Leandro Vendramin

Rings and modules

Notes

Thursday 9th September, 2021

Versión compilada el Thursday 9th September, 2021 a las 16:37.

Leandro Vendramin
Brussels, Belgium

Contents

Part I
Rings

Chapter 1
Rings and ideals

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 $x1_R = 1_R x = x$ for all $x \in R$.

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

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.

Example 1.4. The set

$$\mathbb{R}[X] = \left\{ \sum_{i=0}^{n} a_i X^i : n \in \mathbb{N}_0, a_1, \ldots, a_n \in \mathbb{R} \right\}$$

of real polynomials in one variable is a commutative ring with the usual operations.

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 $\mathrm{End}(A)$ is a ring with

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

Let R be a ring. Some facts:

1) $x0 = 0x = x$ for all $x \in R$.
2) $x(-y) = -xy$ for all $x, y \in R$.
3) If $1 = 0$, then $|R| = 1$.

Example 1.6. 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 $ij = i(ij) = -j$. This is the ring of real **quaternions**.

Example 1.7. Let $n \geq 2$. The abelian group $\mathbb{Z}/n = \{0,1,\ldots,n\}$ of integers modulo n is a ring with the usual multiplication modulo n.

Example 1.8. 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.

Definition 1.9. 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 $xy \in S$.

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

Example 1.10. $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. This is known as the ring of **Gauss integers**.

Example 1.11. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$.

Example 1.12. 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 1.13.

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

Definition 1.15. A **division ring** is a ring R such that $\mathscr{U}(R) = R \setminus \{0\}$.

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

Definition 1.16. A **field** is a commutative division ring with $1 \neq 0$.

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

Exercise 1.17. 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 $x + y\sqrt[3]{2} + z\sqrt[3]{4}$?

Definition 1.18. 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 1.19. 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 1.20. 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 1.21. Let R be a ring.

1) If $\{I_\alpha : \alpha\}$ 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 1.22. 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

$$(X) = \left\{ \sum_{i=1}^{m} r_i x_i s_i : m \in \mathbb{N}_0, r_1, \ldots, r_m, s_1, \ldots, s_m \in R \right\},$$

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

xca:ideals_Z **Exercise 1.23.** Prove that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 0$.

Exercise 1.24. Let $n \geq 2$. Find the ideals of $\mathbb{Z}/n$.

Exercise 1.25. Find the ideals of $\mathbb{R}$.

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

Definition 1.26. 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 1.23.

Exercise 1.27. 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 1.28. Let R be a ring and $x \in R$. Prove that $x \in \mathscr{U}(R)$ if and only if $(x) = R$.

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

Definition 1.29. 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 1.30. 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 1.31. 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 1.32. Let R be a ring. The map $\mathbb{Z} \to R$, $k \mapsto k1$, is a ring homomorphism.

Example 1.33. 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, $\ker f = \{0\}$ 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 1.34. 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 1.35. 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 1.36. There is no ring homomorphism $\mathbb{Z}/6 \to \mathbb{Z}/15$. Why?

Exercise 1.37. 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.

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

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

and the **canonical map** $R \to R/I$, $x \mapsto x+I$, is a surjective group homomorphism. Recall that R/I is the set of cosets $x+I$, where $x+I = y+I$ if and only if $x-y \in I$. 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 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 in such a way that the canonical map $R \to R/I$ is a surjective ring homomorphis. 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 1.38. *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 the multiplication is well-defined. The rest of the proof is left as an exercise.

Example 1.39. Let

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

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 1.40. 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 $a,b \in R$. 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.

An **isomorphism** between the rings R and S is a bijective ring homomorphism $R \to S$. Notation: $R \simeq S$ if and only if there exists an isomorphism $R \to S$. As it happens in the case of groups, to undertand quotient rings one has the first isomorphism theorem.

Theorem 1.41 (first isomorphism theorem). *If $f\colon R \to S$ is a ring homomorphism, then $R/\ker f \simeq f(R)$.*

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

Example 1.42. 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 the usual multiplication rule of the field of complex numbers.

Exercise 1.43. 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 1.44. 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 1.45. Are the rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ isomorphic?

Exercise 1.46. Let R be the ring of continuos maps $[0,2] \to \mathbb{R}$. Prove that the set $I = \{f \in R : f(1) = 0\}$ is an ideal of R and that $R/I \simeq \mathbb{R}$.

Exercise 1.47. 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 $M_n(R)/M_n(I) \simeq M_n(R/I)$.

```
xca:Z[sqrt10]/(2,sqrt10)
```

Exercise 1.48. Let $R = \mathbb{Z}[\sqrt{10}]$ and $I = (2, \sqrt{10})$. Prove that $R/I \simeq \mathbb{Z}/2$.

xca:Z[i]/(1+3i)

Exercise 1.49. Prove that $\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/10$.

Exercise 1.50. Prove that there is no ideal I of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

Exercise 1.51. 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 important result.

