Leandro Vendramin

# Rings and modules

## Notes

Friday 3rd November, 2023

# Preface

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

The material is somewhat standard. Basic texts on abstract algebra are for example [1], [3] and [6]. Lang's book [7] is also a standard reference, but maybe a little bit more advanced. We based the lectures on the representation theory of finite groups on [9] and [10].

We also mention a set of great expository papers by Keith Conrad available at `https://kconrad.math.uconn.edu/blurbs/`. The notes are extremely well-written and are useful at every stage of a mathematical career.

Thanks go to Wouter Appelmans, Arne van Antwerpen, Ilaria Colazzo, Luk De Block, Luca Descheemaeker, Łukas Kubat, Lucas Simons and Geoffrey Jassens.

This version was compiled on Friday 3rd November, 2023 at 15:33. Please send comments and corrections to me at `Leandro.Vendramin@vub.be`.

Leandro Vendramin
Brussels, Belgium

# Contents

# List of topics

# Lecture 1

The objective of the first 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. Rings

**Definition 1.1.** A **ring** is a 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 $x1_R=1_Rx=x$ 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.

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

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

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

**Example 1.4.** 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 real polynomials in $n$ commuting variables $X_1, \ldots, X_n$ with coefficients in $R$ as $R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n]$.

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

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

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

**Exercise 1.6.** 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 $|R| = 1$.

**Example 1.7.** 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**.

**Example 1.8.** 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 $n$.

**Example 1.9.** 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

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

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

**Example 1.10.** 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 $S$.

**Definition 1.11.** 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.

**Example 1.12.** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ 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.

**Example 1.13.** 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?

**Example 1.14.** $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ 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 $b = d$?

**Example 1.15.** 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 $R$.

**Exercise 1.16.**

**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 $R$.

**Definition 1.17.** 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 $\mathcal{U}(\mathbb{Z}/8) = \{1, 3, 5, 7\}$.

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

**Definition 1.19.** A **division ring** is a ring $R$ 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 $a1 + bi + cj + dk \in H(\mathbb{R})$.

**Definition 1.20.** 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.

**Exercise 1.21.** 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 and quotients

**Definition 2.1.** Let $R$ be a ring. A **left ideal** of $R$ is a subset $I$ such that $(I, +)$ is a subgroup of $(R, +)$ and such that $RI \subseteq I$, 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 $IR \subseteq I$.

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

$$I = \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} : x, y \in \mathbb{R} \right\}$$

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

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

**Definition 2.3.** 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 $R$.

**Exercise 2.4.** 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 $R$.

**Example 2.5.** 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 $(X) = (x_1, \ldots, x_n)$.

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

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

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

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

**Exercise 2.9.** 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 $R$.

**Definition 2.10.** 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 $r(X) = X$.

**Exercise 2.11.** 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.

**Exercise 2.12.** 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.

**Definition 2.13.** 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 $f(1) = 1$.

**Example 2.14.** The map $f\colon \mathbb{Z}/6 \to \mathbb{Z}/6$, $x \mapsto 3x$, 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.

**Example 2.15.** 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.

**Example 2.16.** Let $R$ be a ring. The map $\mathbb{Z} \to R$, $k \mapsto k1$, is a ring homomorphism.

**Example 2.17.** 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 $S$.

**Example 2.18.** 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 $\mathbb{Z}[X]$.

**Example 2.19.** 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.

**Example 2.20.** The map $\mathbb{Z}[i] \to \mathbb{Z}/5$, $a+bi \mapsto a+2b \bmod 5$, is a ring homomorphism with $\ker f = \{a+bi : a+2b \equiv 0 \bmod 5\}$.

**Exercise 2.21.** There is no ring homomorphism $\mathbb{Z}/6 \to \mathbb{Z}/15$. Why?

**Exercise 2.22.** 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 $x_0$.

# Lecture 2

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

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

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

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

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 $xy+I=x_1y_1+I$. Since $x-x_1 \in I$,

$$xy-x_1y=(x-x_1)y \in I$$

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

$$x_1y-x_1y_1=x_1(y-y_1) \in I,$$

as $I$ is a left ideal. Thus

$$xy-x_1y_1=xy-x_1y+x_1y-x_1y_1=(x-x_1)y+x_1(y-y_1) \in I.$$

**Theorem 2.23.** *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

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

**Exercise 2.24.** Prove Theorem 2.23.

**Example 2.25.** 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 $R\simeq S$. As it happens in the case of groups, to understand quotient rings, one has the first isomorphism theorem.

**Theorem 2.26 (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.

**Exercise 2.27.** Prove Theorem 2.26.

**Example 2.28.** 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 $R/\ker f \simeq \mathbb{Q}$.

**Example 2.29.** The evaluation map $\mathbb{R}[X] \to \mathbb{C}$, $f(X) \mapsto f(i)$, is a surjective ring homomorphism with kernel $(X^2+1)$. Thus

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

by the first isomorphism theorem. In practice, this is how it 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.

**Exercise 2.30.** Prove that $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[X]/(X^2+5)$.

Similarly, if $N$ is a square-free integer, then $\mathbb{Z}[\sqrt{N}] \simeq \mathbb{Z}[X]/(X^2-N)$.

**Exercise 2.31.** 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)** $\mathbb{R}[X,Y]/(X) \simeq \mathbb{R}[Y]$.

**Exercise 2.32.** Are the rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ isomorphic?

**Exercise 2.33.** Let $R$ be the ring of continuous maps $[0,2] \to \mathbb{R}$, where the operations are given by

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

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

**Exercise 2.34.** 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 $M_n(R)/M_n(I) \simeq M_n(R/I)$.

**Exercise 2.35.** Let $R = \mathbb{Z}[\sqrt{10}]$ and $I = (2, \sqrt{10})$. Prove that $R/I \simeq \mathbb{Z}/2$.

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

**Exercise 2.36.** 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 $\pi$ is the canonical map.

**Exercise 2.37.** Prove that there is no ideal $I$ of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

**Exercise 2.38.** 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.

As it happens in group theory, one has the following significant result.

**Theorem 2.39 (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 $R/I \simeq S/J$.

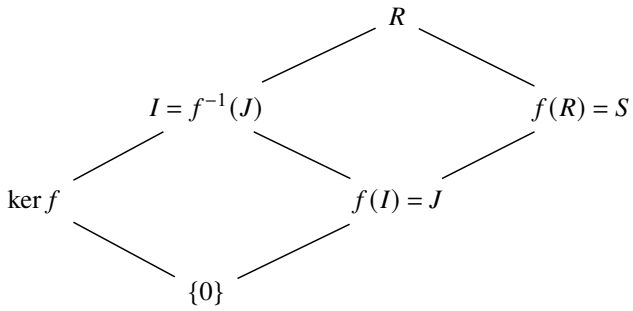
We only prove the fourth statement, the others are left as exercises. Note that the third claim implies that $f(I) = J$ if and only if $I = f^{-1}(J)$. Let $\pi\colon S \to S/J$ be the canonical map. The composition $g = \pi \circ f\colon R \to S/J$ is a ring homomorphism and

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

Since $g(R) = S/J$, the first isomorphism theorem implies that $R/I \simeq S/J$. □

**Exercise 2.40.** Prove Theorem 2.39.

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




## §3. 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.

**Definition 3.1.** 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

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

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 $R$. Why we need to consider finite sums of elements of the form $uv$ for $u \in I$ and $v \in J$?

**Exercise 3.2.** 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 $IJ = (4) \subsetneq (2) = I \cap J$.

**Proposition 3.3.** *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 $v \in J$, $x = x1 = x(u+v) = xu + xv \in IJ$. □

**Exercise 3.4.** 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.

**Theorem 3.5 (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*

$$\begin{cases} x \equiv u \bmod I, \\ x \equiv v \bmod J. \end{cases}$$

*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 $x \equiv u \bmod I$. Similarly, $x - v \in J$ and $x \equiv v \bmod J$. □

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

**Corollary 3.6.** *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 $\pi_I : R \to R/I$ and $\pi_J : R \to R/J$ be the canonical maps. A straightforward 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 use now the Chinese remainder theorem to prove that the map $\varphi$ is surjective. 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 $\varphi$, 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. □

Let $R$ be a commutative ring and $I_1, \dots, I_n$ be ideals of $R$. Then

$$I_1 \cdots I_n = \left\{ \sum_{i=1}^{m} u_{i_1} \cdots u_{i_n} : m \in \mathbb{Z}_{\geq 0}, u_{i_1}, \dots, u_{i_n} \in I_{i_j} \right\}$$

is an ideal of $R$. If $I_1$ and $I_j$ are coprime for all $j \in \{2, \dots, n\}$, then $I_1$ and $I_2 \cdots I_n$ are coprime. If $I_i$ and $I_j$ are coprime whenever $i \neq j$, then

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

With small changes, the Chinese remainder theorem can be proved in arbitrary non-commutative rings, see for example [6, Chapter III, Theorem 2.25].

**Exercise 3.7 (Lagrange's interpolation theorem).** The Chinese remainder theorem proves the following well-known result. Let $x_1, \dots, x_k \in \mathbb{R}$ be such that $x_i \neq x_j$ whenever $i \neq j$ and $y_1, \dots, y_k \in \mathbb{R}$. 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 $(X - x_1)(X - x_2) \cdots (X - x_n)$.

**Exercise 3.8.** 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?

**Exercise 3.9.** Prove that

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

does not have a solution.

**Exercise 3.10.** 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.

**Exercise 3.11.** Prove that for each $n > 0$ there are $n$ consecutive integers such that each integer is divisible by a perfect square $\neq 1$.

# Lecture 3

## §4. Noetherian rings

**Definition 4.1.** 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.

**Exercise 4.2.** Let $R = \{f : [0,1] \to \mathbb{R}\}$ 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.

**Definition 4.3.** 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.

**Proposition 4.4.** *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 $m \geq N$. □

**Exercise 4.5.** 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 $I = (X_1, X_2, \dots)$ 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.

**Proposition 4.6.** *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 $\pi^{-1}(J) = (x_1, \dots, x_k)$ for $x_1, \dots, x_k \in R$. Thus

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

because $\pi$ is surjective and hence $J$ is finitely generated. □

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

**Exercise 4.7.** Prove that $\mathbb{R}[X]$ is noetherian.

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

**Theorem 4.8 (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 such that $f_i(X) \notin (f_1(X), \dots, f_{i-1}(X))$ (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 $f_i(X) \notin (f_1(X), \dots, f_{i-1}(X))$, 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

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

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

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

a contradiction to the minimality of the degree of $f_{m+1}$. □

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

**Example 4.9.** 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.

**Example 4.10.** The ring $\mathbb{Z}[X, X^{-1}]$ is noetherian, as $\mathbb{Z}[X, X^{-1}] \simeq \mathbb{Z}[X, Y]/(XY - 1)$.

**Exercise 4.11.** 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.

**Exercise 4.12.** Let $f\colon R \to R$ be a surjective ring homomorphism. Prove that $f$ is an isomorphism if $R$ is noetherian.

## §5. Factorization

**Definition 5.1.** A **domain** $R$ is a ring 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.

**Example 5.2.** 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.

**Definition 5.3.** 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 $(y) \subseteq (x)$.

**Definition 5.4.** 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 $(x) = (y)$.

**Example 5.5.** The integers 2 and $-2$ are associate in $\mathbb{Z}$.

**Example 5.6.** 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 $R$.

**Example 5.7.** Let $R = \mathbb{R}[X]$ and $f(X) \in R$. Then $f(X)$ and $\lambda f(X)$ are associate in $R$ for all $\lambda \in \mathbb{R}^\times$.

**Definition 5.8.** 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 $(x) \subsetneq (y) \subsetneq R$.

**Example 5.9.** 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 $p \mid y$.

**Example 5.10.** 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

$$\begin{cases} bd = 1, \\ cb + ad = 0, \\ b + d + ac = 0, \\ a + c = 0. \end{cases} \tag{3.1}$$

This is a contradiction. as (3.1) 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 $(\mathbb{Z}/2)[X]$.

**Definition 5.11.** 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 $(p) \neq R$ and $xy \in (p)$ implies that $x \in (p)$ or $y \in (p)$.

**Proposition 5.12.** *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 $x \in \mathcal{U}(R)$. □

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.

**Lemma 5.13.** *Let $N \in \mathbb{Z}$ be a non-zero square-free integer and $R = \mathbb{Z}[\sqrt{N}]$. Then the map*

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

*satisfies the following properties:*

***1)*** *$N(\alpha) = 0$ if and only if $\alpha = 0$.*
***2)*** *$N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in R$.*
***3)*** *$\alpha \in \mathcal{U}(\mathbb{Z}[\sqrt{N}])$ if and only if $N(\alpha) = 1$.*
***4)*** *If $N(\alpha)$ is prime in $\mathbb{Z}$, then $\alpha$ 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 $N(\alpha) = N(\beta)N(\gamma)$. Since $N(\alpha) \in \mathbb{Z}$ is a prime number, it follows that $N(\beta) = 1$ or $N(\gamma) = 1$. Thus $\beta \in \mathcal{U}(R)$ or $\gamma \in \mathcal{U}(R)$. □

**Exercise 5.14.** Prove Lemma 5.13.

**Exercise 5.15.** 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 $n \geq 1$.

**Example 5.16.** 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 $9 = N(\alpha)N(\beta)$. This implies that $N(\alpha) \in \{1, 3, 9\}$. Write $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. If $N(\alpha) = 1$, then $\alpha \in \mathcal{U}(R)$ by the lemma. If $N(\alpha) = 9$, then $N(\beta) = 1$ and hence $\beta \in \mathcal{U}(R)$ by the lemma. Finally, if $N(\alpha) = 3$, 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

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

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

# Lecture 4

**Example 5.17.** 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 $4 = N(x) = N(\alpha)N(\beta)$. Thus $N(\alpha) \in \{1, 2, 4\}$. Write $\alpha = a + b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$. If $N(\alpha) = a^2 + 3b^2 = 2$, then $b = 0$ and hence $a^2 = 2$, a contradiction. If $N(\alpha) = 1$, then $\alpha \in \mathcal{U}(R)$. If $N(\alpha) = 4$, then $N(\beta) = 1$ 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.

