$e_2 = (a_{21}, a_{22}, \ldots, a_{2k}),$$
$$\vdots$$
$$e_l = (a_{l1}, a_{l2}, \ldots, a_{lk}).$$

The matrix $A = (a_{ij})_{1 \leq i \leq l, 1 \leq j \leq k}$ is the **relations matrix** of M with respect to $\{m_1, \ldots, m_k\}$ and $\{e_1, \ldots, e_l\}$.

CLAIM. If $P \in R^{l \times l}$ is invertible, then the rows $\{f_1, \ldots, f_l\}$ of PA generate $\ker \varphi$. Moreover, PA is the relations matrix with respect to $\{m_1, \ldots, m_k\}$ and $\{f_1, \ldots, f_l\}$.

Let us prove the claim. Assume that $P = (p_{ij})$. The rows of PA are

$$f_1 = p_{11}e_1 + \cdots + p_{1l}e_l,$$
$$f_2 = p_{21}e_1 + \cdots + p_{2l}e_l,$$
$$\vdots$$
$$f_l = p_{l1}e_1 + \cdots + p_{ll}e_l.$$

Moreover, $f_j \in \ker \varphi$ for all $j \in \{1, \ldots, l\}$. Since P is invertible, the set $\{f_1, \ldots, f_l\}$ generates $\ker \varphi$. Indeed, each e_j is a linear combination of the f_i's,

$$\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_l \end{pmatrix} = P^{-1} \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_l \end{pmatrix}.$$

In particular, PA is the relations matrix with respect to $\{m_1, \ldots, m_k\}$ and $\{f_1, \ldots, f_l\}$.

CLAIM. If $Q \in R^{k \times k}$ is invertible and $Q^{-1} = (q_{ij})$ and for each $j \in \{1, \ldots, k\}$ we define $n_j = \sum_{i=1}^{k} q_{ji} \cdot m_i$, the set $\{n_1, \ldots, n_k\}$ generates M and the rows of AQ generate $\ker \varphi$. Moreover, AQ is the relations matrix with respect to $\{n_1 \ldots, n_k\}$.

Now we prove the claim. Since

$$
\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} = Q^{-1} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix},
$$

it follows that

$$
\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = A \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = (AQ) \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}.
$$

This implies that the rows of AQ are relations with respect to the generating set $\{n_1, \ldots, n_k\}$. Let $\psi \colon R^k \to M$, $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot n_i$.

The rows of AQ generate $\ker \psi$ with respect to $\{n_1, \ldots, n_k\}$. If $(r_1, \ldots, r_k) \in \ker \psi$, then $\sum_{i=1}^{k} r_i \cdot n_i = 0$. Write

$$
0 = (r_1 \cdots r_k) Q^{-1} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = (r_1 \cdots r_k) \begin{pmatrix} n_1 \\ \vdots \\ n_k \end{pmatrix}.
$$

We remark that each e_j belongs to R^k. Thus

$$
(r_1 \cdots r_k) Q^{-1} = \left(\sum_{i=1}^{k} r_i q_{i1}, \sum_{i=1}^{k} r_i q_{i2}, \ldots, \sum_{i=1}^{k} r_i q_{ik} \right) \in \ker \varphi.
$$

Since $\ker \varphi$ is generated by $\{e_1, \ldots, e_l\}$, there exist $s_1, \ldots, s_l \in R$ such that

$$
(r_1 \cdots r_k) Q^{-1} = \sum_{i=1}^{l} s_i \cdot e_i,
$$

that is

$$
(r_1 \ldots r_k) Q^{-1} = (s_1 \cdots s_l) \begin{pmatrix} e_1 \\ \vdots \\ e_l \end{pmatrix} = (s_1 \cdots s_l) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lk} \end{pmatrix}.
$$

Rewriting this expression as

$$
(r_1 \cdots r_k) = (s_1 \cdots s_l) AQ,
$$

we conclude that $(r_1, \ldots, r_k)$ is a linear combination of the rows of AQ, as

$$
(r_1, \ldots, r_k) = \left(\sum_{i=1}^{l} s_i \cdot x_{i1}, \ldots, \sum_{i=1}^{l} s_i \cdot x_{ik} \right) = \sum_{i=1}^{l} s_i \cdot (x_{i1}, \ldots, x_{ik}).
$$

Therefore $\{n_1, \ldots, n_k\}$ generates M and the rows of AQ generate the corresponding relations submodule and AQ is the relations matrix with respect to $\{n_1, \ldots, n_k\}$ and $\{e_1, \ldots, e_l\}$.

26.1. PROPOSITION. *Let A be the relations matrix of a finitely generated module M with k generators. If there exist invertible matrices $P \in R^{l \times l}$ and $Q \in R^{k \times k}$ such that*

$$PAQ = \begin{pmatrix} a_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & a_2 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & a_r & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{pmatrix}$$

where $a_i \neq 0$ for all $i \in \{1, \ldots, r\}$ and $a_i \mid a_{i+1}$ for all $i \in \{1, \ldots, r-1\}$, then

$$M \simeq R/(a_1) \oplus \cdots \oplus R/(a_r) \oplus R^{k-r}.$$

PROOF. The matrix PAQ is the relations matrix with respect to the generating set $\{m_1, \ldots, m_k\}$ of M and respect to the relations submodule given by the rows of PAQ. If

$$\varphi \colon R^k \to M, \quad (r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot m_i,$$

then $R^k/\ker\varphi \simeq M$, as φ is a surjective homomorphism. For each $j \in \{r+1, \ldots, k\}$ let $a_j = 0$. Let

$$\psi \colon R^k \to R/(a_1) \oplus \cdots \oplus R/(a_k), \quad (s_1, \ldots, s_k) \mapsto (s_1 + (a_1), \ldots, s_k + (a_k)).$$

A straightforward calculation shows that

$$\ker\psi = (a_1) \oplus \cdots \oplus (a_k).$$

Thus $R^k/\ker\psi \simeq \oplus_{i=1}^{k} R/(a_i)$.

It is an exercise to show that $\ker\varphi = \ker\psi$.

Therefore $M \simeq R/(a_1) \oplus \cdots \oplus R/(a_k)$. To finish the proof we need to note that $R/(a_i) \simeq R$ for all $i \in \{r+1, \ldots, k\}$. $\qquad\square$

The decomposition given in the previous proposition is known as the **Smith normal form** of the matrix M. How can we find the matrices P and Q? Consider the following matrix operations:

1) Switch the i-th row and j-th row, that is $R_i \leftrightarrow R_j$.
2) Replace row R_i by $R_i + \lambda R_j$ for some $\lambda \in R$ and $j \neq i$.
3) Switch the i-th column and the j-th column, that is $C_i \leftrightarrow C_j$.
4) Replace column C_i by $C_i + \lambda C_j$ for some $\lambda \in R$ and $j \neq i$.
5) Replace row R_i (resp. column C_i) by λR_i (resp. λC_i) for some $\lambda \in \mathcal{U}(R)$.

These operations are invertible. For example, the first operation corresponds to multiply A on the left by a permutation matrix. The second operation corresponds to multiply A by $I + \lambda E_{ij}$ on the left, where

$$(E_{ij})_{kl} = \begin{cases} 1 & \text{if } i = k \text{ and } j = l, \\ 0 & \text{otherwise.} \end{cases}$$

Concrete examples:

$$E_{3,1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad E_{23} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

Similarly, column operations correspond to multiply on the right the matrix A either by a permutation matrix or a matrix of the form $I + \lambda E_{ij}$.

26.2. THEOREM (Smith's normal form). *Let R be an euclidean domain. If $A \in R^{l \times k}$, there exists invertible matrices $P \in R^{l \times l}$ and $Q \in R^{k \times k}$ such that*

$$PAQ = \begin{pmatrix} a_1 & 0 & \cdots & \cdot & \cdot & \cdots & 0 \\ 0 & a_2 & \cdots & \cdot & \cdot & \cdots & 0 \\ \vdots & & \ddots & & & & \vdots \\ 0 & \cdot & \cdots & a_r & \cdot & \cdots & 0 \\ 0 & \cdot & \cdots & \cdot & 0 & \cdots & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdot & \cdots & \cdot & \cdot & \cdots & 0 \end{pmatrix}$$

where $a_i \neq 0$ for all $i \in \{1, \ldots, r\}$ and $a_i \mid a_{i+1}$ for all $i \in \{1, \ldots, r-1\}$. Moreover, the elements $a_1, \ldots, a_r$ are unique up to multiplication by units.