Theorem 1.52 (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.*

Sketch of the proof. Let I be an ideal of R contaning $\ker f$ 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 $R/I \simeq S/J$. □

Chapter 2
Chinese remainder theorem

Note that 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.

Definition 2.1. 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

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

If I and J are ideals of R, then

$$IJ=\left\{\sum_{i=1}^{m} u_i v_i : m\in\mathbb{N}_0, u_1,\ldots,u_m\in I, v_1,\ldots,v_m\in J\right\}$$

is an ideal of R. Note that $IJ\subseteq I\cap J$. The 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 2.2. *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 $v\in J$, $x=x1=x(u+v)=xu+xv\in IJ$. □

Theorem 2.3 (chinese remainder theorem). *Let R be a commutative ring and I and J be coprime ideals. 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 $x \equiv v \bmod J$. □

Corollary 2.4. *Let R be a commutative ring. If I and J are coprime ideals of R, then $R/(I \cap J) \simeq R/I \times R/J$.*

Proof. Let $\pi_I \colon R \to R/$ and $\pi_J \colon R \to R/J$ 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 an injective ring homomorphism with $\ker \varphi = I \cap J$. The chinese remainder theorem implies that φ 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 φ. Now $R/(I \cap J) \simeq R/I \times R/J$ by the first isomorphism theorem. □

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

$$I_1 \cdots I_n = \left\{ \sum_{i=1}^{m} u_{i_1} \cdots u_{i_n} : m \in \mathbb{N}_0, u_{i_1}, \ldots, u_{i_n} \in I_{i_j} \right\}$$

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

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

Exercise 2.5 (Lagrange's interpolation theorem). The chinese remainder theorem roves the following well-known result. Let $x_1, \ldots, x_k \in \mathbb{R}$ be such that $x_i \neq x_j$ whenever $i \neq j$ and $y_1, \ldots, y_k \in \mathbb{R}$. Then there exists $f(X) \in \mathbb{R}[X]$ such that

$$\begin{cases} f(X) \equiv y_1 \bmod (X - x_1), \\ f(X) \equiv y_2 \bmod (X - x_2), \\ \quad \vdots \\ f(X) \equiv y_k \bmod (X - x_k). \end{cases}$$

The solution $f(X)$ is unique modulo $(X-x_1)(X-x_2)\cdots(X-x_n)$.

xca:gather_people

Exercise 2.6. Let us gather people in the following way. When I count by three, there are two persons left. When I count by four, there is one person left over and when I count by five there is one missing. How many persons are there?

xca:no_solution

Exercise 2.7. Prove that

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

does not have solution.

xca:consecutive

Exercise 2.8. 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.

xca:perfect_square

Exercise 2.9. Prove that for each $n \in \mathbb{N}$ there are n consecutive integers such that each integer is divisible by a perfect square $\neq 1$.

Chapter 3
Noetherian rings

In this chapter we will work with commutative rings.

Definition 3.1. 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 $m \in \mathbb{N}$ and all $n \geq m$.

The ring $\mathbb{Z}$ of integers is noetherian.

Example 3.2. Let $R = \{f\colon\ [0,1] \to \mathbb{R}\}$ with

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x), \quad f,g \in R, x \in [0,1].$$

For $n \in \mathbb{N}$ 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 stabilizes. Thus R is not noetherian.

Definition 3.3. 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.

The zero ideal is always finitely generated.

Proposition 3.4. *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 $\{0\} \subsetneq I_1 \subsetneq I$. 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, sayç $I = (x_1, \ldots, x_n)$. We may assume that $x_j \in I_{i_j}$ for all j. Let $N = \max\{j_1, \ldots, j_n\}$ and $n \geq N$. Then $I_N \subseteq I \subseteq I_N$ and therefore the seuqence stabilizes. □

Exercise 3.5. Let $R = \mathbb{C}[X_1, X_2, \cdots]$ be the ring of polynomial in an infinite number of commuting variables. Prove that the ideal $I = (X_1, X_2, \ldots)$ of polynomials with zero contant term is not finitely generated.

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

Proposition 3.6. *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

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

and hence J is finitely generated. □

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

Exercise 3.7. Prove that $\mathbb{R}[X]$ is noetherian.

Theorem 3.8 (Hilbert). *Let R be a commutative ring. If R is noetherian ring, then $R[X]$ is noetherian.*

Proof. We need to 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. For $i > 1$ let $f_i(X) \in I$ be of minimal degree 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). For each i 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 lowest degree terms. Note that $a_i \neq 0$. 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 J is finitely generated, say $J = (a_1, \dots, a_m)$ for some $m \in \mathbb{N}$. There exist $u_1, \dots, u_m \in R$ such that

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

Let

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

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 $\deg(g(X)) < n_{m+1}$. Since $f_{m+1}(X) \notin (f_1(X) \dots, f_n(X))$,

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

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

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

Example 3.9. 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 3.10. The ring $\mathbb{Z}[X,X^{-1}]$ is noetherian, as $\mathbb{Z}[X,X^{-1}] \simeq \mathbb{Z}[X,Y]/(XY-1)$.