**Exercise 5.18.** 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 $R$.

**Exercise 5.19.** Let $R = \mathbb{Z}[\sqrt{5}]$. Prove that $1 + \sqrt{5}$ is irreducible and not prime in $R$.

**Definition 5.20.** 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.

**Example 5.21.** 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 $f(X), g(X) \in \mathbb{Z}[X]$. 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 $f(X) = a_0 + a_1X$ for $a_0, a_1 \in \mathbb{Z}$ and $a_1 \neq 0$. It follows that

$$X = \pm 2f(X) = \pm 2(a_0 + a_1X)$$

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

**Exercise 5.22.** Let $R$ be a principal domain. Prove that $R$ is noetherian.

**Example 5.23.** 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 $\alpha$. Then $\alpha \mid 2$ and $\alpha \mid 1+\sqrt{-5}$. Then $N(\alpha) \mid 4$ and $N(\alpha) \mid 6$, because $N(2) = 4$ and $N(1+\sqrt{-5}) = 6$. Thus $N(\alpha) \in \{1, 2\}$. If we write $\alpha = a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$, then it follows that $a^2 + 5b^2 = N(\alpha)$. Clearly, $N(\alpha) \neq 2$, as $a^2 = 2$ has no solution in $\mathbb{Z}$. Now $N(\alpha) = 1$ implies that $\alpha \in \mathcal{U}(R)$ and hence $I = R$, a contradiction.

Sometimes primes and irreducibles coincide.

**Proposition 5.24.** *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 $x \mid y$. □

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

**Example 5.25.** Since $\mathbb{Z}[\sqrt{-3}]$ have irreducible elements that are not prime, it follows that $\mathbb{Z}[\sqrt{-3}]$ is not a principal domain.

**Definition 5.26.** 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.

**Example 5.27.** $\mathbb{Z}$ is a euclidean domain with $\varphi(x) = |x|$.

Do we have uniqueness in the previous example?

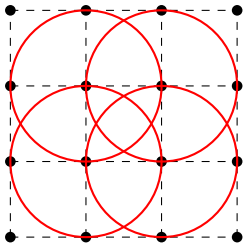
**Example 5.28.** $\mathbb{R}[X]$ is an euclidean domain with $\varphi(f(X)) = \deg(f(X))$.

The previous examples show why in the definition of a euclidean domain we consider $\varphi\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$.

**Example 5.29.** Let $R = \mathbb{Z}[i]$. Then $R$ is an euclidean domain with $\varphi(\alpha) = N(\alpha)$. Let Let $\alpha, \beta \in \mathbb{Z}[i]$ and assume that $\beta \neq 0$. We want to find Gauss integers $\gamma, \delta \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\delta + \gamma$$

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

**Example 5.30.** Let $R = \mathbb{Z}[i]$ and $\alpha = -1+i$ and $\beta = 1+2i$. Let $I = (\beta)$ be the ideal of $R$ generated by $\beta$. 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 $\beta$, see Figure 4.1. 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 $N(-1+i) = 2 < N(\beta) = 5$.

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

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

with $N(-1) = 1 < N(\beta) = 5$.

**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 $N(-2i) = 4 < N(\beta) = 5$.

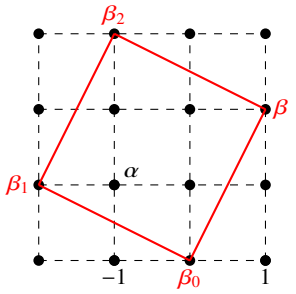



**Figure 4.1** Division algorithm in $\mathbb{Z}[i]$.

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.

**Proposition 5.31.** *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 $I = (y)$. □

**Example 5.32.** Since $\mathbb{Z}[i]$ is euclidean, it is principal.

**Example 5.33.** 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], [14] or [13].

**Definition 5.34.** 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 $c_1, \ldots, c_n$.
**2)** If $x = c_1 \cdots c_n = d_1 \cdots d_m$ for irreducibles $c_1, \ldots, c_n$ and $d_1, \ldots, d_m$, then $n = m$ and there exists $\sigma \in \mathbb{S}_n$ such that $c_i$ and $d_{\sigma(i)}$ are associate for all $i \in \{1, \ldots, n\}$.

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.

**Example 5.35.** 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 $N(a + b\sqrt{-6}) = a^2 + 6b^2 \neq 2$. This implies that 2 is irreducible, as if $2 = \alpha\beta$, then $4 = N(2) = N(\alpha)N(\beta)$. Similarly, 5 is irreducible. It is an exercise to prove that $2 + \sqrt{-6}$ and $2 - \sqrt{-6}$ are both irreducible.

**Theorem 5.36.** *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 5.24. 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 $\sigma$ appears). Since $d_1$ is irreducible, $c_1$ and $d_1$ are associate, that is $c_1 = ud_1$ for some $u \in \mathcal{U}(R)$. Then

$$c_1 c_2 \cdots c_n = (ud_1)c_2 \cdots c_n = d_1 d_2 \cdots d_m.$$

Since $d_1 \neq 0$,

$$d_1(uc_2 \cdots c_n - d_2 \cdots d_m) = 0,$$

which implies that $(uc_2) \cdots c_n = d_2 \cdots d_m$ because $R$ is an integral domain. Note that $uc_2$ is irreducible and hence the claim follows from the inductive hypothesis. □

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

**Example 5.37.** The ring $\mathbb{Z}[i]$ is a unique factorization domain.

Let us show that the converse of Theorem 5.36 does not hold.

**Exercise 5.38.** A polynomial $f \in \mathbb{Z}[X]$ is **primitive** if the greatest common divisors of its coefficients is equal to one. Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial. If $f = af_1$ for some $a \in \mathbb{Z}$ and some primitive polynomial $f_1$, then $a$ is the greatest common divisor of the coefficients of $f$.

**Exercise 5.39.** Prove the following statements:

**1)** Let $f, g \in \mathbb{Z}[X]$ be primitive polynomials. Prove that $fg$ es 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 5.39 is known as Gauss' lemma. The second one is Gauss' theorem. These results should be used to prove the following result:

**Exercise 5.40.** Prove that $\mathbb{Z}[X]$ is a unique factorization domain.

Finally, the example.

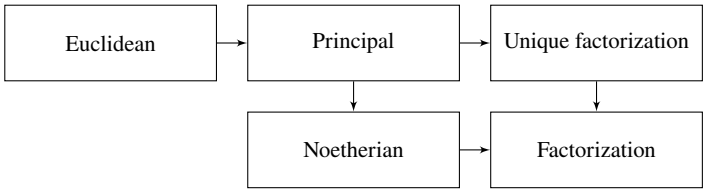
**Example 5.41.** The ring $\mathbb{Z}[X]$ is a unique factorization domain that is not a principal domain.

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, [6, Chapter III, Theorem 6.14].

**Exercise 5.42.** Prove that $\mathbb{R}[X, Y]$ is a unique factorization domain and that the ideal $I = (X, Y)$ is not principal.

# Lecture 5

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




We also know that the reverse implications do not hold.
It is time to give a very nice number-theoretical application.

**Theorem 5.43 (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

$$p^2 = N(p) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$$

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 $a^2+b^2 \equiv 2 \bmod 4$. □

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 $x^2 \equiv -1 \bmod p$.

**Exercise 5.44.** Decompose the prime 41 as a sum of two squares.

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 $p = a^2+b^2$. Simple and beautiful as it is, Gauss's formula does not seem to be of any real computational value.

In [12], the author employs the Euclidean algorithm to determine efficiently the decomposition of a prime number $p = 4k+1$ as the sum of two squares.

**Exercise 5.45.** Let $\alpha \in \mathbb{Z}[i]$ be such that $N(\alpha) = p^2$ for some prime number $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$. Prove that $\alpha$ is irreducible.

**Exercise 5.46.** Let $p \in \mathbb{Z}$ be a prime number such that $p \equiv 1 \bmod 4$. If $\alpha \in \mathbb{Z}[i]$, then $\alpha = \gamma\overline{\gamma}$ for some $\gamma \in \mathbb{Z}[i]$ irreducible.

**Exercise 5.47.** Find the irreducible elements of $\mathbb{Z}[i]$.

As a consequence of Theorem 5.43 one can prove the following result: An integer $\geq 2$ 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:

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

They form the set of all norms of Gaussian integers.

**Exercise 5.48.** This exercise is about **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
$$N\colon R \to \mathbb{Z}_{\geq 0}, \quad N(a + b\omega) = a^2 - ab + b^2,$$
is multiplicative and satisfies $N(\alpha) = \alpha\overline{\alpha}$ for all $\alpha \in R$.
**2)** $\mathcal{U}(R) = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.
**3)** $R$ is an euclidean domain.
**4)** If $N(\alpha)$ is a prime number, then $\alpha$ is irreducible.
**5)** If $N(\alpha) = p^2$ for some prime number $p$ with $p \equiv 2 \bmod 3$, then $\alpha$ 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 $p \equiv 2 \bmod 3$.

## §6. Zorn's lemma

**Definition 6.1.** 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 $r \neq s$.

**Definition 6.2.** Let $R$ be a poset and $r, s \in R$. Then $r$ and $s$ are **comparable** if either $r \leq s$ or $s \leq r$.

**Example 6.3.** 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.

**Definition 6.4.** Let $R$ be a poset and $r \in R$. Then $r$ is **maximal** in $R$ if $r \leq t$ implies $r = t$.

**Example 6.5.** $\mathbb{Z}$ has no maximal elements.

**Example 6.6.** 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.

**Definition 6.7.** 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 $S$.

**Example 6.8.** 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 $X$.

**Example 6.9.** 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 $R$.

**Definition 6.10.** 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 is not intuitive[1] but it is logically equivalent to a more intuitive statement in set theory, the Axiom of Choice, which says every Cartesian product of non-empty sets is non-empty. It is more an axiom than a lemma. The reason for calling Zorn's lemma a lemma rather than an axiom is purely historical.

**Definition 6.11.** 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 $\mathbb{Z}$.

**Exercise 6.12.** Let $R$ be a commutative ring. Prove that $R$ is a field if and only if $\{0\}$ is a maximal ideal of $R$.

**Exercise 6.13.** 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 $I \neq R$.
The following application of Zorn's lemma uses the identity of a ring.

**Theorem 6.14 (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.*

[1] 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?*

*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 $X$ (say for example 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 $M = M_1$. □

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

**Exercise 6.15.** 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 $K$.

**Exercise 6.16.** Let $R$ be a principal domain and $p \in R \setminus \{0\}$. Then $p$ is irreducible if and only if $(p)$ is maximal.

**Definition 6.17.** 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 $\mathbb{Z}$.

**Exercise 6.18.** Let $R$ be a commutative ring. Prove that an ideal $I$ of $R$ is prime if and only if $R/I$ is a domain.

**Exercise 6.19.** 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.

**Example 6.20.** 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.

**Example 6.21.** 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.

**Exercise 6.22.** Compute the maximal ideals of $\mathbb{Z}/n$.

**Exercise 6.23.** 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.

**Exercise 6.24.** Prove that every non-zero vector space has a basis.

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

**Exercise 6.25.** 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 $X$.

**Exercise 6.26.** 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 $V$.

**Exercise 6.27.** Prove that every spanning set of a non-zero vector space contains a basis.

**Exercise 6.28.** Prove that there exists a group homomorphism $f : \mathbb{R} \to \mathbb{R}$ that is not of the form $f(x) = \lambda x$ for some $\lambda \in \mathbb{R}$.

**Exercise 6.29.** Prove that the abelian groups $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic.

**Exercise 6.30.** Prove that if $G$ is a group such that $|G| > 2$, then $|\operatorname{Aut}(G)| > 1$.

## §7. The characteristic of a ring

**Definition 7.1.** 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 $\operatorname{char}\mathbb{Z}/n = n$.

**Proposition 7.2.** *Let $R$ be a ring such that $\operatorname{char} R = n > 0$,*

***1)*** *The map $f : \mathbb{Z} \to R$, $m \mapsto m1$, 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. □

**Exercise 7.3.** 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.

**Exercise 7.4 (binomial theorem).** Let $R$ be a commutative ring and $n \geq 1$. Prove that if $a, b \in R$, then

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

**Exercise 7.5.** 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: Use induction on $n$ and 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 $k \in \{1, 2, \ldots, p^n - 1\}$.

**Exercise 7.6.** 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

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

## §8. Group algebras

We now discuss an important family of examples. Fix a field $K$. For a finite group $G$, let $K[G]$ be the vector space (over $K$) with basis $\{g : g \in G\}$. Then $K[G]$ is a ring with

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

**Example 8.1.** 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 $(13)(12) = (123)$.

Thus $K[G]$ is a ring and also a vector space (over $K$) and these structures are somewhat compatible. Note that

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

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

**Definition 8.2.** Let $A$ be a ring. Then $A$ is 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 $a,b \in A$.

Other examples of algebras are polynomial rings $K[X]$ and $K[X,Y]$ and matrix rings $M_n(K)$.

**Example 8.3.** If $A$ is an algebra, then $M_n(A)$ is an algebra.

The ring $K[G]$ is commutative if and only if $G$ is abelian. Moreover, $K[G]$ is a vector space of dimension $\dim K[G] = |G|$.

**Example 8.4.** 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

$$\alpha\beta = (a_1b_1 + a_2b_3 + a_3b_2)1 + (a_1b_2 + a_2b_1 + a_3b_3)g + a_1b_3 + a_2b_2 + a_3b_1)g^2.$$

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 $\mathbb{C}[X]/(X^n-1)$.

**Exercise 8.5.** Prove that $\mathbb{R}[C_3] \simeq \mathbb{R}\times\mathbb{C}$.

**Exercise 8.6.** 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 $\mathbb{C}[G] \to \mathbb{C}\times\mathbb{C}$, $a1+bg \mapsto (a+b, a-b)$, is a linear isomorphism of rings.

**Exercise 8.7.** Let $K = \mathbb{Z}/2$ and $G = \{1, g\} \simeq C_2$ be the cyclic group of order two. Prove that the map $K[G] \to \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}$, $a1 + bg \mapsto \begin{pmatrix} a+b & b \\ 0 & a+b \end{pmatrix}$, 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 $\varphi|_G = f$.

**Example 8.8.** 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 $\omega$ 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.

# Lecture 6

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.

## §9. Group representations

**Definition 9.1.** 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 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 if $V$ is finite-dimensional, say $\dim V = n$, 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.

**Example 9.2.** We use group representations to show that $G = \langle x, y : x^2 = y^2 = 1\rangle$ 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 shows the power of group representations, even for infinite groups. However, in this course, we will work with complex finite-dimensional representations of finite groups.

**Example 9.3.** 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 $G$.

**Example 9.4.** The sign yields a representation of $\mathbb{S}_n$. It is the group homomorphism $\mathbb{S}_n \to \mathbb{C}^\times$, $\sigma \mapsto \operatorname{sign}(\sigma)$.

**Example 9.5.** 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.

**Definition 9.6.** Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations of a finite group $G$. 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 $\rho\colon G \to \mathbf{GL}(V)$, $g \mapsto \rho_g$, 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 $g \in G$. Although we use the same notation for different representations, there is no risk of confusion.