SKETCH OF THE PROOF. We only prove the existence. Assume that (R, φ) be an euclidean domain. We need to show that A can be turned into a matrix of the form

$$B = \begin{pmatrix} b_{11} & 0 & \cdots & 0 \\ 0 & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & b_{n2} & \cdots & b_{nm} \end{pmatrix}$$

where each b_{ij} is divisible by b_{11}. Then we apply the same procedure to the submatrix

$$\begin{pmatrix} \frac{b_{22}}{b_{11}} & \cdots & \frac{b_{2m}}{b_{11}} \\ \vdots & & \vdots \\ \frac{b_{n2}}{b_{11}} & \cdots & \frac{b_{nm}}{b_{11}} \end{pmatrix}$$

and repeat the method until we cannot continue.

Let us show how to get the matrix B. By applying row and column operations we may assume that the coefficient of A with minimal positive Euclidean norm appears in position $(1, 1)$. If some a_{i1} is not divisible by a_{11}, we use the division algorithm to write $a_{i1} = a_{11}u + r$ for some $u \in R$ and $r \in R$ with $\varphi(r) < \varphi(a_{11})$. The transformation $R_i \leftarrow R_i - uR_1$ turns our matrix into a matrix that has r in position $(i, 1)$. Similarly, if some a_{1j} is not divisible by a_{11}, then $a_{1j} = va_{11} + s$ with $\varphi(s) < \varphi(a_{11})$. By applying $C_j \leftarrow C_j - vC_1$ our matrix turns into a matrix that has s in position $(1, j)$. If every a_{i1} is divisible by a_{11}, say $a_{i1} = a_{11}\lambda_i$, then apply $R_i \leftarrow \lambda_i R_1 - R_i$. Similarly, if every a_{1j} is divisible by a_{11}, say $a_{1j} = a_{11}\mu_j$, then apply $C_j \leftarrow \mu_j C_1 - C_j$. In this way we replace our matrix by a matrix of the form

$$\begin{pmatrix} a_{11} & 0 \\ 0 & A_1 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}.$$

If some entry of the matrix A_1 is not divisible by a_{11}, apply either $R_1 \leftarrow R_1 + R_i$ or $C_1 \leftarrow C_1 + C_j$ and repeat the procedure described before. $\qquad\square$

We refer to Artin's book [1, §14] for a detailed exposition of the Smith normal when the base ring R is $\mathbb{Z}$ or $K[X]$ for any field K. For an application of the Smith's normal to explicit calculations related to homology groups, see [6, §11]. Here we will explain the algorithm with examples.

26.3. EXAMPLE. Let

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 8 & 6 & 4 \\ 3 & 1 & 0 \end{pmatrix}.$$

Let us compute the Smith's normal form of A. Since the element with smallest positive norm appears in position $(3, 2)$, we apply the operations $R_1 \leftrightarrow R_3$ and $C_1 \leftrightarrow C_2$ to transform A into

$$\begin{pmatrix} 1 & 3 & 0 \\ 6 & 8 & 4 \\ 5 & 2 & 3 \end{pmatrix}.$$

To obtain zeros in positions $(1, 2)$, $(1, 3)$, $(2, 1)$ and $(2, 3)$ we apply the transformations $R_2 \leftarrow 6R_1 - R_2$, $R_3 \leftarrow 5R_1 - R_3$ and $C_2 \leftarrow 3C_1 - C_2$. Then our matrix turns into

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -10 & -4 \\ 0 & -13 & -3 \end{pmatrix}.$$

Multiply the second and the third row by -1:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & 4 \\ 0 & 13 & 3 \end{pmatrix}.$$

We perform the same procedure to the submatrix $\begin{pmatrix} 10 & 4 \\ 13 & 3 \end{pmatrix}$. We want the smallest element of the submatrix in position $(2, 2)$. For that purpose, apply $R_1 \leftrightarrow R_2$ and $C_2 \leftrightarrow C_1$:

$$\begin{pmatrix} 3 & 13 \\ 4 & 10 \end{pmatrix}.$$

Write $13 = 3 \cdot 4 + 1$ and apply $C_2 \leftarrow C_2 - 4C_1$ to obtain $\begin{pmatrix} 3 & 1 \\ 4 & -6 \end{pmatrix}$. Interchange the first two columns to obtain $\begin{pmatrix} 1 & 3 \\ -6 & 4 \end{pmatrix}$. Apply now $R_2 \leftarrow 6R_1 + R_2$. To the resulting matrix we apply $C_2 \leftarrow 3C_1 - C_2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 22 \end{pmatrix}.$$

Hence we find the Smith's normal form of the matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -22 \end{pmatrix}.$$

The previous example can be easily solved with Magma:

```
K := Integers();
M := MatrixAlgebra(K, 3);
A := M ! [[2,5,3],[8,6,4],[3,1,0]];
S, P, Q := SmithForm(A);
S;
[ 1  0  0]
[ 0  1  0]
[ 0  0 22]
> S eq P*A*Q;
true
```

How to interpret the Smith normal form if the matrix is not a square matrix? To understand the quotient

$$M = \mathbb{Z}^n / \langle e_1, \ldots, e_m \rangle$$

with $m < n$, each of the $n - m$ missing columns of the Smith's normal form of the matrix gives a factor isomorphic to $\mathbb{Z}$. Thus

$$M \simeq \mathbb{Z}^{n-m} \times M_1$$

where M_1 is the module obtained from the Smith's normal form. If $n < m$, then one only needs to ignore the $m - n$ last columns, which will all be zero columns.

26.4. EXAMPLE. Let M be the abelian group with generators m_1, m_2, m_3 and relations

$$8m_1 + 4m_2 + 8m_3 = 0, \quad 4m_1 + 8m_2 + 4m_3 = 0.$$

The matrix of relations is then

$$A = \begin{pmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \end{pmatrix}.$$

We claim that $M \simeq \mathbb{Z}/4 \times \mathbb{Z}/12$. Apply $R_1 \leftarrow 2R_2 - R_1$ to obtain

$$\begin{pmatrix} 0 & 12 & 0 \\ 4 & 8 & 4 \end{pmatrix}.$$

The row operation used corresponds to multiplying on the left by the invertible matrix $\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}$. Thus $\begin{pmatrix} 0 & 12 & 0 \\ 4 & 8 & 4 \end{pmatrix}$ corresponds to the set of generators $\{m_1, m_2, m_3\}$ and relations $12m_2 = 0$ and $4m_1 + 8m_2 + 4m_3 = 0$. Apply $C_2 \leftarrow C_2 - 2C_1$ and $C_3 \leftarrow C_3 - C_1$ to obtain the matrix

$$\begin{pmatrix} 0 & 12 & 0 \\ 4 & 0 & 0 \end{pmatrix},$$

which corresponds to generators $\{m_1 + 2m_2 + m_3, m_2\}$ and relations

$$12m_2 = 0, \quad 4(m_1 + 2m_2 + m_3) = 0.$$

The first column operation corresponds to multiplying on the right by the matrix

$$I - 2E_{12} = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and the second one to right multiplication by the matrix

$$I - E_{13} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Finally, interchange the first two rows to obtain the Smith's normal form of A:

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}.$$

This matrix corresponds to the set of generators $\{m_2, m_1 + 2m_2 + m_3\}$ and relations

$$4(m_1 + 2m_2 + m_3) = 0, \quad 12m_2 = 0.$$

The column operation used corresponds to left multiplication by the permutation matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus $M \simeq \mathbb{Z}/4 \times \mathbb{Z}/12$. We also obtained that