**Definition 9.7.** The representations $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are **equivalent** if there exists a bijective map $T\colon V \to W$ invariant with respect to $\rho$ and $\psi$.

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

Now we can understand why we can alternatively use representations or matrix representations.

**Example 9.8.** 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

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

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

**Example 9.9.** 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 $T = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$.

**Definition 9.10.** Let $\rho\colon G \to \mathbf{GL}(V)$ a representation. A subspace $W$ of $V$ is said to be **invariant** (with respect to $\rho$) if $\rho_g(W) \subseteq W$ for all $g \in G$.

If $\rho\colon G \to \mathbf{GL}(V)$ is a representation and $W \subseteq V$ is invariant, then the map $\rho|_W : G \to \mathbf{GL}(W), g \mapsto (\rho_g)|_W$, is a representation. The map $\rho|_W$ is the **restriction** of $\rho$ to $W$.

**Example 9.11.** If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations and $T\colon V \to W$ is an invariant map, then the **kernel**

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

is an invariant of $V$ and the **image**

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

is an invariant subspace of $W$.

**Definition 9.12.** Let $\rho\colon G \to \mathbf{GL}(V)$ a representation. A **subrepresentation** of $\rho$ is a restricted representation of the form $\rho|_W : G \to \mathbf{GL}(W)$ for some invariant subspace $W$ of $V$.

**Definition 9.13.** A 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.

**Example 9.14.** 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 $\{s, t\}$ are 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?

**Exercise 9.15.** Let $\rho\colon G \to \mathbf{GL}(V)$ be a degree-two representation. Prove that $\rho$ is irreducible if and only if there is no common eigenvector for the $\rho_g$, $g \in G$.

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.

**Example 9.16.** 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 $\rho$ and $\psi$ 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 $\rho$ and $\psi$ 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 $V \simeq V \oplus \{0\}$ and $W \simeq \{0\} \oplus W$ are invariant subspaces of $V \oplus W$.

**Definition 9.17.** A representation $\rho\colon G \to \mathbf{GL}(V)$ is said to be **completely reducible** if $\rho$ 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 $V = V_1 \oplus \cdots V_n$. Moreover, on some basis of $V$, the matrix $\rho_g$ can be written as

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

**Definition 9.18.** 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.

**Exercise 9.19.** 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 $\rho$ is irreducible, then $\psi$ is irreducible.
**2)** If $\rho$ is decomposable, then $\psi$ is decomposable.
**3)** If $\rho$ is completely reducible, then $\psi$ is completely reducible.

Since we are considering finite-dimensional vector spaces, our vector spaces are Hilbert spaces, so they have an inner product $V \times V \to \mathbb{C}$, $(v,w) \mapsto \langle v,w \rangle$.

**Definition 9.20.** 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 $v, w \in V$.

**Example 9.21.** Let $G$ be a finite group and $V = \mathbb{C}[G]$. 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 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.

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:

**Proposition 9.22.** *Let $\rho\colon G \to \mathbf{GL}(V)$ be a unitary representation. Then $\rho$ is either irreducible or decomposable.*

*Proof.* If $\rho$ is not irreducible, there exists an invariant subspace $W$ of $V$ such that $\{0\} \subsetneq W \subsetneq V$. Then $V = W \oplus W^\perp$ as complex vector spaces, where $W^\perp \neq \{0\}$. So $\rho$ 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. □

**Theorem 9.23 (Weyl's trick).** *Every representation $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ of a finite group is unitary.*

*Proof.* Let $V = \mathbb{C}^n$ and $V \times V \to \mathbb{C}$, $(v, w) \mapsto \langle v, w\rangle_0$, be an inner product on $V$. A straightforward calculation shows that

$$\langle v, w\rangle = \sum_{g\in G} \langle \rho_g v, \rho_g w\rangle_0$$

is an inner product of $V$. Since

$$\begin{aligned}\langle \rho_g v, \rho_g w\rangle &= \sum_{h\in G} \langle \rho_h\rho_g v, \rho_h\rho_g w\rangle_0 \\ &= \sum_{h\in G} \langle \rho_{hg} v, \rho_{hg} w\rangle_0 = \sum_{x\in G} \langle \rho_x v, \rho_x w\rangle_0 = \langle v, w\rangle,\end{aligned}$$

the representation $\rho$ is unitary. □

Weyl's trick has several interesting consequences:

**Corollary 9.24.** *Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation of a finite group $G$. The following properties hold:*

***1)*** *$\rho$ is equivalent to a unitary representation.*
***2)*** *$\rho$ is either irreducible or decomposable.*
***3)*** *Each $\rho_g$ is diagonalizable.*

*Proof.* The first claim follows from Example 9.8 and Weyl's trick. The second claim, from 1) and Proposition 9.22. Finally, 3) follows from Weyl's trick immediately, as unitary matrices are diagonalizable. □

**Exercise 9.25.** 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 $\mathbb{Z} \to \mathbf{GL}_2(\mathbb{C})$, $1 \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

# Lecture 7

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

**Theorem 9.26 (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 $\rho$ has degree $n+1$. If $\rho$ is irreducible, we are done. If not, 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 $\rho$ is completely reducible. □

**Example 9.27.** 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 $\rho_g$ 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

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

**Exercise 9.28.** 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.

**Lemma 9.29 (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 $\rho$ is irreducible. Thus $T$ is injective. Since $T(V)$ is a non-zero invariant subspace of $W$, it follows from the fact that $\psi$ is irreducible that $T$ is surjective. Therefore $T$ is bijective. □

Two applications:

**Proposition 9.30.** *If $G$ is finite, $\rho\colon G \to \mathbf{GL}(V)$ is an irreducible representation, and $T\colon V \to V$ is invariant, then $T = \lambda \operatorname{id}$ for some $\lambda \in \mathbb{C}$.*

*Proof.* Let $\lambda$ be an eigenvalue of $T$. Then $T - \lambda \operatorname{id}$ is invariant, as

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

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

**Proposition 9.31.** *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 $\rho_h = \lambda_h \operatorname{id}$. 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 $\rho$ is irreducible, it follows that $V = \langle v \rangle$. □

## §10. Characters

This lecture is devoted to study character theory. Fix a group and consider (matrix) representations of groups. How can we study those matrices? Since equivalence of representations translates into equivalence of matrices, it makes sense to use linear algebra. We can use the characteristic polynomial of the matrix,

$$A \in \mathbb{C}^{n\times n} \rightsquigarrow \chi_A(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{C}[X],$$

or any of the numbers $a_0, \ldots, a_n \in \mathbb{C}$, as all of them are indeed invariants of the matrix $A$. The determinant and the trace of $A$ are examples of such numbers. In the context of group representations, the trace is particularly interesting.

**Definition 10.1.** Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. The **character** of $\rho$ is the map $\chi_\rho\colon G \to \mathbb{C}$, $g \mapsto \operatorname{trace}\rho_g$.

If a representation $\rho$ is irreducible, its character is said to be an **irreducible character**. The **degree** of a character is the degree of the affording representation.

**Proposition 10.2.** *Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation, $\chi$ be its character and $g \in G$. The following statements hold:*

***1)*** $\chi(1) = \dim V$.
***2)*** $\chi(g) = \chi(hgh^{-1})$ *for all* $h \in G$.
***3)*** $\chi(g)$ *is the sum of* $\chi(1)$ *roots of one of order* $|g|$.
***4)*** $\chi(g^{-1}) = \overline{\chi(g)}$.
***5)*** $|\chi(g)| \le \chi(1)$.

*Proof.* The first statement is trivial. To prove 2) note that

$$\chi(hgh^{-1}) = \operatorname{trace}(\rho_{hgh^{-1}}) = \operatorname{trace}(\rho_h\rho_g\rho_h^{-1}) = \operatorname{trace}\rho_g = \chi(g).$$

Statement 3) follows from the fact that the trace of $\rho_g$ is the sum of the eigenvalues of $\rho_g$ and these numbers are roots of the polynomial $X^{|g|} - 1 \in \mathbb{C}[X]$. To prove 4) write $\chi(g) = \lambda_1 + \cdots + \lambda_k$, where the $\lambda_j$ are roots of one. Then

$$\overline{\chi(g)} = \sum_{j=1}^{k} \overline{\lambda_j} = \sum_{j=1}^{k} \lambda_j^{-1} = \operatorname{trace}(\rho_g^{-1}) = \operatorname{trace}(\rho_{g^{-1}}) = \chi(g^{-1}).$$

Finally, we prove 5). Use 3) to write $\chi(g)$ as the sum of $\chi(1)$ roots of one, say $\chi(g) = \lambda_1 + \cdots + \lambda_k$ for $k = \chi(1)$. Then

$$|\chi(g)| = |\lambda_1 + \cdots + \lambda_k| \le |\lambda_1| + \cdots + |\lambda_k| = \underbrace{1 + \cdots + 1}_{k\text{-times}} = k. \qquad \square$$

If two representations are equivalent, their characters are equal.

**Definition 10.3.** Let $G$ be a group and $f\colon G \to \mathbb{C}$ be a map. Then $f$ is a **class function** if $f(g) = f(hgh^{-1})$ for all $g, h \in G$.

Characters are class functions.

**Proposition 10.4.** *If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations, then $\chi_{\rho\oplus\psi} = \chi_\rho + \chi_\psi$.*

*Proof.* For $g \in G$, it follows that $(\rho \oplus \psi)_g = \begin{pmatrix} \rho_g & 0 \\ 0 & \psi_g \end{pmatrix}$. Thus

$$\chi_{\rho\oplus\psi}(g) = \operatorname{trace}((\rho \oplus \phi)_g) = \operatorname{trace}(\rho_g) + \operatorname{trace}(\psi_g) = \chi_\rho(g) + \chi_\psi(g). \qquad \square$$

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 $\{v_i \otimes w_j : 1 \le i \le k, 1 \le j \le l\}$ 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

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

Note that 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 $\lambda_{ij} \in \mathbb{C}$, and not of the form $v \otimes w$ for $v \in V$ and $w \in W$.

The bilinearity of tensor products is crucial. For example,

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

**Definition 10.5.** Let $\rho : G \to \mathbf{GL}(V)$ and $\psi : G \to \mathbf{GL}(W)$ be representations. The **tensor product** of $\rho$ and $\psi$ is the representation of $G$ given by

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

where

$$(\rho \otimes \psi)_g(v \otimes w) = \rho_g(v) \otimes \psi_g(w)$$

for $v \in V$ and $w \in W$.

A direct calculation shows that the tensor product of representations is indeed a representation.

**Proposition 10.6.** *If $\rho : G \to \mathbf{GL}(V)$ and $\psi : G \to \mathbf{GL}(W)$ are representations, then*

$$\chi_{\rho\otimes\psi} = \chi_\rho \chi_\psi.$$

*Proof.* For each $g \in G$, the map $\rho_g$ is diagonalizable. Let $\{v_1, \ldots, v_n\}$ be a basis of eigenvectors of $\rho_g$ and let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ be such that $\rho_g(v_i) = \lambda_i v_i$ for all $i \in \{1, \ldots, n\}$. Similarly, let $\{w_1, \ldots, w_m\}$ be a basis of eigenvectors of $\psi_g$ and $\mu_1, \ldots, \mu_m \in \mathbb{C}$ be such that $\psi_g(w_j) = \mu_j w_j$ for all $j \in \{1, \ldots, m\}$. Each $v_i \otimes w_j$ is eigenvector of $\rho \otimes \psi$ with eigenvalue $\lambda_i \mu_j$, as

$$(\rho\otimes\psi)_g(v_i\otimes w_j)=\rho_g v_i\otimes\psi_g w_j=\lambda_i v_i\otimes\mu_j v_j=(\lambda_i\mu_j)v_i\otimes w_j.$$

Thus $\{v_i\otimes w_j : 1\le i\le n, 1\le j\le m\}$ is a basis of eigenvectors and the $\lambda_i\mu_j$ are the eigenvalues of $(\rho\otimes\psi)_g$. It follows that

$$\chi_{\rho\otimes\psi}(g)=\sum_{i,j}\lambda_i\mu_j=\left(\sum_i\lambda_i\right)\left(\sum_j\mu_j\right)=\chi_\rho(g)\chi_\psi(g). \qquad \square$$

For completeness, we mention without proof that it is also possible to define the dual $\rho^*\colon G\to\mathbf{GL}(V^*)$ of a representation $\rho\colon G\to\mathbf{GL}(V)$ by the formula

$$(\rho_g^* f)(v)=f(\rho_g^{-1}v),\quad g\in G,\ f\in V^* \text{ and } v\in V.$$

We claim that the character of the dual representation is then $\overline{\chi_\rho}$. Let $\{v_1,\dots,v_n\}$ be a basis of $V$ and $\lambda_1,\dots,\lambda_n\in\mathbb{C}$ be such that $\rho_g v_i=\lambda_i v_i$ for all $i\in\{1,\dots,n\}$. If $\{f_1,\dots,f_n\}$ is the dual basis of $\{v_1,\dots,v_n\}$, then

$$(\rho_g^* f_i)(v_j)=f_i(\rho_g^{-1}v_j)=\overline{\lambda_j}f_i(v_j)=\overline{\lambda_j}\delta_{ij}$$

and the claim follows.

## §11. Schur's orthogonality relations

Let $\rho\colon G\to\mathbf{GL}(V)$ and $\psi\colon G\to\mathbf{GL}(W)$ be representations of a finite group $G$. Since $V$ and $W$ are vector spaces, the set

$$\mathrm{Hom}(V,W)=\{T\colon V\to W : T \text{ is linear}\}$$

is a vector space with

$$\begin{aligned}(\lambda T)(v)&=\lambda T(v) && \text{for all } \lambda\in\mathbb{C} \text{ and all } v\in V,\\ (T+T_1)(v)&=T(v)+T_1(v) && \text{for all } v\in V.\end{aligned}$$

We claim that the set $\mathrm{Hom}_G(V,W)$ of invariant maps is a subspace of $\mathrm{Hom}(V,W)$. Indeed, the zero map is clearly invariant. If $T,T_1\in\mathrm{Hom}_G(V,W)$ and $\lambda\in\mathbb{C}$, then

$$(T+\lambda T_1)(\rho_g v)=T(\rho_g v)+\lambda T_1(\rho_g v)=\psi_g T(v)+\lambda\psi_g T_1(v)=\psi_g((T+\lambda T_1)(v))$$

for all $v\in V$.

**Proposition 11.1.** *Let $\rho\colon G\to\mathbf{GL}(V)$ and $\psi\colon G\to\mathbf{GL}(W)$ be representations and $T\colon V\to W$ be a linear map. Then*

$$T^{\#}=\frac{1}{|G|}\sum_{g\in G}\psi_{g^{-1}}T\rho_g\in\mathrm{Hom}_G(V,W).$$

*Moreover, the map* $\mathrm{Hom}(V,W) \to \mathrm{Hom}_G(V,W)$, $T \mapsto T^{\#}$, *is linear and surjective.*

*Proof.* Let $h \in G$ and $v \in V$. Then

$$\begin{aligned} T^{\#}\rho_h(v) &= \frac{1}{|G|}\sum_{g\in G} \psi_{g^{-1}} T \rho_g \rho_h(v) = \frac{1}{|G|}\sum_{g\in G} \psi_{g^{-1}} T \rho_{gh}(v) \\ &= \frac{1}{|G|}\sum_{x\in G} \psi_{hx^{-1}} T \rho_x(v) = \frac{1}{|G|}\sum_{x\in G} \psi_h \psi_{x^{-1}} T \rho_x(v) = \psi_h T^{\#}(v). \end{aligned}$$

It is a routine calculation to show that $T \mapsto T^{\#}$ is a linear map. The map $T \mapsto T^{\#}$ is surjective since if $T \in \mathrm{Hom}_G(V,W)$, then

$$T^{\#}(v) = \frac{1}{|G|}\sum_{g\in G} \psi_{g^{-1}} T \rho_g(v) = \frac{1}{|G|}\sum_{g\in G} \psi_{g^{-1}} \psi_g T(v) = T(v)$$

holds for all $v \in V$, so $T^{\#} = T$. □

If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are non-equivalent irreducible representations and $T\colon V \to W$ is a linear map, then $T^{\#} = 0$, as $T^{\#} \in \mathrm{Hom}_G(V,W) = \{0\}$ by the previous proposition and Schur's lemma.

**Theorem 11.2 (Ergodic theorem).** *Let* $\rho\colon G \to \mathbf{GL}(V)$ *be an irreducible representation. If* $T\colon V \to V$ *is linear, then* $T^{\#} = (\dim V)^{-1}\,\mathrm{trace}(T)\,\mathrm{id}$.

*Proof.* The previous proposition and Schur's lemma imply that $T^{\#} = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$. We now compute the trace of $T^{\#}$. On the one hand,

$$\mathrm{trace}(T^{\#}) = \mathrm{trace}(\lambda\,\mathrm{id}) = (\dim V)\lambda.$$

On the other hand.

$$\mathrm{trace}(T^{\#}) = \frac{1}{|G|}\sum_{g\in G} \mathrm{trace}(\rho_{g^{-1}} T \rho_g) = \frac{1}{|G|}\sum_{g\in G} \mathrm{trace}(T) = \mathrm{trace}(T),$$

as $\mathrm{trace}(ABA^{-1}) = \mathrm{trace}(B)$ for all $A$ and $B$. Hence

$$\mathrm{trace}(T^{\#}) = (\dim V)^{-1}\,\mathrm{trace}(T)\,\mathrm{id}\,.$$ □

# Lecture 8

We now prove Schur's orthogonality relations. We need some preliminary material. First, recall that the matrix $E_{ij}$ is given by

$$(E_{ij})_{kl} = \delta_{ik}\delta_{jl}, \qquad \delta_{xy} = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise.} \end{cases}$$

If $\rho\colon G \to \mathbf{GL}(V) \simeq \mathbf{GL}_n(\mathbb{C})$ is a representation of a finite group $G$, then $\rho_g$ is the matrix $(\rho_{ij}(g))$ and hence the character of $\rho$ is given by

$$\chi_\rho(g) = \sum_{i=1}^{n} \rho_{ii}(g).$$

**Lemma 11.3.** *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations. Then $(E_{ki}^{\#})_{lj} = \langle \rho_{ij}, \psi_{kl} \rangle$.*

*Proof.* Assume that $\rho$ is unitary. Then $\rho_g^{-1} = \rho_{g^{-1}} = \rho_g^* = \overline{\rho}_g^T$ for all $g \in G$. Thus

$$\begin{aligned}
(E_{ki}^{\#})_{lj} &= \frac{1}{|G|} \sum_{g \in G} (\psi_{g^{-1}} E_{ki} \rho_g)_{lj} \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{p,q} \psi_{lq}(g^{-1})(E_{ki})_{qp} \rho_{pj}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \psi_{lk}(g^{-1}) \rho_{ij}(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \overline{\psi_{kl}(g)} \rho_{ij}(g) = \langle \rho_{ij}, \psi_{kl} \rangle.
\end{aligned}$$

□

**Theorem 11.4 (Schur).** *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations of a finite group $G$. Then the following statements hold:*

***1)*** *$\langle \rho_{ij}, \psi_{kl} \rangle = 0$ if $\rho$ and $\psi$ are not equivalent.*

***2)*** $\langle \rho_{ij}, \rho_{kl} \rangle = \dfrac{1}{\dim V} \delta_{ik} \delta_{lj}$.

*Proof.* Let us prove the first claim. Since $\rho$ and $\psi$ are not equivalent, it follows from Schur's lemma that $\mathrm{Hom}_G(V, W) = \{0\}$. Thus $E_{ki}^{\#} \in \mathrm{Hom}_G(V, W) = \{0\}$ by the Ergodic theorem.

To prove the second claim, we use the previous lemma:

$$(E_{ki}^{\#})_{lj} = \langle \rho_{ij}, \rho_{kl} \rangle = \frac{1}{\dim V} (\operatorname{trace} E_{ki}) \delta_{lj} = \frac{1}{\dim V} \delta_{ki} \delta_{lj}. \qquad \square$$

Now we can prove Schur's first orthogonality relation.

**Theorem 11.5 (Schur).** *Let $\rho \colon G \to \mathbf{GL}(V)$ and $\psi \colon G \to \mathbf{GL}(W)$ be irreducible representations of a finite group $G$. Then*

$$\langle \chi_\rho, \chi_\psi \rangle = \begin{cases} 1 & \text{if } \rho \simeq \psi, \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* Let $n = \dim V$ and $m = \dim W$. We compute

$$\begin{aligned} \langle \chi_\rho, \chi_\psi \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_\psi}(g) \\ &= \sum_{1=1}^{n} \sum_{j=1}^{m} \sum_{g \in G} \frac{1}{|G|} \rho_{ii}(g) \overline{\psi_{jj}(g)} \\ &= \sum_{1=1}^{n} \sum_{j=1}^{m} \langle \rho_{ii}, \psi_{jj} \rangle = \begin{cases} 1 & \text{if } \rho \simeq \psi, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \qquad \square$$

Schur's theorem has several corollaries.

**Exercise 11.6.** If $\rho \colon G \to \mathbf{GL}(V)$ is a unitary irreducible representation of degree $n$, then

$$\{\sqrt{n} \rho_{ij} : 1 \le i, j \le n\}$$

is an orthonormal set of size $n^2$.

Recall that $L(G) = \{f \colon G \to \mathbb{C}\}$ is a vector space with

$$(f+g)(x) = f(x) + g(x), \quad (\lambda f)(x) = \lambda f(x), \quad f, g \in L(G), \lambda \in \mathbb{C}, x \in G.$$

Let $C(G)$ be the subspace of class functions. We claim that $\dim C(G) = K(G)$, the number of conjugacy classes of $G$. If $C$ is a conjugacy class, then

$$\delta_C \colon G \to \mathbb{C}, \quad \delta_C(x) = \begin{cases} 1 & \text{if } x \in C, \\ 0 & \text{otherwise.} \end{cases}$$

is a class function. Let us prove that the set $\{\delta_C : C \text{ is a conjugacy class of } G\}$ is a basis of $C(G)$. It is a generating set because each $f$ can be written as

$$f = \sum_C f(C)\delta_C.$$

The $\delta_C$ are linearly independent because they are orthogonal: If $C$ and $D$ are conjugacy classes of $G$, then

$$\langle \delta_C, \delta_D \rangle = \frac{1}{|G|} \sum_{x \in G} \delta_C(x)\overline{\delta_D(x)} = \begin{cases} |C|/|G| & \text{if } C = D, \\ 0 & \text{otherwise.} \end{cases}$$

**Corollary 11.7.** *A finite group has finitely many classes of irreducible representations.*

*Proof.* Let $G$ be a finite group. Every isomorphism class of representations of $G$ contains a unitary representation (Corollary 9.24). Since $\dim L(G) = |G|$, every linearly independent set of vectors from $L(G)$ have at most $|G|$ elements. By Schur's theorem 11.5, the entries of inequivalent unitary representations of $G$ form an orthogonal set of non-zero vectors of $L(G)$. Thus there are at most $|G|$ equivalence classes of irreducible representations. □

Let $G$ be a finite group. Since $G$ has only finitely many non-equivalent irreducible representation, we will often say that

$$\rho_1, \ldots, \rho_r$$

are *the* irreducible representations of $G$, where it is assumed that the $\rho_i$ form a complete set of representatives of irreducible representations of $G$. For each $i$ we write $\chi_i = \chi_{\rho_i}$. The set of irreducible characters will be denoted by

$$\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_r\}.$$

**Corollary 11.8.** *Let $G$ be a finite group. There are at most $K(G)$ equivalence classes of irreducible representations of $G$.*

*Proof.* Non-equivalent representations have different characters. Irreducible characters form an orthonormal set, thus they are linearly independent. Since irreducible characters are class functions, it follows that there are at most $K(G)$ irreducible different characters. □

Let $m \in \mathbb{Z}_{>0}$. If $V$ is a vector space, we write $mV = V \oplus \cdots \oplus V$ ($m$-times). Similarly, if $\rho$ is a representation, we write $m\rho = \rho \oplus \cdots \oplus \rho$ ($m$-times).

**Theorem 11.9.** *Let $\rho_1, \ldots, \rho_r$ be the irreducible representations of a finite group $G$. If $\rho = \sum_{j=1}^r m_j \rho_j$ where $m_1, \ldots m_r \in \mathbb{Z}_{\geq 0}$, then $m_i = \langle \chi_\rho, \chi_i \rangle$ for all $i \in \{1, \ldots, r\}$.*

*Proof.* Write $\chi_\rho = \sum_{j=1}^r m_j \chi_j$. Then

$$\langle \chi_\rho, \chi_i \rangle = \sum_{j=1}^r m_j \langle \chi_j, \chi_i \rangle = m_i$$

for all $i \in \{1, \ldots, r\}$. □

The theorem states that the decomposition of a representation $\rho$ into irreducibles is unique and is determined (up to equivalence) by its character.

**Corollary 11.10.** *A representation $\rho$ of a finite group is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

*Proof.* We first decompose $\rho$ as a sum of irreducibles, say $\rho = \sum_{j=1}^r m_j \rho_j$ with $m_1, \ldots, m_r \geq 0$. Then $\langle \chi_\rho, \chi_\rho \rangle = \sum_{j=1}^r m_j^2$. Now $\langle \chi_\rho, \chi_\rho \rangle = 1$ if and only if there is exactly one $j$ such that $m_j = 1$ and $m_i = 0$ for all $i \neq j$. □

**Exercise 11.11.** Let $G$ and $H$ be finite groups. If $\rho \colon H \to \mathbf{GL}(V)$ is an irreducible representation of $H$ and $f \colon G \to H$ is a surjective group homomorphism, then the composition $\rho f \colon G \to \mathbf{GL}(V)$ is an irreducible representation.

Recall that the left regular representation of a finite group $G$ is the group homomorphism $L \colon G \to \mathbf{GL}(V)$, where $V$ is the complex vector space with basis $\{g : g \in G\}$ and $L_g(x) = gx$ for all $g, x \in G$.

**Theorem 11.12.** *Let $G$ be a finite group and $L$ be its regular representation. Then $L = \sum_{j=1}^r n_j \rho_j$, where $n_j = \deg \rho_j$.*

*Proof.* Let $G = \{g_1, \ldots, g_n\}$, $n = |G|$. If $g \in G$, since $L_g(g_i) = g g_i$ for all $i$, the matrix of $L_g$ in the basis $\{g_1, \ldots, g_n\}$ is then

$$(L_g)_{ij} = \begin{cases} 1 & \text{if } g_i = g g_j, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\chi_L(g) = \operatorname{trace}(L_g) = \sum_{i=1}^n (L_g)_{ii} = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$\langle \chi_L, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_L(g) \overline{\chi_i(g)} = \frac{1}{|G|} |G| \overline{\chi_i(1)} = n_i$$

for all $i \in \{1, \ldots, n\}$. □

Now several corollaries.

**Corollary 11.13.** *Let $G$ be a finite group and $\rho_1, \dots, \rho_r$ be the irreducible representations of $G$. For each $k$ let $n_k = \deg \rho_k$. The following statements hold:*

***1)*** $|G| = n_1^2 + \cdots + n_r^2$.
***2)*** $\{\sqrt{n_k}(\rho_k)_{ij} : 1 \le k \le r, 1 \le i, j \le n_k\}$ *is an orthonormal basis of* $L(G)$.
***3)*** $r$ *is equal to the number of conjugacy classes of* $G$.

*Proof.* Since $\chi_L = \sum_{j=1}^r n_j \chi_j$, the first claim follows. The second claim follows from the orthogonality relations. Let us prove the third claim. Let $f \in C(G)$ and write $f$ as a linear combination of the $(\rho_k)_{ij}$, say

$$f = \sum_{i,j,k} \lambda_{ijk} (\rho_k)_{ij}, \quad \lambda_{ijk} \in \mathbb{C}.$$

If $x \in G$, then

$$\begin{aligned} f(x) &= \frac{1}{|G|} \sum_{g \in G} f(g^{-1}xg) \\ &= \frac{1}{|G|} \sum_{g \in G} \sum_{i,j,k} \lambda_{ijk} (\rho_k)_{ij}(g^{-1}xg) = \sum_{i,j,k} \lambda_{ijk} \frac{1}{|G|} \sum_{g \in G} (\rho_k)_{ij}(g^{-1}xg). \end{aligned}$$

Let $T = (\rho_k)_x = \rho_k(x) \colon V \to V$. Then

$$T^{\#} = \frac{1}{|G|} \sum_{g \in G} (\rho_k)_{g^{-1}} (\rho_k)_x (\rho_k)_g = \frac{1}{|G|} \sum_{g \in G} (\rho_k)(g^{-1}xg) = \frac{1}{n_k} \chi_k(x) \operatorname{id}$$

by the Ergodic theorem and because $\rho_k$ is a group homomorphism. Thus

$$f(x) = \sum_{i,j,k} \lambda_{ijk} \left((\rho_k)_x\right)_{ij} = \sum_{i,j,k} \lambda_{ijk} \frac{1}{n_k} \chi_k(x) \delta_{ij} = \sum_{i,k} \lambda_{iik} \frac{1}{n_k} \chi_k(x). \qquad \square$$

This implies that $\dim C(G) \le r$ and the claim follows.