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$$

and that

$$Q = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that the matrices P and Q are not uniquely determined. Here is the Magma code that solves the previous exercise:

```
> A := Matrix(Integers(), 2, 3, [8,4,8,4,8,4]);
> S,P,Q := SmithForm(A);
> S;
[ 4  0  0]
[ 0 12  0]
> ElementaryDivisors(A);
[ 4, 12 ]
```

26.5. EXAMPLE. Let M be the abelian group generated by $\{m_1, \ldots, m_4\}$ and let K be the subgroup of M generated by $\{e_1, e_2, e_3\}$, where

$$e_1 = 22m_3, \quad e_2 = -2m_1 + 2m_2 - 6m_3 - 4m_4, \quad e_3 = 2m_1 + 2m_2 + 6m_3 + 8m_4.$$

We want to determine the structure of M/K. The matrix of relations is

$$A = \begin{pmatrix} 0 & 0 & 22 & 0 \\ -2 & 2 & -6 & -4 \\ 2 & 2 & 6 & 8 \end{pmatrix}.$$

Apply $R_1 \leftrightarrow R_3$ and then $R_2 \leftarrow R_1 + R_2$ to obtain

$$\begin{pmatrix} 2 & 2 & 6 & 8 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}.$$

Apply $C_2 \leftarrow C_2 - C_1$, $C_3 \leftarrow C_3 - 3C_1$ and $C_4 \leftarrow C_4 - 4C_1$ to obtain

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 \\ 0 & 0 & 22 & 0 \end{pmatrix}.$$

Apply $C_4 \leftarrow C_4 - C_2$ to get

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 22 & 0 \end{pmatrix}.$$

Note that $4 \nmid 22$. Apply $R_2 \leftarrow R_2 + R_3$, $C_3 \leftarrow C_3 - 5C_2$, $C_3 \leftarrow C_2$, $R_3 \leftarrow R_3 - 11R_2$ and $C_3 \leftarrow C_3 - C_2$ to get

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -44 & 0 \end{pmatrix}.$$

The group M/K has basis $\{n_1, n_2, n_3, n_4\}$ and relations $2n_1 = 0$, $2n_2 = 0$ and $44n_3 = 0$. Thus $M/K \simeq \mathbb{Z} \times (\mathbb{Z}/2)^2 \times (\mathbb{Z}/44)$.

26.6. EXAMPLE. Let $A = \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} -1 \\ 5 \end{pmatrix}$. Let us solve the linear system $AX = b$ in the integers. We need to compute Smith's normal form of A. For example, computer calculations show that

$$P = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & -2 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}, \quad S = PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Note that the matrix S is unique, but not the matrices P and Q. To solve $AX = b$ we proceed as follows. Let $Y = Q^{-1}X$. Then $AX = b$ implies that

$$SY = (PAQ)(Q^{-1}X) = Pb = \begin{pmatrix} 5 \\ 1 \end{pmatrix}.$$

Write $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$. Since $Q^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, it follows that $Y = Q^{-1}X = \begin{pmatrix} x + 2z \\ y + z \\ y \end{pmatrix}$ and hence $SY = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$ turns into

$$\begin{pmatrix} x + 2z \\ y + z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x + 2z \\ y + z \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}.$$

It follows that the solution of $AX = b$ is then $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 5 - 2z \\ 1 - z \\ z \end{pmatrix}$ for $z \in \mathbb{Z}$.

26.7. EXERCISE. Solve $AX = b$ in $\mathbb{Z}$ for $A = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} 5 \\ 1 \\ 7 \end{pmatrix}$.

26.8. EXERCISE. Prove that $\mathbb{Z}^3/\langle(6,6,4),(6,12,8)\rangle \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/6$.

26.9. EXERCISE. Prove that the abelian group with generators a, b and c with relations

$$3a + 2b + c = 0, \quad 8a + 4b + 2c = 0, \quad 7a + 6b + 2c = 0, \quad 9a + 6b + c = 0,$$

is cyclic of order four.

26.10. EXERCISE. Compute the Smith normal form of $\begin{pmatrix} 1+i & 2-i \\ 3 & 5i \end{pmatrix} \in M_2(\mathbb{Z}[i])$.

26.11. EXERCISE. Compute the Smith normal form of

$$\begin{pmatrix} 7 & X & 0 & -X \\ 0 & X-3 & 0 & 3 \\ 0 & 0 & X-4 & 0 \\ X-6 & -1 & 0 & X+1 \end{pmatrix} \in M_4(\mathbb{Q}[X]).$$

26.12. EXERCISE. Let G be an abelian group of rank n with basis $\{x_1, \ldots, x_n\}$. For $i \in \{1, \ldots, n\}$ let

$$y_i = \sum_{j=1}^{n} a_{ij} x_j,$$

where $A = (a_{ij}) \in M_n(\mathbb{Z})$. Then $\{y_1, \ldots, y_n\}$ is a basis of G if and only if A is unimodular, that is $\det A \in \{-1, 1\}$.

Some solutions

1.6.

1) Since $x0 = x(0+0) = x0 + x0$, it follows that $x0 = 0$. Similarly, $0x = 0$.

2) $0 = x0 = x(y + (-y)) = xy + x(-y)$. Thus $-xy = x(-y)$.

3) Assume that $1 = 0$ and let $x \in R$. Using the first item, $x = x1 = x0 = 0$.

1.16.

1) To see that $S \cap T$ is a subring, we first note that $S \cap T$ is a subgroup of $(R, +)$, as the intersection of subgroups is a subgroup. Since S and T are subrings, $1 \in S \cap T$. Now let $x, y \in S \cap T$. Then $xy \in S$ and $xy \in T$, because S and T are subrings. Thus $xy \in S \cap T$.

2) To see that $\cup_{i \geq 1} R_i$ is a subring, we first note that $(\cup_{i \geq 1} R_i, +)$ is a subgroup of $(R, +)$ as the union of a sequence of subgroups is a subgroup. Since R_i are subrings, $1 \in R_i$ for every i, hence $1 \in \cup_{i \geq 1} R_i$. Finally let $x, y \in \cup_{i \geq 1} R_i$, then there exist $i, j \geq 1$ such that $x \in R_i$ and $y \in R_j$. Let $k = \max(i, j)$, then $R_i \subseteq R_k$ and $R_j \subseteq R_k$. Therefore $x, y \in R_k$ and, since R_k is a subring, $xy \in R_k \subseteq \cup_{i \geq 1} R_i$.

3) Suppose, by contradiction, that $S \cup T$ is a subring of R and that there exist $s \in S \setminus T$ and $t \in T \setminus S$. Then $s + t \in S \cup T$, so either $s + t \in S$ or $s + t \in T$. In both cases, we obtain a contradiction since either $t = (s + t) - s \in S$ or $s = (s + t) - t \in T$.

1.18. We claim that $\mathcal{U}(\mathbb{R}[X]) = \mathcal{U}(\mathbb{R}) = \mathbb{R} \setminus \{0\}$. Let $f \in \mathcal{U}(R[X])$. Then there exists $g \in \mathbb{R}[X]$ such that $fg = 1$. In particular, since the degree of the product of two polynomials over a field is the sum of their degrees, $0 = \deg(fg) = \deg(f) + \deg(g)$. Thus $\deg(f) = \deg(g) = 0$ and hence f is an invertible element of $\mathbb{R}$.

1.21. Let $x + y\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$. Observe that $(x + y\sqrt{2})(x - y\sqrt{2}) = x^2 - 2y^2 \in \mathbb{Q}$. Therefore

$$(x + y\sqrt{2})\left(\frac{x}{x^2 - 2y^2} - \frac{y\sqrt{2}}{x^2 - 2y^2}\right) = \frac{(x + y\sqrt{2})(x - y\sqrt{2})}{x^2 - 2y^2} = \frac{x^2 - 2y^2}{x^2 - 2y^2} = 1$$

and so $\frac{x}{x^2 - 2y^2} - \frac{y\sqrt{2}}{x^2 - 2y^2}$ is the inverse of $x + y\sqrt{2}$ in $\mathbb{Q}[\sqrt{2}]$.

2.4.