In the following exercise, the reader is asked to prove the second Schur's orthogonality relation.

**Exercise 11.14.** Let $G$ be a finite group and $C$ and $D$ be conjugacy classes of $G$. If $g \in C$ and $h \in D$, then

$$\sum_{\chi \in \operatorname{Irr}(G)} \chi(g) \overline{\chi(h)} = \begin{cases} |G|/|C| & \text{if } C = D, \\ 0 & \text{otherwise.} \end{cases}$$

## §12. Examples

Let $G$ be a finite group and $\chi_1, \ldots, \chi_r$ be the irreducible characters of $G$. Without loss of generality we may assume that $\chi_1$ is the trivial character, i.e. $\chi_1(g) = 1$ for all $g \in G$. Recall that $r$ is the number of conjugacy classes of $G$. Each $\chi_j$ is constant on conjugacy classes. The **character table** of $G$ is given by

| | $1$ | $k_2$ | $\cdots$ | $k_r$ |
|---|---|---|---|---|
| | $1$ | $g_2$ | $\cdots$ | $g_r$ |
| $\chi_1$ | $1$ | $1$ | $\cdots$ | $1$ |
| $\chi_2$ | $n_2$ | $\chi_2(g_2)$ | $\cdots$ | $\chi_2(g_r)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| $\chi_r$ | $n_r$ | $\chi_r(g_2)$ | $\cdots$ | $\chi_r(g_r)$ |

where the $n_j$ are the degrees of the irreducible representations of $G$ and each $k_j$ is the size of the conjugacy class of the element $g_j$. By convention, the character table contains not only the values of the irreducible characters of the group.

**Example 12.1.** Sea $G = \langle g : g^4 = 1 \rangle$ be the cyclic group of order four. The character table of $G$ is given by

| | $1$ | $1$ | $1$ | $1$ |
|---|---|---|---|---|
| | $1$ | $g$ | $g^2$ | $g^3$ |
| $\chi_1$ | $1$ | $1$ | $1$ | $1$ |
| $\chi_2$ | $1$ | $\lambda$ | $\lambda^2$ | $\lambda^3$ |
| $\chi_3$ | $1$ | $\lambda^2$ | $\lambda^4$ | $\lambda^2$ |
| $\chi_4$ | $1$ | $\lambda^3$ | $\lambda^2$ | $\lambda$ |

**Exercise 12.2.** Let $n \in \mathbb{Z}_{>0}$ be such that $n \geq 2$. Let $C_n = \langle g : g^n = 1 \rangle$ be the cyclic group of order $n$.

**1)** Prove that the maps $\chi_i : C_n \to \mathbb{C}^\times$, $g^k \mapsto e^{2\pi i k/n}$, where $i \in \{0, 1, \ldots, n-1\}$, are the irreducible representations of $C_n$.

**2)** Let $\lambda$ be a primitive root of 1 of order $n$. Prove that the character table of $C_n$ of order $n$ is given by

| | $1$ | $1$ | $1$ | $\cdots$ | $1$ |
|---|---|---|---|---|---|
| | $1$ | $g$ | $g^2$ | $\cdots$ | $g^{n-1}$ |
| $\chi_1$ | $1$ | $1$ | $1$ | $\cdots$ | $1$ |
| $\chi_2$ | $1$ | $\lambda$ | $\lambda^2$ | $\cdots$ | $\lambda^{n-1}$ |
| $\chi_3$ | $1$ | $\lambda^2$ | $\lambda^4$ | $\cdots$ | $\lambda^{n-2}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ |
| $\chi_n$ | $1$ | $\lambda^{n-1}$ | $\lambda^{n-2}$ | $\cdots$ | $\lambda$ |

**Exercise 12.3.** Let $A$ and $B$ be abelian groups. We write $\mathrm{Irr}(A) = \{\rho_1, \ldots, \rho_r\}$ and $\mathrm{Irr}(B) = \{\phi_1, \ldots, \phi_s\}$. Prove that the maps

$$\varphi_{ij}\colon A\times B\to\mathbb{C}^\times,\quad (a,b)\mapsto \rho_i(a)\phi_j(b),$$

where $i\in\{1,\dots,r\}$ and $j\in\{1,\dots,s\}$, are the irreducible representations of $A\times B$.

Let us show a particular example of the previous exercise.

**Example 12.4.** The character table of the group $C_2\times C_2=\{1,a,b,ab\}$ is

| | 1 | 1 | 1 | 1 |
|---|---|---|---|---|
| | 1 | $a$ | $b$ | $ab$ |
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | −1 | −1 |
| $\chi_3$ | 1 | −1 | 1 | −1 |
| $\chi_4$ | 1 | −1 | −1 | 1 |

**Example 12.5.** The symmetric group $\mathbb{S}_3$ has three conjugacy classes. The representatives are id, (12) and (123). There are three irreducible representations. We already found all the irreducible characters! The character table of $\mathbb{S}_3$ is given by

| | 1 | 3 | 2 |
|---|---|---|---|
| | 1 | (12) | (123) |
| $\chi_1$ | 1 | 1 | 1 |
| $\chi_2$ | 1 | −1 | 1 |
| $\chi_3$ | 2 | 0 | −1 |

Let us recall how this table was computed. Degree-one irreducibles were easy to compute. To compute the third row of the table one possible approach is to use the irreducible representation

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

Then

$$\chi_3((12))=\operatorname{trace}\begin{pmatrix}-1&1\\0&1\end{pmatrix}=0,$$
$$\chi_3((123))=\chi_3((12)(23))=\operatorname{trace}\begin{pmatrix}0&-1\\1&-1\end{pmatrix}=-1.$$

We should remark that the irreducible representation mentioned is not really needed to compute the third row of the character table. We can, for example, use the regular representation $L$. The character of $L$ is given by

$$\chi_L(g)=\begin{cases}6 & \text{si } g=\mathrm{id},\\ 0 & \text{si } g\neq\mathrm{id}.\end{cases}$$

The equality $0=\chi_L((12))=1-1+2\chi_3((12))$ implies that $\chi_3((12))=0$ and the equality $0=\chi_L((123))=1+1+2\chi_3((123))$ implies that $\chi_3((123))=-1$.

Another approach uses the orthogonality relations. We need to compute $\chi_3((12))$ and $\chi_3((123))$. Let $a = \chi_3((12))$ and $b = \chi_3((123))$. Then we get that $a = 0$ and $b = -1$. We just need to solve

$$0 = \langle \chi_3, \chi_1 \rangle = \frac{1}{6}(2 + 3a + 2b),$$
$$0 = \langle \chi_3, \chi_2 \rangle = \frac{1}{6}(2 - 3a + 2b).$$

**Exercise 12.6.** Compute the character table of $\mathbb{S}_4$.

**Example 12.7.** We now compute the character table of the alternating group $\mathbb{A}_4$. This group has 12 elements and four conjugacy classes.

| representative | id | (123) | (132) | (123) |
|---|---|---|---|---|
| size | 1 | 4 | 4 | 3 |

Since $[\mathbb{A}_4, \mathbb{A}_4] = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, $\mathbb{A}_4/[\mathbb{A}_4, \mathbb{A}_4]$ has three elements. Thus $\mathbb{A}_4$ has three degree-one irreducibles and an irreducible character of degree three. Let $\omega = \exp(2\pi i/3)$ be a primitive cubic root of 1. If $\chi$ is a non-trivial degree-one character, then $\chi((123)) = \omega^j$ for some $j \in \{1, 2\}$ and $\chi((132)) = \omega^{2j}$. Since $(132)(134) = (12)(34)$ and the permutations (134) and (123) are conjugate,

$$\chi_i((12)(34)) = \chi_i((132)(134)) = \chi_i((132))\chi_i((134)) = \omega^3 = 1$$

for all $i \in \{1, 2\}$.

To compute $\chi_4$ we use the regular representation.

$$0 = \chi_L((12)(34)) = 1 + 1 + 1 + 3\chi_4((12)(34)),$$
$$0 = \chi_L((123)) = 1 + \omega + \omega^2 + 3\chi_4((123)),$$
$$0 = \chi_L((132)) = 1 + \omega + \omega^2 + 3\chi_4((132)).$$

Then we obtain that $\chi_4((123)) = \chi_4((132)) = 0$ and $\chi_4((12)(34)) = -1$. Therefore, the character table of $\mathbb{A}_4$ is given by

| | id | (123) | (132) | (12)(34) |
|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | $\omega$ | $\omega^2$ | 1 |
| $\chi_3$ | 1 | $\omega^2$ | $\omega$ | 1 |
| $\chi_4$ | 3 | 0 | 0 | $-1$ |

**Example 12.8.** Let $Q_8 = \{-1, 1, i, -i, j, -j\}$ be the quaternion group. The group $Q_8$ is generated by $\{i, j\}$ and the map $\rho\colon Q_8 \to \mathbf{GL}_2(\mathbb{C})$,

$$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

is a representation. The conjugacy classes of $Q_8$ are $\{1\}$, $\{-1\}$, $\{-i,i\}$, $\{-j,j\}$ and $\{-k,k\}$. So there are five irreducible representations. We can compute the character of $\rho$:

| | 1 | −1 | $i$ | $j$ | $k$ |
|---|---|---|---|---|---|
| $\chi_\rho$ | 2 | 2 | 0 | 0 | 0 |

Then $\rho$ is irreducible, es $\langle \chi_\rho, \chi_\rho \rangle = 1$.

Since $[Q_8, Q_8] = \{-1, 1\} = Z(Q_8)$, the quotient group $Q_8/[Q_8, Q_8]$ has four elements and hence there are four irreducible degree-one representations. Since $Q_8$ is non-abelian, $Q_8/Z(Q_8)$ cannot be cyclic. This implies that $Q_8/[Q_8, Q_8] \simeq C_2 \times C_2$. This allows us to compute almost all the character table of $Q_8$.

| | 1 | −1 | $i$ | $j$ | $k$ |
|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | −1 | 1 | −1 |
| $\chi_3$ | 1 | 1 | 1 | −1 | −1 |
| $\chi_4$ | 1 | 1 | −1 | −1 | 1 |
| $\chi_5$ | 2 | −2 | 0 | 0 | 0 |

It remains to compute $\chi_j(-1)$ for $j \in \{2,3,4\}$, these missing values are presented in shaded cells. To compute these values that $\langle \chi_i, \chi_j \rangle = 0$ whenever $i \neq j$. The calculations are left as an exercise.

**Exercise 12.9.** Compute the character table of the dihedral group of eight elements.

## §13. Finite simple groups (optional)

Recall that a non-trivial group is **simple** if it contains no non-trivial normal proper subgroups. Examples of simple groups are cyclic groups of prime order and the alternating groups $\mathbb{A}_n$ for $n \geq 5$. We can use the character table to detect simple groups:

**Proposition 13.1.** *Let $G$ be a finite group. Then $G$ is not simple if and only if there exists a non-trivial irreducible character $\chi$ such that $\chi(g) = \chi(1)$ for some $g \in G \setminus \{1\}$.*

The proof is out of the scope of this course.

**Example 13.2.** If there exists a group $G$ with a character table of the form

| | | | | | | |
|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 1 | 1 | 1 | -1 | 1 | -1 |
| $\chi_3$ | 1 | 1 | 1 | 1 | -1 | -1 |
| $\chi_4$ | 1 | 1 | 1 | -1 | -1 | 1 |
| $\chi_5$ | 2 | -2 | 2 | 0 | 0 | 0 |
| $\chi_6$ | 8 | 0 | -1 | 0 | 0 | 0 |

then $G$ cannot be simple. Note that such a group $G$ would have order $\sum_{i=1}^{6} \chi_i(1)^2 = 72$. Mathieu's group $M_9$ has this character table!

**Example 13.3.** Let $\alpha = \frac{1}{2}(-1+\sqrt{7}i)$. If there exists a group $G$ with a character table of the form

| | | | | | | |
|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 7 | -1 | -1 | 1 | 0 | 0 |
| $\chi_3$ | 8 | 0 | 0 | -1 | 1 | 1 |
| $\chi_4$ | 3 | -1 | 1 | 0 | $\alpha$ | $\overline{\alpha}$ |
| $\chi_5$ | 3 | -1 | 1 | 0 | $\overline{\alpha}$ | $\alpha$ |
| $\chi_6$ | 6 | 2 | 0 | 0 | 0 | 0 |

then $G$ is simple. Note that such a group $G$ would have order $\sum_{i=1}^{6} \chi_i(1)^2 = 168$. The group

$$\mathbf{PSL}_2(7) = \mathbf{SL}_2(7)/Z(\mathbf{SL}_2(7))$$

is a simple group that has this character table!

Character theory is one of the tools in the classification of finite simple groups. One of the first non-trivial applications one finds of character theory is the following result:

**Theorem 13.4 (Burnside).** *Let $G$ be a finite simple group of order $p^a q^b$ for some prime numbers $p$ and $q$. Then $G$ is cyclic.*

The proof uses character theory. It is not hard, but it is out of the scope of this course. Burnside's theorem is essential and generalizes in many different directions.

**Theorem 13.5 (Feit–Thompson).** *Let $G$ be a finite simple group of odd order. Then $G$ is cyclic.*

The proof is hard and occupies a full volume of the *Pacific Journal of Mathematics*, see [4]. Feit–Thompson theorem was formally verified by the computer proof assistant Coq, see [5] for the announcement.

The proof of Feit–Thompson theorem suggests the following conjecture:

**Conjecture 13.6 (Feit–Thompson).** There are not distinct prime numbers $p$ and $q$ such that $\frac{p^q-1}{p-1}$ divides $\frac{q^p-1}{q-1}$.

The conjecture is still open; see [11] for some partial results.

Feit–Thompson theorem is one of the starting points of the classification of finite simple groups (CFSG). This classification is one of the deepest theorems of the 20th century.

**Theorem 13.7 (CFSG).** *Let $G$ be a finite simple group. Then $G$ lies in one (or more) of the following families:*

***1)*** *Cyclic groups of prime order.*
***2)*** *$\mathbb{A}_n$ for $n \geq 5$.*

***3)*** *Finite groups of Lie type.*
***4)*** *26 sporadic simple groups.*

Groups of Lie type are finite analogs of simple Lie groups, such as $\mathbf{SL}_n(\mathbb{C})$. A typical example of a finite simple group of Lie type is $\mathbf{PSL}_n(p)$ for some prime number $p$, which is defined as $\mathbf{SL}_n(p)$ over its center.

The sporadic groups are 26 groups that do not follow a systematic pattern. The first five of the sporadic groups were discovered by Mathieu in the 1860s, and the other 21 were found between 1965 and 1975. Several of these groups were predicted to exist before they were constructed, sometimes just knowing their character tables! The full list of sporadic simple groups is as follows:

- Mathieu groups $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$ and $M_{24}$.
- Janko groups $J_1$, $J_2$, $J_3$ and $J_4$.
- Conway groups $Co_1$, $Co_2$ and $Co_3$.
- Fischer groups $Fi_{22}$, $Fi_{23}$ and $Fi_{24}$.
- Higman–Sims group $HS$.
- McLaughlin group $McL$.
- Held group $He$.
- Rudvalis group $Ru$.
- Suzuki group $Suz$.
- O'Nan group $ON$.
- Harada–Norton group $HN$.
- Lyons group $Ly$.
- Thompson group $Th$.
- Baby Monster group $B$.
- Monster group $M$.

Mathieu groups can be realized as automorphism groups of certain very complicated combinatorial structures known as **Steiner systems**. A concrete example:

$$M_{11} = \langle (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11), (3\,7\,11\,8)(4\,10\,5\,6) \rangle,$$

which is a subgroup of $\mathbb{S}_{11}$ of order 7920. The group $M_{11}$ contains ten irreducible characters, so the character table of $M_{11}$ is essentially a $10 \times 10$ matrix. Let us use the computer software GAP to see the character table:

```
gap> Display(CharacterTable("M11"));
M11

      2  4  4  1  3  .  1  3  3  .  .
      3  2  1  2  .  .  1  .  .  .  .
      5  1  .  .  .  1  .  .  .  .  .
     11  1  .  .  .  .  .  .  .  1  1

        1a 2a 3a 4a 5a 6a 8a 8b 11a 11b
     2P 1a 1a 3a 2a 5a 3a 4a 4a 11b 11a
     3P 1a 2a 1a 4a 5a 2a 8a 8b 11a 11b
     5P 1a 2a 3a 4a 1a 6a 8b 8a 11a 11b
```

```
     11P 1a 2a 3a 4a 5a 6a 8a 8b  1a  1a

X.1    1  1  1  1  1  1  1  1   1   1
X.2   10  2  1  2  . -1  .  .  -1  -1
X.3   10 -2  1  .  .  1  A -A  -1  -1
X.4   10 -2  1  .  .  1 -A  A  -1  -1
X.5   11  3  2 -1  1  . -1 -1   .   .
X.6   16  . -2  .  1  .  .  .   B  /B
X.7   16  . -2  .  1  .  .  .  /B   B
X.8   44  4 -1  . -1  1  .  .   .   .
X.9   45 -3  .  1  .  . -1 -1   1   1
X.10  55 -1  1 -1  . -1  1  1   .   .

A = E(8)+E(8)^3
  = Sqrt(-2) = i2
B = E(11)+E(11)^3+E(11)^4+E(11)^5+E(11)^9
  = (-1+Sqrt(-11))/2 = b11
```

Thus the character table of the Mathieu group $M_{11}$ is given by

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $\chi_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\chi_2$ | 10 | 2 | 1 | 2 | 0 | -1 | 0 | 0 | -1 | -1 |
| $\chi_3$ | 10 | -2 | 1 | 0 | 0 | 1 | $\alpha$ | $-\alpha$ | -1 | -1 |
| $\chi_4$ | 10 | -2 | 1 | 0 | 0 | 1 | $-\alpha$ | $\alpha$ | -1 | -1 |
| $\chi_5$ | 11 | 3 | 2 | -1 | 1 | 0 | -1 | -1 | 0 | 0 |
| $\chi_6$ | 16 | 0 | -2 | 0 | 1 | 0 | 0 | 0 | $\beta$ | $1/\beta$ |
| $\chi_7$ | 16 | 0 | -2 | 0 | 1 | 0 | 0 | 0 | $1/\beta$ | $\beta$ |
| $\chi_8$ | 44 | 4 | -1 | 0 | -1 | 1 | 0 | 0 | 0 | 0 |
| $\chi_9$ | 45 | -3 | 0 | 1 | 0 | 0 | -1 | -1 | 1 | 1 |
| $\chi_{10}$ | 55 | -1 | 1 | -1 | 0 | -1 | 1 | 1 | 0 | 0 |

where $\alpha = \sqrt{-2}$ and $\beta = \frac{-1-\sqrt{-11}}{2}$.

The largest sporadic simple group is the **Monster group** $M$ and has order

$$808017424794512875886459904961710757005754368000000000,$$

which is roughly $8 \times 10^{53}$. The monster group was predicted by Fischer and Griess. Griess proved the existence of the Monster group, realizing it as the automorphism group of a certain space of dimension 196884. The group $M$ can be represented as a subgroup of $\mathbf{GL}_{196883}(\mathbb{C})$. It has 194 conjugacy classes, so the character table is a $194 \times 194$ array.

# Lecture 9

## §14. Modules

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

**Definition 14.1.** Let $R$ be a ring. A **module** (over $R$) is an abelian group $M$ 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 $r_1, r_2 \in R$ y $m \in M$.
**2)** $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ for all $r \in R$ y $m_1, m_2 \in M$.
**3)** $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ for all $r_1, r_2 \in R$ y $m \in M$.
**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).

**Example 14.2.** A module over a field is a vector space.

**Example 14.3.** Every abelian group is a module over $\mathbb{Z}$.

**Example 14.4.** Let $R$ be a ring. Then $R$ is a module (over $R$) with $x \cdot m = xm$. This is the **(left) regular representation** of $R$, and it usually is denoted by ${}_R R$.

**Example 14.5.** 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 $r \cdot (x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$.

**Example 14.6.** 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.

**Example 14.7.** 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,

$$1 \cdot m = f(1)m = 1m = m,$$
$$r_1 \cdot (r_2 \cdot m) = f(r_1)(r_2 \cdot m) = f(r_1)(f(r_2)m) = (f(r_1)f(r_2))m = f(r_1r_2)m$$

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

**Example 14.8.** 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 $M = \mathbb{R}^n$ 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 $R$).

**Example 14.9.** 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 $I \to M_i$, $i \mapsto m_i$. This module is the **direct product** of the family $\{M_i : i \in I\}$.

**Example 14.10.** 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 $x \in R$.

**Example 14.11.** 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 $\mathbb{Z}/6$).

**Exercise 14.12.** Prove that $\mathbb{Z}/4$ is not a module over $\mathbb{Z}/2$.

**Definition 14.13.** Let $M$ be a module. A subset $N$ of $M$ is a **submodule** of $M$ if $(N,+)$ is a subgroup of $(M,+)$ and $x \cdot n \in N$ for all $x \in R$ and $n \in N$.

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

**Example 14.14.** 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 $M$.

**Example 14.15.** 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 $M$

**Example 14.16.** 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 $R$.

**Example 14.17.** If $V$ is a vector space and $T\colon V \to V$ 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 $n_1, n_2 \in N$.

**Exercise 14.18.** 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 $M$.

**Definition 14.19.** Let $M$ and $N$ be modules over $R$. A map $f\colon M \to N$ 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 $\mathrm{Hom}_R(M, N)$ the set of module homomorphisms $M \to N$.

**Exercise 14.20.** Let $f \in \mathrm{Hom}_R(M, N)$.

**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 $f \in \mathrm{Hom}_R(M, N)$, 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.

**Exercise 14.21.** Let $f \in \mathrm{Hom}_R(M, N)$. Prove that the following statements are equivalent:

**1)** $f$ is a monomorphism.
**2)** $\ker f = \{0\}$.
**3)** For every module $V$ and every $g, h \in \mathrm{Hom}_R(V, M)$, $fg = fh \implies g = h$.
**4)** For every module $V$ and every $g \in \mathrm{Hom}(V, M)$, $fg = 0 \implies g = 0$.

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

**Example 14.22.** Let $R = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}$. We claim that $\begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix} \ncong \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix}$ 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 $M$.

**Example 14.23.** 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 $M$.

**Example 14.24.** If $M = \mathbb{Z}$ as a module over $\mathbb{Z}$, then $m\mathbb{Z}$ is a direct sum of $M$ if and only if $m \in \{0, 1\}$, as $n\mathbb{Z} \cap m\mathbb{Z} = \{0\}$ if and only if $nm = 0$.

**Exercise 14.25.** 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 $v_1 \in V_1, \ldots, v_n \in V_n$.

**Exercise 14.26.** 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 $M$.

**Exercise 14.27.** 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)** $T(x,y) = (y,x)$.

Prove that $\{0\}$, $M$, $\mathbb{R}\times\{0\}$ and $\{0\}\times\mathbb{R}$ are the only submodules of $M$.

**Exercise 14.28.** Let $V$ be a 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 a module homomorphism $g\colon V \to V$ commutes with $T$.

**Exercise 14.29.** Prove that $\mathrm{Hom}_R(M,N)$ is a module over $Z(R)$ with the following action: If $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$, 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.

**Example 14.30.** If $R = M = \mathbb{Z}$ and $N = 2\mathbb{Z}$, then $M/N \simeq \mathbb{Z}/2$.

**Example 14.31.** Let $R$ be a commutative ring and $M$ be an $R$-module. We claim that

$$M \simeq \mathrm{Hom}_R({}_R R, M).$$

Since $R$ is commutative, it follows that $\mathrm{Hom}_R({}_R R, M)$ is a module, see Exercise 14.29. Let $\varphi\colon M \to \mathrm{Hom}_R({}_R R, M)$, $m \mapsto f_m$, where $f_m\colon R \to M$, $r \mapsto r \cdot m$. To show that $\varphi$ is well-defined it is enough to see that $\varphi(m) \in \mathrm{Hom}_R({}_R R, M)$, 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 $\varphi$ is a module homomorphism. We first note that

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

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

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

Moreover,

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

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

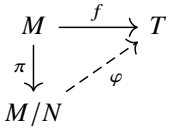
$$\begin{aligned}\varphi(r \cdot m)(s) &= f_{r \cdot m}(s) = s \cdot (r \cdot m) = (sr) \cdot m \\ &= (rs) \cdot m = f_m(rs) = \varphi(m)(rs) = (r \cdot \varphi(m))(s).\end{aligned}$$

It remains to show that $\varphi$ is bijective. We first prove that $\varphi$ 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 $\varphi$ is surjective. If $f \in \mathrm{Hom}_R({}_R R, M)$, 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




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

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 $f \in \mathrm{Hom}_R(M, N)$, 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 $(S+T)/S \simeq T/(S \cap T)$.

**Example 14.32.** 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, $(S+T)/T \simeq S/(S \cap T)$ as vector spaces. By applying dimension,

$$\dim(S+T) - \dim T = \dim(S) - \dim(S \cap T).$$

**Example 14.33.** If $N$ is a direct summand of $M$ and $M$ 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 $\pi^{-1}(Y) \hookleftarrow Y$ and $X \mapsto \pi(X)$.

**Exercise 14.34.** Let $f \in \mathrm{Hom}_R(M,N)$. 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 $g,h \in \mathrm{Hom}_R(N,T)$, $gf = hf \implies g = h$.
**4)** For every module $T$ and every $g \in \mathrm{Hom}_R(N,T)$, $gf = 0 \implies g = 0$.

**Exercise 14.35.** 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 $rM_1 \subseteq M_2$.

# Lecture 10

## §15. Noetherian modules

**Exercise 15.1.** Let $M$ be a module. Prove that the intersection of submodules of $M$ is a submodule of $M$.

**Definition 15.2.** 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

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

**Definition 15.3.** 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 $\mathbb{Z} \neq (2)$.

**Exercise 15.4.** 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.

**Exercise 15.5.** 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.

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

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0 \tag{10.1}$$

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

$$0 \longrightarrow M \xrightarrow{f} M \oplus N \xrightarrow{g} N \longrightarrow 0,$$

where $f(m) = (m, 0)$ and $g(m, n) = n$, is exact.

**Exercise 15.6.** Let

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

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.

**Exercise 15.7.** Find a finitely generated module that contains a submodule that is not finitely generated.

**Proposition 15.8.** *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 $M = (m_1, \dots, m_k)$ is finitely generated. A routine calculation shows that the map

$$\varphi\colon R^k \to M, \quad (r_1, \dots, r_k) \mapsto \sum_{j=1}^{k} r_j \cdot m_j,$$

is a surjective module homomorphism. The first isomorphism theorem implies that $R^k/\ker\varphi \simeq \varphi(R^k) = M$.

Now assume that there exists a surjective module homomorphism $\varphi\colon R^k \to M$. Since $R^k = (e_1, \dots, e_k)$, where

$$(e_i)_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

it follows that $\{\varphi(e_1), \dots, \varphi(e_k)\}$ generates $\varphi(R^k) = M$. Indeed, if $m \in M$, we write $m = \varphi(r_1, \dots, r_k)$ for some $(r_1, \dots, r_k) \in R^k$ and hence

$$m = \varphi(r_1, \dots, r_k) = \varphi\left(\sum_{i=1}^{k} r_i \cdot e_i\right) = \sum_{i=1}^{k} r_i \cdot \varphi(e_i). \qquad \square$$

**Definition 15.9.** A module $M$ is **noetherian** if every sequence $M_1 \subseteq M_2 \subseteq \cdots$ of submodules of $M$ stabilizes, that is there exists $n$ such that $M_k = M_{n+k}$ for all $k$.

**Proposition 15.10.** *Let $M$ be a module. The following statements are equivalent:*

***1)*** *$M$ is noetherian.*
***2)*** *Submodules of $M$ are finitely generated.*
***3)*** *Every non-empty family of submodules of $M$ has a maximal element (with respect to the inclusion).*

*Proof.* We first prove 2) $\implies$ 1). If $S_1 \subseteq S_2 \subseteq \cdots$ is a sequence of submodules of $M$, it follows that $S = \cup_{i\geq 1} S_i$ is a submodule 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, 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, 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 $x \notin N$. □

**Exercise 15.11.** Find a non-noetherian module such that every proper submodule is finitely generated.

**Exercise 15.12.** 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.

**Exercise 15.13.** A commutative ring $R$ is noetherian if and only if ${}_R R$ is noetherian.

**Exercise 15.14.** 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?

**Proposition 15.15.** *If $R$ is noetherian and $M$ is a finitely generated module, then $M$ is noetherian.*

*Proof.* Assume that $M = (m_1, \ldots, m_k)$. There exists a surjective homomorphism $R^k \to M$, $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^k r_i \cdot m_i$, where $R^k = \oplus_{i=1}^k R$. Since $R$ is noetherian, $R^k$ is noetherian. Thus $M$ is noetherian. □

## §16. Quotient fields

Let $R$ be an integral domain and $S = R \setminus \{0\}$. On $R \times S$ we define the following relation:

$$(r,s) \sim (r_1,s_1) \Longleftrightarrow rs_1 - r_1 s = 0.$$

**Exercise 16.1.** 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

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1}, \quad \frac{r}{s}\frac{r_1}{s_1} = \frac{rr_1}{ss_1}. \tag{10.2}$$

**Definition 16.2.** $K(R)$ is known as the **quotient field** of $R$.

Simple example: $K(\mathbb{Z}) = \mathbb{Q}$.