1) We first note that $(\cap_\alpha I_\alpha, +)$ is a subgroup of $(R, +)$, as the intersection of subgroups is a subgroup. Let now $r \in R$ and $y \in \cap_\alpha I_\alpha$. Then for every α we have that $y \in I_\alpha$, hence, since I_α is an ideal, $ry, yr \in I_\alpha$ for every α. Thus $ry \in \cap_\alpha I_\alpha$ and $yr \in \cap_\alpha I_\alpha$.

2) We first note that $(\cup_{i \geq 1} I_i, +)$ is a subgroup of $(R, +)$, as the union of a sequence of subgroups is a subgroup. Let now $r \in R$ and $y \in \cup_{i \geq 1} I_i$. Then, there exists $i \geq 1$ such that $y \in I_i$ and so $ry, yr \in I_i$, since I_i is an ideal of R. Thus $ry, yr \in \cup_{i \geq 1} I_i$.

2.6. Let I be an ideal of $\mathbb{Z}$, if $I = \{0\}$, then we are done as $I = 0\mathbb{Z}$. Suppose now $I \setminus \{0\} \neq \emptyset$, then there is at least an element $i \in I \cap \mathbb{Z}_{>0}$. So we can consider $n = \min(I \cap \mathbb{Z}_{>0})$ and we claim that $I = n\mathbb{Z}$.

Since $n \in I$ then $nx \in I$ for every $x \in \mathbb{Z}$, hence $n\mathbb{Z} \subseteq I$.

73

Vice versa, if $y \in I$ we can divide y by n obtaining $y = nq + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$. Hence $r = y - nq \in I \cap \mathbb{Z}_{\geq 0}$ and $r < n$, so $r = 0$ and thus $y = nq \in n\mathbb{Z}$ proving that $I \subseteq n\mathbb{Z}$.

2.7. We claim that the ideals of $\mathbb{Z}/n$ are of the form $d\mathbb{Z}/n$ for some $d \in \mathbb{Z}_{\geq 0}$ such that d divides n.

Let I be an ideal of $\mathbb{Z}/n$, if $I = \{0\}$, then we are done as $I = 0\mathbb{Z}/n$. Suppose now $I \setminus \{0\} \neq \emptyset$ and let d be the minimal in $\{1, \ldots, n-1\}$ such that $d \in I$. We claim that $I = n\mathbb{Z}$ and that d divides n.

If d would not divide n, then $n = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 < r < d$. But then in $\mathbb{Z}/n$ we would have $r = n - qd = -qd \in I$, a contradiction to the minimality of d.

Since $d \in I$ then $dx \in I$ for every $x \in \mathbb{Z}/n$, hence $d\mathbb{Z}/n \subseteq I$.

Vice versa, let $y \in I$, then $y = qd + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$. Hence $r = y - qd \in I$ and $0 \leq r < n$, so $r = 0$ and thus $y = qd \in d\mathbb{Z}/n$ proving that $I \subseteq d\mathbb{Z}/n$.

2.8. We claim that $\{0\}$ and $\mathbb{R}$ are the only ideals of $\mathbb{R}$. Suppose that I is an ideal of $\mathbb{R}$ and that $I \neq \{0\}$. Then there exists $x \in I \setminus \{0\}$, but then x is invertible and so $1 = x^{-1}x \in \mathbb{R}I \subseteq I$. Therefore for every $r \in \mathbb{R}$ we have that $r = r1 \in \mathbb{R}I \subseteq I$ and so $\mathbb{R} \subseteq I \subseteq \mathbb{R}$. Hence $I = \mathbb{R}$.

2.9. We will denote with E_{ij} the matrix in $M_n(R)$ with all zeros and a 1 in position (i,j).

Let J be an ideal of $M_n(R)$. We claim that $E(J) = \{r \in R : rE_{11} \in J\}$ is an ideal of R and that $J = M_n(E(J))$.

Using the fact that $(J, +)$ is a subgroup of $(R, +)$ we obtain that $(E(J), +)$ is a subgroup of R. More precisely, $0 \in E(J)$ since $0E_{11} = 0 \in J$. Given $r, s \in E(J)$, i.e. $rE_{11}, sE_{11} \in J$, then $(r+s)E_{11} = rE_{11} + sE_{11} \in J$ and $(-r)E_{11} = -(rE_{11}) \in J$, i.e. $r+s, -r \in E(J)$.

Moreover, since J is an ideal of R, $xrE_{11} = rxE_{11} = r(xE_{11}) \in RJ \subseteq J$ for every $r \in R$ and $x \in E(J)$. So $E(J)$ is an ideal of R.

Finally, we can show that $J = M_n(E(J))$ and for that we are going to use the following property: given a matrix $A = (a_{ij}) \in M_n(R)$,

(26.1) $$E_{ki}AE_{jl} = a_{ij}E_{kl} \text{ for all } i, j, k, l.$$

Consider $A = (a_{ij}) \in J$, then, by Equation 26.1, $a_{ij}E_{11} = E_{1i}AE_{j1} \in J$ for every $i, j \in \{1, \ldots, n\}$. Hence $a_{ij} \in E(J)$ for every $i, j \in \{1, \ldots, n\}$, i.e. $A \in M_n(E(J))$. Thus $J \subseteq M_n(E(J))$.

Conversely, if $A = (a_{ij}) \in M_n(E(J))$, then $A = \sum_{i,j=1}^{n} a_{ij}E_{ij}$ with $a_{ij} \in E(J)$, i.e. $a_{ij}E_{11} \in J$. But using Equation 26.1 applied for $A = Id$ we also know that $E_{ki}E_{jl} = E_{kl}$, so

$$a_{ij}E_{ij} = a_{ij}E_{i1}E_{1j} = a_{ij}E_{i1}E_{11}E_{1j} = E_{i1}(a_{ij}E_{11})E_{1j} \in J.$$

Thus $A = \sum_{i,j=1}^{n} a_{ij}E_{ij}$ is a sum of elements of J, so $A \in J$. Therefore $M_n(E(J)) = J$.

2.11. Let I be an ideal of $R[X]$. If $I = \{0\}$, then it is principal generated by 0.

Suppose now $I \neq \{0\}$, then we can consider a polynomial $g(X) \in I$ such that $\deg(g(X))$ is minimal. We claim that $I = (g(X))$.

Clearly $(g(X)) \subseteq I$, since $g(X) \in I$.

Conversely, consider $f(X) \in I$, then there exist $q(X), r(X) \in \mathbb{R}[X]$ with $r(X) = 0$ or $\deg(r(X)) < \deg(g(X))$ such that $f(X) = q(X)g(X) + r(X)$. Assume that $r(X) \neq 0$. Since

$$r(X) = f(X) - q(X)g(X) \in I,$$

the minimality of $\deg g(X)$ implies that $\deg(r(X)) \geq \deg(g(X))$, a contradiction. Thus $r(X) = 0$ and hence $f(X) = q(X)g(X) \in (g(X))$. Therefore $I \subseteq (g(X))$.

2.12. If x is a unit, then $yx = xy = 1$ for some $y \in R$ and hence $ryx = r$ for all $r \in R$. Conversely, if $R = (x)$, then, in particular, $1 \in R = (x)$ and hence $1 = xy$ and $1 = zx$ for some $y, z \in R$. Now $z = z1 = z(xy) = (zx)y = 1y = y$ and hence x is a unit.

3.10. Let $f \colon \mathbb{Z}/6 \to \mathbb{Z}/15$ be a ring homomorphism. Then

$$0 = f(0) = f(6) = f(\underbrace{1 + \cdots + 1}_{6-\text{times}}) = 6f(1) = 6,$$

a contradiction, as $6 \neq 0$ in $\mathbb{Z}/15$.

3.11. Let $x_0 = f(X) \in \mathbb{R}$, and let $p(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{R}[X]$. Since f is a ring homomorphism and $f(a_i) = a_i$ for every $i \in \{0, \dots, n\}$,

$$f(p(X)) = f\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} f(a_i) f(X)^i = \sum_{i=0}^{n} a_i f(X)^i = \sum_{i=0}^{n} a_i x_0^i = p(x_0).$$

So f is the evaluation map at x_0

4.2. From group theory, we know that R/I is abelian group with addition

$$(x + I) + (y + I) = (x + y) + I$$

and neutral element $0 + I = I$.

We have already seen that multiplication is well-defined. As an example, we also showed that the left distributive property holds, that is

$$(x + I)\left((y + I) + (z + I)\right) = (x + I)(y + I) + (x + I)(z + I)$$

for all $x, y, z \in R$. The right distributivity is similar:

$$\left((x + I) + (y + I)\right)(z + I) = (x + I)(z + I) + (y + I)(z + I)$$

for all $x, y, z \in R$. Let us prove the associativity of the multiplication:

$$\begin{aligned}
(x + I)\left((y + I)(z + I)\right) &= (x + I)(yz + I) \\
&= x(yz) + I \\
&= (xy)z + I \\
&= (xy + I)(z + I) \\
&= \left((x + I)(y + I)\right)(z + I).
\end{aligned}$$

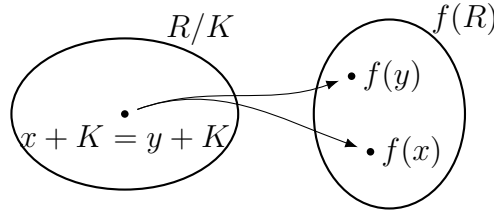Finally, let us see why $1 + I$ is the neutral element of the multiplication:

$$(x + I)(1 + I) = x1 + I = x + I = 1x + I = (1 + I)(x + I)$$

for all $x \in R$.

4.6. We first note that $K = \ker f$ is an ideal of R. Thus R/K is a ring. Let

$$\varphi \colon R/K \to f(R), \quad x + K \mapsto f(x).$$

We first need to prove that φ is a well-defined map, that is if $x + K = y + K$, then $f(x) = f(y)$. Thus we want to avoid situations as in the following picture:

To prove this fact, we proceed as follows:

$$x + K = y + K \implies x - y \in K = \ker f$$
$$\implies f(x) - f(y) = f(x - y) = 0$$
$$\implies f(x) = f(y).$$

Now we need to prove that φ is a ring homomorphism. First we prove that $\varphi(1+K) = 1$:

$$\varphi(1 + K) = f(1) = 1.$$

To finish the proof of the fact that φ is a ring homomorphism, let $x, y \in R$. Then

$$\varphi((x + K) + (y + K)) = \varphi(x + y + K)$$
$$= f(x + y)$$
$$= f(x) + f(y)$$
$$= \varphi(x + K) + \varphi(y + K).$$

and

$$\varphi((x + K)(y + K)) = \varphi(xy + K)$$
$$= f(xy)$$
$$= f(x)f(y)$$
$$= \varphi(x + K)\varphi(y + K)$$

because f is a ring homomorphism.

The map φ is surjective: if $y \in f(R)$, then $y = f(x)$ for some $x \in R$. Then

$$\varphi(x + K) = f(x) = y.$$

Finally, we show that φ is injective:

$$\varphi(x + K) = \varphi(y + K) \implies f(x) = f(y)$$
$$\implies x - y \in K = \ker f$$
$$\implies x + K = y + K.$$

4.11. Suppose there exists an isomorphism $f \colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$. Since f is additive and $f(1) = 1$, $f(m) = m$ for all $m \in \mathbb{Z}$. Furthermore, $f(m/n) = m/n$ for all $m/n \in \mathbb{Q}$. This implies that $f(a + b\sqrt{2}) = a + bf(\sqrt{2})$. Let $z = f(\sqrt{2})$. Then

$$z^2 = f(\sqrt{2})^2 = f(2) = 2$$

and hence $z \in \{-\sqrt{2}, \sqrt{2}\}$. But there are no numbers $\mathbb{Q}[\sqrt{3}]$ whose square is 2: if

$$\left(a + b\sqrt{3}\right)^2 = 2$$

for some $a, b \in \mathbb{Q}$, then

$$2 = \left(a + b\sqrt{3}\right)^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Since $\sqrt{3} \notin \mathbb{Q}$, either $a = 0$ or $b = 0$. Both cases yield a contradiction.

4.15. Let $\varphi \colon \mathbb{Z} \to \mathbb{Z}[i] \xrightarrow{\pi} \mathbb{Z}[i]/(1 + 3i)$, where π denotes the canonical map. We claim that φ is a surjective ring homomorphism with kernel $\ker \varphi = 10\mathbb{Z}$. Then

$$\mathbb{Z}/10\mathbb{Z} \simeq \varphi(\mathbb{Z}) = \mathbb{Z}[i]/(1 + 3i)$$

by the first isomorphism theorem.

Note first that φ is a ring homomorphism, as it is the composition of ring homomorphisms. We now show that $\ker \varphi = 10\mathbb{Z}$:

$$
\begin{aligned}
m \in \ker \varphi &\Longleftrightarrow \varphi(m) + m \in (1 + 3i) \\
&\Longleftrightarrow m = (1 + 3i)(x + iy) \text{ for some } x, y \in \mathbb{Z} \\
&\Longleftrightarrow m = 10x \text{ for some } x \in \mathbb{Z} \\
&\Longleftrightarrow m \in 10\mathbb{Z}.
\end{aligned}
$$

Finally, to see that φ is surjective it is enough to see that $i \in \varphi(\mathbb{Z})$, as then, for $a, b \in \mathbb{Z}$, one has $\varphi(a + 3b) \equiv a + ib \bmod (1 + 3i)$. To show that $i \in \varphi(\mathbb{Z})$ note that

$$\varphi(3) = 3 \equiv i \bmod (1 + 3i),$$

as $3 - i = -i(1 + 3i)$.

4.16. Suppose there is an isomorphism $\varphi \colon Z[i]/I \to \mathbb{Z}/15$ for some ideal I. In particular,

$$\varphi(-1 + I) + \varphi(1 + I) = \varphi(I) = 0$$

and hence, since $\varphi(1 + I) = 1$, it follows that $\varphi(-1 + I) = -1$. Since $i^2 \equiv -1 \bmod I$, one also has $\varphi(i^2 + I) = -1$. But there are no elements $x \in \mathbb{Z}/15$ such that $x^2 = -1$, a contradiction.

7.2. Let $K = \{uv : u \in I, v \in J\}$. Then $X^2 \in K$ and $Y^2 \in K$ but $X^2 + Y^2 \notin K$, so K is not an ideal.

7.4. Assume first that $I \cap J = IJ$ holds for all ideals I and J. Let $a \in R$. Since $Ra = RaR$ and Ra is an ideal,

$$Ra = (Ra)(Ra) = (RaR)a = (Ra)a = Ra^2.$$

In particular, $a \in Ra^2$ and hence $a = xa^2$ for some $x \in R$.

Conversely, assume that R is strongly regular. Since I and J are ideals, $I \cap J \supseteq IJ$. Let $a \in I \cap J$. There exists $x \in R$ such that $a = xa^2$. In particular, $a = (xa)a \in IJ$.

8.11. We want to imitate the proof of Hilbert's Theorem, but the degree used for polynomials cannot be used for power series. So we define the **order** of a power series $f = \sum_{i \geq 0} a_i X^i$ the smallest $d \in \mathbb{Z}_{\geq 0}$ such that $a_d \neq 0$. We also define the order of 0 as 0.

We must show that every ideal of $R[\![X]\!]$ is finitely generated. Assume that there is an ideal I of $R[\![X]\!]$ that is not finitely generated. In particular, $I \neq \{0\}$. Let $f_1(X) \in I \setminus \{0\}$ be of minimal order n_1. Since I is not finitely generated, it follows that $I \neq (f_1(X))$. Let $f_2(X) \in I \setminus (f_1(X))$ be of minimal order n_2. In particular, the minimality of the order of $f_1(X)$ implies that $n_2 \geq n_1$. We continue with this procedure. For $i > 1$ let $f_i(X) \in I$ be a

series of minimal order n_i such that such that $f_i(X) \notin (f_1(X), \ldots, f_{i-1}(X))$ (note that such an $f_i(X)$ exists because I is not finitely generated). Moreover, $n_i \geq n_{i-1}$. This happens because if $n_i < n_{i-1}$, then $f_i(X) \notin (f_1(X), \ldots, f_{i-1}(X))$, which contradicts the minimality of $n_{i-1} = \deg f_{i-1}(X)$. For each $i \geq 1$ let a_i be the coefficient of $f_i(X)$ related to its order, that is

$$f_i(X) = a_i X^{n_i} + \cdots,$$

where the dots denote a series of order $> n_i$. Note that $a_i \neq 0$ for all $i \geq 1$.