**Exercise 16.3.** 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 (10.2) 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

$$(rs_1 + r_1 s)s's_1' = rs_1 s's_1' + r_1 ss's_1' = r'ss_1 s_1' + r_1' s_1 ss' = (r's_1' + r_1' s)ss_1.$$

## §17. Free modules

**Definition 17.1.** 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.

A set is said to be **linearly dependent** if it is not linearly independent.

**Examples 17.2.**

**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 $M$. Is $y \in M \setminus \{x\}$, 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.

**Examples 17.3.** 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.

**Exercise 17.4.** 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 $N = (f(X))$.

**Definition 17.5.** 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.

As a consequence of Zorn's lemma, vector spaces are free.

**Examples 17.6.**

**1)** If $R$ is a ring, then $\{1\}$ is a basis of ${}_RR$, so ${}_RR$ is free.
**2)** If $R$ is a ring, then $R^n$ is free as a module over $R$.

**Exercise 17.7.** 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.

**Exercise 17.8.** Prove that $\mathbb{Q}$ is not free as a module over $\mathbb{Z}$.

**Exercise 17.9.** 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.

**Example 17.10.** $\mathbb{R}[X]$ is a free module (over $\mathbb{R}$) with basis $\{1, X, X^2, \dots\}$.

**Exercise 17.11.** 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 $ad - bc \in \{-1, 1\}$.

**Example 17.12.** If $u \in \mathcal{U}(R)$, then $\{u\}$ is a basis of ${}_RR$. Conversely, if $R$ is an integral domain and $\{z\}$ is a basis of ${}_RR$, then $z \in \mathcal{U}(R)$. Since $1 = yz$ for some $y \in R$, 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

$$R^{(I)} \simeq \bigoplus_{i \in I} R.$$

**Example 17.13.** If $I$ is a non-empty set, the module $R^{(I)}$ is free with basis $\{\delta_i : i \in I\}$, where

$$\delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

**Example 17.14.** 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.

**Example 17.15.** Let $V$ be the complex vector space with infinite basis $e_0, e_1, e_2, \ldots$ and let $R = \mathrm{End}(V)$ 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 $\{\mathrm{id}\}$ 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 $\beta = 0$.

**Example 17.16.** 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

$$\{(x, 0) : x \in X\} \cup \{(0, y) : y \in Y\}.$$

**Exercise 17.17.** Let $R$ be a commutative ring. If $M$ and $N$ are free and finitely generated, then $\mathrm{Hom}_R(M, N)$ is free and finitely generated.

Some properties of free modules:

**Proposition 17.18.** *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 $i \in I$. □

**Proposition 17.19.** *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 $f \in \mathrm{Hom}_R(M, N)$ such that $f(m_i) = n_i$ for all $i \in I$.*

*Sketch of the proof.* Note that the unique homomorphism $f : M \to N$ is defined as $f(\sum r_i \cdot m_i) = \sum r_i \cdot n_i$. □

Another application:

**Example 17.20.** There is no surjective homomorphism $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ (of modules over $\mathbb{Z}$). If $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ 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 17.19 implies that there exists a homomorphism $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $g(u) = k$ and $g(v) = l$. In particular, $fg = \mathrm{id}_{\mathbb{Z} \times \mathbb{Z}}$ 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 constradiction

Another important property:

**Proposition 17.21.** *If $M$ is a free $R$-moodule, then $M \simeq R^{(I)}$ for some set $I$.*

*Proof.* Suppose that $M$ has basis $\{m_i : i \in I\}$. There exists a unique homomorphism $f \in \mathrm{Hom}_R(M, R^{(I)})$ such that $f(m_i) = \delta_i$ for all $i \in I$, where

$$\delta_i(j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

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:

$$0 = f(\sum r_i \cdot m_i) = \sum r_i \cdot f(m_i) = \sum r_i \cdot \delta_i \implies r_i = 0 \text{ for all } i \in I. \qquad \square$$

**Corollary 17.22.** *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 $f \in \mathrm{Hom}_R(L, M)$. 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. $\square$

Another important property of free modules: free modules are *projective*.

**Proposition 17.23.** *If $M$ is a free module and $f \in \mathrm{Hom}_R(N,T)$ is surjective and $h \in \mathrm{Hom}_R(M,T)$, then there exists $\varphi \in \mathrm{Hom}_R(M,N)$ such that $f\varphi = h$.*

*Proof.* We will prove that there exists a homomorphism $\varphi$ that makes the diagram

$$\begin{array}{ccccc} & & & & M \\ & & \overset{\varphi}{\swarrow} & & \downarrow{\scriptstyle h} \\ N & \xrightarrow[f]{} & T & \longrightarrow & 0 \end{array}$$

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 $f\varphi = h$. $\square$

A consequence of the previous proposition that we will use later:

**Proposition 17.24.** *Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

*be an exact sequence of modules. If $C$ is free, then $A \oplus C \simeq B$.*

*Proof.* By considering the diagram

$$\begin{array}{ccccc} & & & & C \\ & & \overset{h}{\swarrow} & & \| \\ B & \xrightarrow[g]{} & C & \longrightarrow & 0 \end{array}$$

the previous proposition yields a homomorphism $h\colon C \to B$ such that $gh = \mathrm{id}_C$. In fact, let $\{c_i : i \in I\}$ be a basis of $C$. For each $i \in I$ let $b_i \in B$ be such that $g(b_i) = c_i$.

The map $h\colon C \to B$, $h(\sum r_i \cdot c_i) = \sum r_i \cdot b_i$, is a module homomorphism 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 $\varphi$ is a module homomorphism.

We prove that $\varphi$ 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 $f(a) = 0$, is follows that $(a,c) = (0,0)$.

Now we prove that $\varphi$ 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

$$\varphi(a,c) = f(a) + h(c) = b - h(c) + h(c) = b. \qquad \square$$

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.

**Exercise 17.25.** 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.

**Theorem 17.26.** *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

$$f_i\colon M \to K, \quad e_j \mapsto \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

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 $f(e_j) = (\sum_{i=1}^{n} f(e_i)f_i)(e_j)$ for all $j \in \{1,\dots,n\}$. Moreover, $\{f_1,\dots,f_n\}$ 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 $j \in \{1,\dots,n\}$. Thus $n = \dim V$. □

The previous result can be proved for commutative rings.

**Definition 17.27.** 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 $\operatorname{rank}(M)$.

# Lecture 11

## §18. Modules over principal domains

**Theorem 18.1.** *Let $R$ be a commutative principal domain. If $F$ is a finitely generated free module and $N$ is a submodule of $F$, then $N$ is free and* $\operatorname{rank}(N) \leq \operatorname{rank}(F)$.

*Proof.* We proceed by induction on $n = \operatorname{rank}(F)$. Si $n = 1$, 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 proves 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 $r_1 = \cdots = r_k = 0$. □

The previous theorem also holds for infinite bases. However, the proof requires the use of Zorn's lemma.

**Corollary 18.2.** *Let $R$ be a commutative principal domain. If $M$ is finitely generated 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 $\operatorname{rank}(N_1) \leq \operatorname{rank} F < \infty$. 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 $\varphi$ is surjective. $N$ is generated by $\leq k = \operatorname{rank}(N_1) \leq \operatorname{rank}(F) < \infty$ elements. □

Some exercises:

**Exercise 18.3.** Let $R$ be a commutative principal domain and let $M$ be a free 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

$$\operatorname{rank}(M) = \operatorname{rank}(S) + \operatorname{rank}(M/S).$$

**Exercise 18.4.** Let $R$ be a commutative principal domain. If $M$ is a free module of rank $n$, then every linearly independent subset of $M$ contains at most $n$ elements.

**Exercise 18.5.** Let $R$ be a commutative principal domain. and $M$ and $N$ be free modules. Prove that $M \simeq N$ if and only if $\operatorname{rank}(M) = \operatorname{rank}(N)$.

**Exercise 18.6.** Let $R$ be a commutative principal domain. If $M$ is a free module of finite rank $n$ and $\{s_1, \ldots, s_n\}$ is a generating set, then $\{s_1, \ldots, s_n\}$ is a basis of $M$.

If $M$ is a module, the **annihilator** of $M$ is defined as

$$\operatorname{Ann}(M) = \{r \in R : r \cdot m = 0 \text{ for all } m \in M\}.$$

For $m \in M$ let

$$\operatorname{Ann}(m) = \{r \in R : r \cdot m = 0\}.$$

Note that $\operatorname{Ann}(M) = \cap_{m \in M} \operatorname{Ann}(m)$. It is an exercise to show that both $\operatorname{Ann}(M)$ and $\operatorname{Ann}(m)$ are ideals of $R$. If $r \in R$, the annihilator of $r$ in $M$ is defined as

$$\operatorname{Ann}_M(r) = \{m \in M : r \cdot m = 0\}.$$

It is an exercise to show that $\operatorname{Ann}_M(r)$ is a submodule of $M$.

**Exercise 18.7.** Let $M$ be a module. Let $m \in M$ and $r \in R$ be such that $\mathrm{Ann}(m) = (r)$. Let $p \in R$ be an irreducible element.

**1)** If $p$ divides $r$, then $(m)/p \cdot (m) \simeq R/(p)$.
**2)** If $p$ does not divide $r$, then $p \cdot (m) = (m)$.

The **torsion** of a 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 $T(M) \neq \{0\}$.

**Exercise 18.8.** If $M \simeq N$, then $T(M) \simeq T(N)$.

**Exercise 18.9.** Prove that $T(\oplus_{i\in I} M_i) \simeq \oplus_{i\in I} T(M_i)$.

**Exercise 18.10.** Let $R$ be a commutative principal domain and $M$ be a 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

$$T(\mathbb{Z}\times\mathbb{Z}/3) \simeq T(\mathbb{Z}) \times T(\mathbb{Z}/3) \simeq \{0\}\times\mathbb{Z}/3 \simeq \mathbb{Z}/3.$$

**Example 18.11.** Let $R$ be a ring, viewed as a module with left multiplication. Then $T(R) = \{r \in R : rs = 0 \text{ for some non-zero } s \in R\}$.

**Example 18.12.** Let $M$ be the module (over $\mathbb{Z}$) of integer sequences, that is $M = \mathbb{Z}^I$, where $I = \{1, 2, 3, \dots\}$. Then $T(M) = \{0\}$.

**Example 18.13.** If $V$ is a real finite-dimensional vector space and $T\colon V \to V$ is a linear transformation, $V$ is a module (over $\mathbb{R}[X]$) with

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

We claim that $V$ is a torsion module, that is $V = T(V)$. Let $n = \dim V$. If $v \in V$, then $\{v, T(v), \dots, T^n(v)\}$ 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

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

Thus $v \in T(V)$.

**Theorem 18.14.** *Let $R$ be a commutative principal domain and $M$ be a finitely generated module. If $T(M) = \{0\}$, then $M$ is free.*

*Proof.* Without loss of generality we may assume that $M$ is non-zero. By assumption, $M = (X)$, where $X$ is a finite set. If $x \in X$, then $r \cdot x = 0 \iff r = 0$, as $T(M) = \{0\}$. Let $S = \{x_1, \dots, x_k\} \subseteq X$ be maximal with respect to the following property:

$$r_1 \cdot x_1 + \cdots + r_k \cdot x_k = 0 \text{ for } r_1, \dots, r_k \in R \implies r_1 = \cdots = r_k = 0.$$

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 $r_y, r_1, \dots, r_k \in R$ 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 $s_{i_1}, \dots, s_{i_m} \in R$ such that $m = \sum s_j \cdot x_{i_j}$. Then

$$r \cdot m = \sum (r s_{i_j}) \cdot x_{i_j} = \sum s_{i_j} \cdot (r \cdot x_{i_j}) \in F,$$

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. □

**Theorem 18.15.** *Let $R$ be a commutative principal domain. If $M$ is a finitely generated 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

$$0 \longrightarrow T(M) \xrightarrow{\iota} M \xrightarrow{\pi} M/T(M) \longrightarrow 0$$

where $\iota$ is the inclusion map and $\pi$ is the canonical map. Since $M/T(M)$ is free, there exists a module homomorphism $h\colon M/T(M) \to M$ such that $\pi h = \mathrm{id}$, see Proposition 17.23. This homomorphism is needed to prove that $M \simeq T(M) \oplus M/T(M)$, see Proposition 17.24.

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 $t \in T$ y $l \in L$. 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 $M/T(M)$. □

# Lecture 12

## §19. Smith's 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 $\{m_1, \dots, m_k\}$ be a set of generators. There exists a surjective module homomorphism

$$\varphi\colon R^k \to M, \quad (r_1, \dots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot m_i,$$

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 $\{e_1, \dots, e_l\}$ be a generating set of $\ker\varphi$, say

$$\begin{aligned} e_1 &= (a_{11}, a_{12}, \dots, a_{1k}), \\ e_2 &= (a_{21}, a_{22}, \dots, a_{2k}), \\ &\vdots \\ e_l &= (a_{l1}, a_{l2}, \dots, a_{lk}). \end{aligned}$$

The matrix $A = (a_{ij})_{1 \le i \le l, 1 \le j \le k}$ is the **relations matrix** of $M$ with respect to $\{m_1, \dots, m_k\}$ and $\{e_1, \dots, e_l\}$.

*Claim.* If $P \in R^{l \times l}$ is invertible, then the rows $\{f_1, \dots, f_l\}$ of $PA$ generate $\ker\varphi$. Moreover, $PA$ is the relations matrix with respect to $\{m_1, \dots, m_k\}$ and $\{f_1, \dots, f_l\}$.

Let us prove the claim. Assume that $P = (p_{ij})$. The rows of $PA$ are

$$\begin{aligned} f_1 &= p_{11}e_1 + \cdots + p_{1l}e_l, \\ f_2 &= p_{21}e_1 + \cdots + p_{2l}e_l, \\ &\vdots \\ f_l &= p_{l1}e_1 + \cdots + p_{ll}e_l. \end{aligned}$$

Moreover, $f_j \in \ker\varphi$ for all $j \in \{1,\dots,l\}$. Since $P$ is invertible, the set $\{f_1,\dots,f_l\}$ 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 $\{m_1,\dots,m_k\}$ and $\{f_1,\dots,f_l\}$.