Let $J = (a_1, a_2, \ldots)$. Since R is noetherian, the sequence

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots (a_1, a_2, \ldots, a_k) \subseteq \cdots$$

stabilizes, so we may assume that $J = (a_1, \ldots, a_m)$ for some $m \in \mathbb{Z}_{>0}$. In particular, there exist $u_1, \ldots, u_m \in R$ such that

$$a_{m+1} = \sum_{i=1}^{m} u_i a_i.$$

Let

$$g(X) = \sum_{i=1}^{m} u_i f_i(X) X^{n_{m+1} - n_i} \in (f_1(X), \ldots, f_m(X)) \subseteq I.$$

The order of $g(X)$ is n_{m+1} and the coefficient of $g(X)$ of degree n_{m+1} is $\sum_{i=1}^{m} u_i a_i = a_{m+1}$. Thus the order of $g(X) - f_{m+1}(X)$ is $< n_{m+1}$.

Since $f_{m+1}(X) \notin (f_1(X) \ldots, f_m(X))$ and $g(X) \in (f_1(X) \ldots, f_m(X))$,

$$g(X) - f_{m+1}(X) \notin (f_1(X), \ldots, f_m(X)),$$

a contradiction to the minimality of the order of f_{m+1}.

9.22. Let $I_1 \subsetneq I_2 \subsetneq$ be a sequence of ideals of R. Since R is principal, each I_j is principal, say $I_j = (a_j)$ for some $a_j \in R$, so the sequence is of the form

$$(a_1) \subsetneq (a_2) \subsetneq \cdots .$$

Since $I = \cup_{i \geq 1} (a_i)$ is an ideal of R, there exists $x \in R$ such that $I = (x)$. Since $x \in (a_n)$ for some $n \in \mathbb{Z}_{>0}$, it follows that $(a_k) \subseteq I = (x) \subseteq (a_n)$ for all $k \in \mathbb{Z}_{>0}$.

9.38. Let d be the greatest common divisor of the coefficients of f. Since a divides all the coefficients of f, it follows that a divides d. If p is a prime that divides d, then either p divides a or p divides all the coefficients of the primitive polynomial f_1. It follows that d divides a.

9.39.

1) Let $f = \sum_{i=0}^{n} a_i X^i$, $g = \sum_{i=0}^{m} b_i X^i$. Suppose that fg is not primitive and let p be a prime number dividing all the coefficients of fg. Since both f and g are primitive, there exist $i \in \{0, \ldots, n\}$ and $j \in \{0, \ldots, m\}$ minimal such that $p \nmid a_i$ and $p \nmid b_j$. If c_{i+j} is the coefficient of X^{i+j} in fg, then

$$c_{i+j} = \sum_{k>i} a_k b_{i+j-k} + \sum_{k<i} a_k b_{i+j-k} + a_i b_j.$$

Thus p divides $\sum_{k>i} a_k b_{i+j-k} + \sum_{k<i} a_k b_{i+j-k}$ and does not divide the integer $a_i b_j$, that is p does not divide c_{i+j}, a contradiction.

2) Suppose that f is irreducible in $\mathbb{Z}[X]$. If f is not primitive, then $f = af_1$ for some $a \in \mathbb{Z} \setminus \{-1, 1\}$ and some primitive polynomial f_1, a contradiction to the irreducibility of f. Let us prove that f is irreducible in $\mathbb{Q}[X]$. If not, say $f = gh$ for some $g, h \in \mathbb{Q}[X]$ of positive degree. After multiplying by a suitable rational number, we may assume that

$$f = \frac{a}{b} g_1 h_1,$$

where $\gcd(a, b) = 1$ and $g_1, h_1 \in \mathbb{Z}[X]$ are primitive polynomials, that is

$$bf = ag_1 h_1.$$

The greatest common divisor of the coefficients of bf is b. Since $g_1 h_1$ is primitive by the previous item, the greatest common divisor of the coefficients of $ag_1 h_1$ is a. Thus $a = b$ or $a = -b$, that is $f = g_1 h_1$ or $f = -g_1 h_1$ in $\mathbb{Z}[X]$.

9.40. Since $\mathbb{Z}$ is noetherian, it follows that $\mathbb{Z}[X]$ is noetherian by Hilbert's theorem. Then $\mathbb{Z}[X]$ admits factorizations. We need to show that the factorization into irreducibles is unique. Let $f \in \mathbb{Z}[X]$ be non-zero and assume that

$$f = f_1 \cdots f_k = g_1 \cdots g_l$$

be factorizations of f into non-constant irreducibles integer polynomials. Since $f_1, \ldots, f_k$ and $g_1, \ldots, g_k$ are irreducible in $\mathbb{Q}[X]$ and $\mathbb{Q}[X]$ is a unique factorization domain, it follows that $k = l$ and there exits $\sigma \in \mathbb{S}_k$ such that g_i and $h_{\sigma(i)}$ are associate for all $i \in \{1, \ldots, k\}$. After reordering we may assume that for each $i \in \{1, \ldots, k\}$ there exists $a_i/b_i \in \mathbb{Q}$ such that $b_i g_i = a_i h_i$. Since both g_i and h_i are irreducible integer polynomials, it follows from Exercise 9.39 that both g_i and h_i are primitive. By Exercise 9.38, a_i (resp. b_i) is the greatest common divisor of the coefficients of $a_i h_i$ (resp. $b_i g_i$). This implies that a_i and b_i are associate, so a_i/b_i is a unit. Hence g_i and h_i are associate in $\mathbb{Z}[X]$.

10.4. Since $p \equiv 1 \bmod 4$, p is not prime in $\mathbb{Z}[i]$ (see Theorem 10.1). Thus $p = \alpha\beta$ for some $\alpha, \beta \notin \mathcal{U}(\mathbb{Z}[i])$. Hence $p^2 = \text{norm}(p) = \text{norm}(\alpha) \text{norm}(\beta)$. Since $\text{norm}(\alpha) \neq 1$ and $\text{norm}(\beta) \neq 1$,

$$\text{norm}(\alpha) = \text{norm}(\beta) = p.$$

Therefore $\alpha\overline{\alpha} = \text{norm}(\alpha) = p$.

10.5. We claim that the set of irreducible elements of $\mathbb{Z}[i]$ is the union of the following three subsets:

$$\{1 + i, 1 - i, -1 + i, -1 - i\},$$
$$\{a + bi : a, b \in \mathbb{Z}, a^2 + b^2 = p \text{ is a prime such that } p \equiv 1 \bmod 4\},$$
$$\{p, -p, ip, -ip : p \text{ prime } p \equiv 3 \bmod 4\}$$

Let $\alpha \in \mathbb{Z}[i]$ be irreducible. Then α is prime in $\mathbb{Z}[i]$. We claim that $p \in (\alpha)$ for some prime number $p \in \mathbb{Z}$. In fact, $(\alpha) \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$, so $(\alpha) \cap \mathbb{Z} = (p)$ for some positive integer $p \in \mathbb{Z}$. To see that p is a prime number, let us assume that $p \mid xy$ for some $x, y \in \mathbb{Z}$. Then $xy = pm \in (\alpha) \cap \mathbb{Z}$ for some $m \in \mathbb{Z}$. In particular, $xy = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$. Thus $\alpha \mid xy$ in $\mathbb{Z}[i]$ and therefore $\alpha \mid x$ or $\alpha \mid y$ in $\mathbb{Z}[i]$. Thus $x \in (\alpha) \cap \mathbb{Z} = (p)$ or $y \in (\alpha) \cap \mathbb{Z} = (p)$. Hence $p \mid x$ or $p \mid y$ in $\mathbb{Z}$, so p is a prime number.

Let $\beta \in \mathbb{Z}[i]$ be such that $p = \alpha\beta$. Then

$$p^2 = \operatorname{norm}(p) = \operatorname{norm}(\alpha\beta) = \operatorname{norm}(\alpha)\operatorname{norm}(\beta).$$

Thus $\operatorname{norm}(\alpha) \in \{p, p^2\}$, as $\operatorname{norm}(\alpha) \neq 1$ because $\alpha \notin \mathcal{U}(\mathbb{Z}[i])$.

Assume first that $\operatorname{norm}(\alpha) = p$. By Lemma 9.13, every such α is irreducible. It remains to check which prime numbers p can be written as $\operatorname{norm}(\alpha)$. Write $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. So $p = \operatorname{norm}(\alpha) = a^2 + b^2$ and by Theorem 10.1, we have that $p = 2$ or $p \equiv 1 \bmod 4$. Moreover if $p = 2$, then $a^2 = b^2 = 1$, so $\alpha \in \{1 + i, 1 - i, -1 + i, -1 - i\}$.

Assume now that $\operatorname{norm}(\alpha) = p^2$. Then $\beta \in \mathcal{U}(\mathbb{Z}[i])$. So $p = \alpha\beta \in \{\alpha, -\alpha, i\alpha, -i\alpha\}$. Therefore $\alpha \in \{p, -p, ip, -ip\}$ and is irreducible. Hence, by Theorem 10.1, $p \equiv 3 \bmod 4$.

11.14. Assume that I is a maximal ideal of R. We need to show that every non-zero element of R/I is invertible. Recall that $1_{R/I} = 1 + I$. Let $a \notin I$. Then $(I, a) = R$, as I is maximal. Then $1 + x + ab$ for some $x \in I$ and $b \in R$. In particular,

$$(ab) + I = (a + I)(b + I) = 1 + I.$$

Conversely, let J be an ideal of R such that $I \subsetneq J$. Let $a \in J \setminus I$. Since R/I is a field, there exists $b \in R$ such that

$$(ab) + I = (a + I)(b + I) = 1 + I.$$

Thus $ab = 1 + x$ for some $x \in I \subseteq J$. Since $ab \in J$, it follows that $1 \in J$ and therefore $J = R$.

11.19. Recall that R/I is a ring with $0_{R/I} = I$. Thus $x + I = 0_{R/I}$ if and only if $x \in I$. Assume first that I is a prime ideal. Let $a, b \in R$ be such that

$$(ab) + I = (a + I)(b + I) = I.$$

Since $ab \in I$ and I is prime, $a \in I$ or $b \in I$. This means that $a + I = I$ or $b + I = I$.

Conversely, if there are $a, b \in R$ are such that $a \notin I$ and $b \notin I$ and

$$(ab) + I = (a + I)(b + I) = I,$$

then $ab \in I$ and I is not prime.

11.20.

1) Let $a, b \in R$ be such that $ab \in I$. If $a \notin I$, then $(I, a) = R$, as I is a maximal ideal. Thus $1 = x + ra$ for some $x \in I$ and $r \in R$. Multiplying by b and using that $x \in I$ and $ab \in I$, $b = xb + rab \in I$.

2) The ideal (X) is prime as $R/(X) \simeq \mathbb{Z}$ is a domain. Since $\mathbb{Z}$ is not a field, the ideal (X) cannot be maximal (see Exercise 11.14).

3) Let J be an ideal such that $I \subseteq J$. There exist $a, b \in R \setminus \{0\}$ such that $I = (a)$ and $J = (b)$. In particular, since $a \in I \subseteq J$, there exists $r \in R$ such that $a = rb \in I$. Since I is prime, $r \in I$ or $b \in I$. If $b \in I$, then $I = J$. If $r \in I = (a)$, then $r = sa$ for some $s \in R$. Thus $a = rb = s(ab)$, so $a(1 - sb) = 0$. Since $a \neq 0$, $b \in \mathcal{U}(R)$ and therefore $J = R$.

.

11.29. Consider $\mathbb{R}$ as a $\mathbb{Q}$-vector space. Since $\sqrt{2} \notin \mathbb{Q}$, the subset $\{1, \sqrt{2}\}$ of $\mathbb{R}$ is linearly independent over $\mathbb{Q}$. Extend $\{1, \sqrt{2}\}$ to a basis B of $\mathbb{R}$ as a $\mathbb{Q}$-vector space. The linear map $f \colon \mathbb{R} \to \mathbb{R}$ such that $f(1) = \sqrt{2}$, $f(\sqrt{2}) = 1$ and $f(b) = b$ for all $b \in B \setminus \{1, \sqrt{2}\}$ is not

of the form $f(x) = \lambda x$. Indeed, if $f(x) = \lambda x$ for some $\lambda \in \mathbb{R}$, then $\sqrt{2} = f(1) = \lambda$ and $1 = f(\sqrt{2}) = \lambda\sqrt{2}$, a contradiction.

11.30. Let $\{x_i : i \in I\}$ be a basis of $\mathbb{R}$ as a $\mathbb{Q}$-vector space and let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{R}^n$ as a vector space over $\mathbb{R}$. Routine calculations prove that

$$\{x_i e_j : i \in I, 1 \le j \le n\}$$

is a basis of $\mathbb{R}^n$ as a $\mathbb{Q}$-vector space. Since I and $I \times \{e_1, \ldots, e_n\}$ have the same cardinality, there exists a bijective map $f\colon I \to I \times \{e_1, \ldots, e_n\}$. This bijective map extends to a linear isomorphisms between the rational vector spaces $\mathbb{R}^n$ and $\mathbb{R}$. In particular, $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic as abelian groups.

11.31. Let G be a group such that $\operatorname{Aut}(G) = \{\operatorname{id}\}$. Then G is abelian, as the map $G \to G$, $x \mapsto gxg^{-1}$, is an automorphism of G. Since G is abelian, the map $G \to G$, $x \mapsto x^{-1}$, is an automorphism of G. Since the automorphism group of G is trivial, $x = x^2$ for all $x \in G$. At this point it is convenient to write G additively. We claim that G is a vector space over the field $\mathbb{Z}/2$ of two elements, the action is $\mathbb{Z}/2 \times G \to G$, $(\lambda, g) \mapsto \lambda g$. Note that we need $g + g = 0$ to prove that G is indeed a vector space over $\mathbb{Z}/2$, as for example

$$0 = 0g = (1+1)g = 1g + 1g = g + g$$

for all $g \in G$. Let B be a basis of G over $\mathbb{Z}/2$. If $|I| \ge 2$, the automorphism of G that exchanges to basis elements of B and and fixes all other elements of B would be non-trivial. Hence $|I| = 1$ and G is either trivial of cyclic of order two. Both groups have trivial automorphism group.

12.5. One approach to solve this exercise requires the following fact: p is a prime number and $1 \le k \le p^n - 1$, then $\binom{p^n}{k}$ is divisible by p. Let us prove this claim. Write

$$\binom{p^n}{k} = \frac{(p^n)!}{k!(p^n - k)!} = \frac{p^n}{k}\binom{p^n - 1}{k - 1}.$$

Then

$$k\binom{p^n}{k} = p^n\binom{p^n - 1}{k - 1},$$

that is p^n divides $k\binom{p^n}{k}$.

If $\gcd(p, k) = 1$, then it follows that p divides $\binom{p^n}{k}$ by unique decomposition of every integer as a product of primes. We may assume then that $\gcd(p, k) \ne 1$, say $k = p^\alpha m$ for some integer m not divisible by p. Then

$$p^n\binom{p^n - 1}{k - 1} = k\binom{p^n}{k} = p^\alpha m\binom{p^n}{k}$$

and hence

$$p^{n-\alpha}\binom{p^n - 1}{k - 1} = m\binom{p^n}{k}.$$

Since $k < p^n$, it follows that $n - \alpha \ge 1$. Thus p divides $m\binom{p^n}{k}$ and hence p divides $\binom{p^n}{k}$ because p and m are coprime.