*Claim.* If $Q \in R^{k\times k}$ is invertible and $Q^{-1} = (q_{ij})$ and for each $j \in \{1,\dots,k\}$ we define $n_j = \sum_{i=1}^{k} q_{ji} \cdot m_i$, the set $\{n_1,\dots,n_k\}$ generates $M$ and the rows of $AQ$ generate $\ker\varphi$. Moreover, $AQ$ is the relations matrix with respect to $\{n_1\dots,n_k\}$.

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 $\{n_1,\dots,n_k\}$. Let $\psi\colon R^k \to M$, $(r_1,\dots,r_k) \mapsto \sum_{i=1}^{k} r_i \cdot n_i$.

Let us prove that the rows of $AQ$ generate $\ker\psi$ with respect to $\{n_1,\dots,n_k\}$. If $(r_1,\dots,r_k) \in \ker\psi$, then $\sum_{i=1}^{k} r_i \cdot n_i = 0$. Write

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (r_1 \cdots r_k) Q^{-1} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_k \end{pmatrix} = (r_1 \cdots r_k) \begin{pmatrix} n_1 \\ \vdots \\ n_k \end{pmatrix}.$$

We remark that each $e_j$ belongs to $R^k$. Thus

$$(r_1 \cdots r_k)Q^{-1} = \left( \sum_{i=1}^{k} r_i q_{i1}, \sum_{i=1}^{k} r_i q_{2i}, \ldots, \sum_{i=1}^{k} r_i q_{ki} \right) \in \ker \varphi.$$

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

$$(r_1 \ldots r_k)Q^{-1} = (s_1 \cdots s_l) \begin{pmatrix} e_1 \\ \vdots \\ e_l \end{pmatrix} = (s_1 \cdots s_l) \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lk} \end{pmatrix}.$$

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

$$(r_1, \ldots, r_k) = \left( \sum_{i=1}^{l} s_i \cdot x_{i1}, \ldots, \sum_{i=1}^{l} s_i \cdot x_{ik} \right) = \sum_{i=1}^{l} s_i \cdot (x_{11}, \ldots, x_{1k}).$$

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 $\{e_1, \ldots, e_l\}$.

**Proposition 19.1.** *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 $\varphi \colon R^k \to M$, $(r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i \cdot m_i$, then $R^k/\ker \varphi \simeq M$, as $\varphi$ 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 $i\in\{r+1,\ldots,k\}$. □

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 $\lambda R_i$ (resp. $\lambda C_i$) 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 $I+\lambda E_{ij}$.

**Theorem 19.2 (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 $i \in \{1,\dots,r\}$ and $a_i \mid a_{i+1}$ for all $i \in \{1,\dots,r-1\}$. Moreover, the elements $a_1,\dots,a_r$ are unique up to multiplication by units.*

*Sketch of the proof.* We only prove the existence. Assume that $(R,\varphi)$ 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

$$\begin{pmatrix} \frac{b_{22}}{b_{11}} & \dots & \frac{b_{2m}}{b_{11}} \\ \vdots & & \vdots \\ \frac{b_{n2}}{b_{11}} & \dots & \frac{b_{nm}}{b_{11}} \end{pmatrix}$$

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. □

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 [8, §11]. Here we will explain the algorithm with examples.

**Example 19.3.** Let

$$A = \begin{pmatrix} 2 & 5 & 3 \\ 8 & 6 & 4 \\ 3 & 1 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}.$$

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 $R_2 \leftarrow 6R_1 - R_2$, $R_3 \leftarrow 5R_1 - R_3$ and $C_1 \leftarrow 3C_1 - C_2$. Then out 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:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -22 \end{pmatrix}.$$

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 $m - m$ last columns, which will all be zero columns.

**Example 19.4.** Let $M$ be the abelian group with generators $m_1, m_2, m_3$ and relations $8m_1 + 4m_2 + 8m_3 = 0$, $4m_1 + 8m_2 + 4m_3 = 0$. 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 la 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 $12m_2 = 0$ and $4(m_1 + 2m_2 + m_3) = 0$. 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 $4(m_1 + 2m_2 + m_3) = 0$ and $12m_2 = 0$. 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

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

**Example 19.5.** 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 $F_1 \leftrightarrow F_3$ and then $F_2 \leftarrow F_1 + F_2$ 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 $F_2 \leftarrow F_2 + F_3$, $C_3 \leftarrow C_3 - 5C_2$, $C_3 \leftarrow C_2$, $F_3 \leftarrow F_3 - 11F_2$ 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 $M/K \simeq \mathbb{Z} \times (\mathbb{Z}/2)^2 \times (\mathbb{Z}/44)$.

**Example 19.6.** 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 $z \in \mathbb{Z}$.

**Exercise 19.7.** Solve $AX = b$ in $\mathbb{Z}$ for $A = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} 5 \\ 1 \\ 7 \end{pmatrix}$.

**Exercise 19.8.** Prove that $\mathbb{Z}^3/\langle (6,6,4), (6,12,8) \rangle \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/6$.

**Exercise 19.9.** 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.

**Exercise 19.10.** Compute the Smith's normal form of $\begin{pmatrix} 1+i & 2-i \\ 3 & 5i \end{pmatrix} \in M_2(\mathbb{Z}[i])$.

**Exercise 19.11.** Compute the Smith's normal form of

$$\begin{pmatrix} 7 & X & 0 & -X \\ 0 & X-3 & 0 & 3 \\ 0 & 0 & X-4 & 0 \\ X-6 & -1 & 0 & X+1 \end{pmatrix} \in \mathbb{Q}[X].$$

**Exercise 19.12.** 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

**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.

**2.21** Let $f : \mathbb{Z}/6 \to \mathbb{Z}/15$ 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 $\mathbb{Z}/15$.

**2.24** 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

$$(x + I)\,((y + I) + (z + I)) = (x + I)(y + I) + (x + I)(z + I)$$

for all $x, y, z \in R$. The right distributivity is similar:

$$((x + I) + (y + I))\,(z + I) = (x + I)(z + I) + (y + I)(z + I)$$

for all $x, y, z \in R$. Let us prove the associativity of the multiplication:

$$\begin{aligned}(x+I)\,((y+I)(z+I)) &= (x+I)(yz+I)\\ &= x(yz)+I\\ &= (xy)z+I\\ &= (xy+I)(z+I)\\ &= ((x+I)(y+I))\,(z+I).\end{aligned}$$

Finally, let us see why $1+I$ is the neutral element of the multiplication:

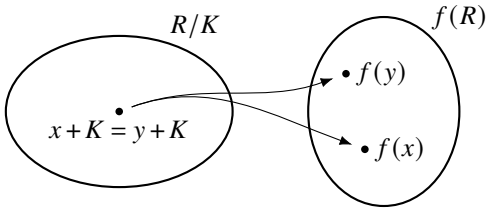
$$(x+I)(1+I) = x1+I = x+I = 1x+I = (1+I)(x+I)$$

for all $x \in R$.

**2.27** 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 $\varphi$ 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:

$$\begin{aligned}x+K = y+K &\implies x-y \in K = \ker f\\ &\implies f(x)-f(y) = f(x-y) = 0\\ &\implies f(x) = f(y).\end{aligned}$$

Now we need to prove that $\varphi$ 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 $\varphi$ is a ring homomorphism, let $x, y \in R$. Then

$$\begin{aligned}\varphi((x+K)+(y+K)) &= \varphi(x+y+K)\\ &= f(x+y)\\ &= f(x)+f(y)\\ &= \varphi(x+K)+\varphi(y+K).\end{aligned}$$

and

$$\begin{aligned}\varphi((x+K)(y+K)) &= \varphi(xy+K)\\ &= f(xy)\\ &= f(x)f(y)\\ &= \varphi(x+K)\varphi(y+K)\end{aligned}$$

because $f$ is a ring homomorphism.

The map $\varphi$ is clearly surjective, as if $y\ inf(R)$, then $y = f(x)$ for some $x \in R$. Then $\varphi(x+K) = f(x) = y$.

Finally, we show that $\varphi$ is injective:

$$\begin{aligned}\varphi(x+K) = \varphi(y+K) &\implies f(x) = f(y)\\ &\implies x - y \in K = \ker f\\ &\implies x + K = y + K.\end{aligned}$$

**2.36** Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}[i] \xrightarrow{\pi} \mathbb{Z}[i]/(1+3i)$, where $\pi$ denotes the canonical map. We claim that $\varphi$ 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 $\varphi$ is a ring homomorphism, as it is the composition of ring homomorphisms.

We now show that $\ker\varphi = 10\mathbb{Z}$:

$$\begin{aligned}m \in \ker\varphi &\iff \varphi(m) + m \in (1+3i)\\ &\iff m = (1+3i)(x+iy) \text{ for some } x, y \in \mathbb{Z}\\ &\iff m = 10x \text{ for some } x \in \mathbb{Z}\\ &\iff m \in 10\mathbb{Z}.\end{aligned}$$

Finally, to see that $\varphi$ 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 $3 - i = -i(1+3i)$.

**2.37** 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.

**3.2** 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.

**3.4** 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, $a = (xa)a \in IJ$.

**5.22** 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 $k \in \mathbb{Z}_{>0}$.

**5.38** 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 $a$.

**5.39**

**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 $\mathbb{Z}[X]$.

**5.40** 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 $k = s$ 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 5.39 that both $g_i$ and $h_i$ are primitive. By Exercise 5.38, $a_i$ (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 $\mathbb{Z}[X]$.

**5.46** Since $p \equiv 1 \bmod 4$, $p$ is not prime in $\mathbb{Z}[i]$ (see Theorem 5.43). Thus $p = \alpha\beta$ for some $\alpha, \beta \notin \mathcal{U}(\mathbb{Z}[i])$. Hence $p^2 = N(p) = N(\alpha)N(\beta)$. Since $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, $N(\alpha) = N(\beta) = p$. Therefore $\alpha\overline{\alpha} = N(\alpha) = p$.

**5.47** We claim that (up to units) the irreducible elements of $\mathbb{Z}[i]$ are $1+i$, $a+bi$, where $a, b \in Z$ and $a^2 + b^2 = p$ with $p$ a prime number such that $p \equiv 1 \bmod 4$, and a prime number $p$ with $p \equiv 3 \bmod 4$.

Let $\alpha \in \mathbb{Z}[i]$ be irreducible. Then $\alpha$ 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

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Thus $N(\alpha) \in \{p, p^2\}$, as $N(\alpha) \neq 1$ because $\alpha \notin \mathcal{U}(\mathbb{Z}[i])$.

Assume first that $N(\alpha) = p$. Write $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. If $p = 2$, then

$$\alpha \in \{1+i, 1-i, -1+i, -1-i\}.$$

If $p \equiv 1 \bmod 4$, then $p = N(\alpha) = a^2 + b^2$. If $p \equiv 3 \bmod 4$, then $p = N(\alpha) = a^2 + b^2$, a contradiction to Theorem 5.43.

Assume now that $N(\alpha) = p^2$. Then $\beta \in \mathcal{U}(\mathbb{Z}[i])$. If $p = 2$, then $\alpha$ is not irreducible, as $\alpha \in \{2, -2, 2i, -2i\}$. If $p \equiv 3 \bmod 4$, then $\alpha \in \{p, -p, pi, -pi\}$. If $p \equiv 1 \bmod 4$, then $p = \gamma\overline{\gamma}$ for some irreducible $\gamma$ such that $N(\gamma) = p$ (see Exercise 5.46). Thus $\alpha$ is not irreducible, a contradiction.

**6.13** 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 $J = R$.

**6.18** 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.

**6.19**

**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 6.13).

**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 $J = R$.

.

**6.28** 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.

**6.29** 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

$$\{x_i e_j : i \in I, 1 \leq j \leq n\}$$

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.

**6.30** Let $G$ be a group such that $\mathrm{Aut}(G) = \{\mathrm{id}\}$. 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 $g \in G$. º Let $B$ be a basis of $G$ over $\mathbb{Z}/2$. If $|I| \geq 2$, 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.

**7.5** One approach to solve this exercise requires the following fact: $p$ is a prime and $1 \leq k \leq p^n - 1$, 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 $\gcd(p,k) \neq 1$, 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 $m - \alpha \geq 1$. Thus $p$ divides $m\binom{p^n}{k}$ and hence $p$ divides $\binom{p^n}{k}$ because $p$ and $m$ are coprime.

**8.5** Let $G = \langle g : g^3 = 1\rangle$ be the cyclic group of order three and $\omega$ 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 $\varphi$ is a bijective.

**9.19** 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 $\psi$ 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 $w = 0$.

**9.25** 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 $\rho$ is not irreducible, as since $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ an eigenvector of $\rho_m$ for all $m \in \mathbb{Z}$, the subspace $\mathbb{C}v_1$ is an invariant subspace of $\mathbb{C}^2$. To prove that $\rho$ is indecomposable, let us assume that it is not, that is $\rho$ 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.

**14.12** 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.

**14.27**

**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 thu $N = M$. 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 $(1, -1)$.

**15.11** Take for example the $\mathbb{Z}$-module $\cup_{k \geq 1} \mathbb{Z}/(p^k)$.

**19.7** The Smith's normal form yields

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ -1 & -2 & 1 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix}, \quad S = PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The solution of the integer linear system is then $X = \begin{pmatrix} 1+t \\ t \\ -5+2t \end{pmatrix}$ for $t \in \mathbb{Z}$.

**19.8** 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 $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

**19.9** Let $A = \begin{pmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{pmatrix}$. The Smith's normal form of $A$ is $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 0 \end{pmatrix}$. Thus the abelian group is isomorphic to $\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/\mathbb{Z}/\times\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/4$.

**19.10** The Smith's normal form is $\begin{pmatrix} 1 & 0 \\ 0 & -11+8i \end{pmatrix}$.

**19.11** 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 $f(X) = X^4 - 3X^3 - 11X^2 + 7X + 84$.

**19.12** 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 $A = (a_{ij}) \in M_n(\mathbb{Z})$ 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. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
5. G. Gonthier, A. Asperti, J. Avigad, and et al. A machine-checked proof of the odd order theorem. In *Interactive theorem proving*, volume 7998 of *Lecture Notes in Comput. Sci.*, pages 163–179. Springer, Heidelberg, 2013.
6. T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
7. S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.
8. J. R. Munkres. *Elements of algebraic topology*. Addison-Wesley Publishing Company, Menlo Park, CA, 1984.
9. 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.
10. B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.
11. N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.
12. S. Wagon. Editor's corner: the Euclidean algorithm strikes again. *Amer. Math. Monthly*, 97(2):125–129, 1990.
13. J. C. Wilson. A principal ideal ring that is not a Euclidean ring. *Math. Mag.*, 46:34–38, 1973.
14. 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