13.6. Let $G = \langle g : g^3 = 1 \rangle$ be the cyclic group of order three and ω be a primitive cubic root of one. The map $G \to \mathbb{R} \times \mathbb{C}$, $g \mapsto (1, \omega)$, extends to an algebra homomorphism $\varphi\colon \mathbb{R}[G] \to \mathbb{R} \times \mathbb{C}$. Since $\dim_{\mathbb{R}} \mathbb{R} \times \mathbb{C} = \dim \mathbb{R}[G] = 3$, it follows that φ is a bijective.

14.20. Let $T\colon V \to W$ be a bijective linear map such that $T\rho_g = \psi_g T$ for all $g \in G$.

1) Assume that ψ is not irreducible. Let Y be an invariant subspace of W. Then $X = T^{-1}(Y)$ is an invariant subspace of V, as

$$\rho_g(X) = \rho_g T^{-1}(Y) = T^{-1}\psi_g(Y) \subseteq T^{-1}(Y) = X$$

for all $g \in G$.

2) By assumption V can be decomposed as $V = X \oplus Y$ for some invariant subspaces X and Y. Let $X_1 = T(X)$ and $Y_1 = T(Y)$. Note that X_1 and Y_1 are invariant. In fact, if $g \in G$, then $\psi_g(X_1) = \psi_g T(X) = T\rho_x(X) \subseteq T(X) = X_1$. Similarly, $\psi_g(Y_1) \subseteq Y_1$ for all $g \in G$. Now we prove that $W = X_1 \oplus Y_1$. If $w \in W = T(V)$, then $w = T(v)$ for some $v \in V$ since T is surjective. Write $v = x + y$ for $x \in X$ and $y \in Y$. Then $w = T(v) = T(x) + T(y) \in X_1 + Y_1$. Now if $w \in X_1 \cap Y_1$, then $w = T(x) = T(y)$ for some $x \in X$ and $y \in Y$. Since T is injective, it follows that $x = y \in X \cap Y = \{0\}$. Hence $w = 0$.

17.4. Let $\rho\colon \mathbb{Z} \to \mathbf{GL}_2(\mathbb{C})$ be the homomorphism given by $m \mapsto \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. Then ρ is not irreducible, as since $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ an eigenvector of ρ_m for all $m \in \mathbb{Z}$, the subspace $\mathbb{C}v_1$ is an invariant subspace of $\mathbb{C}^2$. To prove that ρ is indecomposable, let us assume that it is not, that is ρ is equivalent to a direct sum of degree-one (and hence diagonal) representations. However, $\rho_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not diagonalizable, a contradiction.

19.13. Note that if M is a module over $\mathbb{Z}/2$, then $2m = 0$ for all $m \in M$. If $\mathbb{Z}/4$ is a moduel over $\mathbb{Z}/2$, then $0 = 2 \cdot 1 = 1 + 1 = 2$, a contradiction.

19.28.

1) We prove that $\{0\}$, M, $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ are the only submodules of M. If N is a non-zero submodule of M, then let $(x_0, y_0) \in N \setminus \{(0, 0)\}$. If $(x, y) \in M$ is such that $xy \neq 0$, then

$$\left(\frac{x}{x_0} + \left(\frac{y}{y_0} - \frac{x}{x_0} \right) X \right) \cdot (x_0, y_0) = (x, y)$$

and thus $N = M$. If $y_0 = 0$, then $N = \mathbb{R} \times \{0\}$, as $\frac{x}{x_0} \cdot (x_0, 0) = (x, 0)$. If $x_0 = 0$, then $N = \{0\} \times \mathbb{R}$, as $\frac{y}{y_0} \cdot (0, y_0) = (0, y)$

2) If $N \subseteq M$ is a submodule, then N is real vector space. Assume that $N \neq \{(0, 0)\}$ and that $N \neq \mathbb{R}^2$. Since $\dim N = 1$, let $\{(a_0, b_0)\}$ be a basis of N. Since N is a submodule of M, $(b_0, a_0) = X \cdot (a_0, b_0) \in N$. In particular, there exists $\lambda \in \mathbb{R}$ such that $(b_0, a_0) = \lambda(a_0, b_0)$. Since $(a_0, b_0) \neq (0, 0)$, without loss of generality we may assume that $a_0 \neq 0$. Thus $\lambda^2 a_0 = \lambda(\lambda a_0) = \lambda b_0 = a_0$ and hence $\lambda^2 = 1$. If $\lambda = 1$, then $a_0 = b_0$. If $\lambda = -1$, then $a_0 = -b_0$. In conclusion, N is generated either by $(1, 1)$ or $(1, -1)$.

20.12. Take for example the $\mathbb{Z}$-module $\bigcup_{k \geq 1} \mathbb{Z}/(p^k)$.

26.7. The Smith's normal form yields

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -2 & -2 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad S = PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The solution of the integer linear system is then $X = \begin{pmatrix} 1 \\ 0 \\ 5 \end{pmatrix}$.

26.8. We do not provide the full solutions. It should be enough to show that the Smith's normal form of the matrix $\begin{pmatrix} 6 & 6 & 4 \\ 6 & 12 & 8 \\ 0 & 0 & 0 \end{pmatrix}$ is $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

26.9. Let $A = \begin{pmatrix} 3 & 2 & 1 \\ 8 & 4 & 2 \\ 7 & 6 & 2 \\ 9 & 6 & 1 \end{pmatrix}$. The Smith's normal form of A is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}$. Thus the abelian group is isomorphic to $\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/4$.

26.10. The Smith's normal form is $\begin{pmatrix} 1 & 0 \\ 0 & -11 + 8i \end{pmatrix}$.

26.11. The Smith normal form is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & f(X) \end{pmatrix},$$

where $f(X) = X^4 - 3X^3 - 18X^2 + 56X$.

26.12. Since $\det A \neq 0$, the set $\{y_1, \ldots, y_n\}$ is linearly independent over $\mathbb{Q}$ and hence they are linearly independent over $\mathbb{Z}$. Let $B = (b_{ij}) \in M_n(\mathbb{Q})$ be the inverse of A. Then

$$B = A^{-1} = (\det A)^{-1} \operatorname{adj}(A) = \pm \operatorname{adj}(A) \in M_n(\mathbb{Z}).$$

Then $x_i = \sum_{j=1}^{n} b_{ij}y_j$ for all $i \in \{1, \ldots, n\}$ and hence $\{y_1, \ldots, y_n\}$ generates G and therefore $\{y_1, \ldots, y_n\}$ is a basis of G.

Assume now that $\{y_1, \ldots, y_n\}$ is a basis of G. There exist matrices $A = (a_{ij}) \in M_n(\mathbb{Z})$ and $B = (b_{ij}) \in M_n(\mathbb{Z})$ such that

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \quad x_i = \sum_{j=1}^{n} b_{ij}y_j$$

for all $i \in \{1, \ldots, n\}$. In particular, $AB = I$. Applying determinant, $(\det A)(\det B) = 1$ and hence $\det A = \det B \in \{-1, 1\}$.

References

[1] M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[2] O. A. Cámpoli. A principal ideal domain that is not a Euclidean domain. *Amer. Math. Monthly*, 95(9):868–871, 1988.

[3] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[5] S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.

[6] J. R. Munkres. *Elements of algebraic topology*. Addison-Wesley Publishing Company, Menlo Park, CA, 1984.

[7] J.-P. Serre. *Linear representations of finite groups*. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.

[8] B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.

[9] S. Wagon. Editor's corner: the Euclidean algorithm strikes again. *Amer. Math. Monthly*, 97(2):125–129, 1990.

[10] J. C. Wilson. A principal ideal ring that is not a Euclidean ring. *Math. Mag.*, 46:34–38, 1973.

[11] R. A. Wilson. 101.15 An elementary proof that not all principal ideal domains are Euclidean domains. *Math. Gaz.*, 101(551):289–293, 2017.

Index