Exercise 3.11. Prove that $R[[X]]$ is noetherian if R is noetherian.

Exercise 3.12. Let $f\colon R \to R$ be surjective ring homomorphism. Prove that f is an isomorphism if R is noetherian.

Chapter 4
Factorization

Definition 4.1. A commutative ring R is said to be an **integral domain** if $xy = 0$ implies $x = 0$ or $y = 0$.

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.

Definition 4.2. Let R be an integral domain and $x, y \in R$. Then x **divides** y if $y = xz$ for some $x \in R$. 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 4.3. Let R be an integral domain and $x, y \in R$. Then x and y are **associate** in R if $x = yu$ for some $u \in \mathscr{U}(R)$.

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

Example 4.4. The integers 2 and -2 are associate in $\mathbb{Z}$.

Example 4.5. 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 4.6. 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 4.7. Let R be an integral domain and $x \in R \setminus \{0\}$. Then x is **irreducible** if and only if $x \notin \mathscr{U}(R)$ and $x = ab$ with $a, b \in R$ implies that $a \in \mathscr{U}(R)$ or $b \in \mathscr{U}(R)$.

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

Example 4.8. Let $R = \mathbb{R}[X]$ and $f(X) \in R \setminus \{0\}$. Then $f(X)$ 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.

Definition 4.9. Let R be an integral domain and $p \in R \setminus \{0\}$. Then p is **prime** if $p \notin \mathscr{U}(R)$ and $yz \in (p)$ implies that $y \in (p)$ or $z \in (p)$.

In $\mathbb{Z}$ primes and irreducible coincide. This does not happend in full generality. However, the following result holds.

Proposition 4.10. *Let R be an integral domain and $x \in R$. If x is prime, then x is irreducible.*

Proof. Let p be a prime. Then $p \neq 0$ and $p \notin \mathscr{U}(R)$. Let x be such that $x \mid p$. Then $p = xy$ for some $y \in R$. This means $xy \in (p)$, so $x \in (p)$ or $y \in (p)$ because p is prime. If $x \in (p)$, then $x = pz$ for some $z \in R$ and hence

$$p = xy = (pz)y.$$

Since $p - pzy = p(1 - zy)$ and R is an integral domain, it follows that $1 - zy = 0$. Thus $y \in \mathscr{U}(R)$. Similarly, if $y \in (p)$, then $x \in \mathscr{U}(R)$. □

To show that there rings where some irreducibles are not prime, we need the following lemma.

Lemma 4.11. *Let $N \in \mathbb{Z}$ be a square-free integer and $R = \mathbb{Z}[\sqrt{N}]$. The map*

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

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) *$\alpha \in \mathscr{U}(\mathbb{Z}[\sqrt{N}])$ if and only if $N(\alpha) = 1$.*
4) *If $N(\alpha)$ is prime in $\mathbb{Z}$, then α is irreducible in R.*

Proof. The first three items are left as an exercises. Let us prove 4). If $\alpha = \beta\gamma$ for some $\beta, \gamma \in R$, then $N(\alpha) = N(\beta)N(\gamma)$. Since $N(\alpha)$ is a prime number, it follows that $N(\alpha) = 1$ or $N()\beta) = 1$. Thus $\beta \in \mathscr{U}(R)$ or $\gamma \in \mathscr{U}(R)$. □

Example 4.12. Let $R = \mathbb{Z}[i]$.

1) $\mathscr{U}(R) = \{-1, 1, i, -i\}$.
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 $\alpha \in \mathscr{U}(R)$ by the lemma. If $N(\alpha) = 9$, then $N(\beta) = 1$ and hence $\beta \in \mathscr{U}(R)$ 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 $1 + i \notin \mathscr{U}(R)$ and $1 - i \notin \mathscr{U}(R)$.

Exercise 4.13. 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.

Example 4.14. 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 $4 = N(x) = N(\alpha)N(\beta)$. Write $\alpha = a+b\sqrt{-3}$ for some $a, b \in \mathbb{Z}$. Then $N(\alpha) = a^2+3b^2 \neq 2$. If $N(\alpha) = 2$, then $a^2+3b^2 = 2$ and then a and b both have the same parity.
If both a and b are even, say $a = 2k$ and $b = 2l$ for some $k, l \in \mathbb{Z}$, then

$$2 = a^2+3b^2 = 4k^2+12l^2$$

is divisible by 4, a contradiction.
If both a and b are odd, say $a = 2k+1$ and $b = 2l+1$ for some $k, l \in \mathbb{Z}$, then

$$2 = a^2+3b^2 = 4k^2+4k+12l^2+12l+4$$

is divisible by 4, a contradiction.
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 4.15. Let $R = \mathbb{Z}[\sqrt{5}]$. Prove that $1+\sqrt{5}$ is irreducible and not prime in R.

Definition 4.16. Let R be an integral domain. Then R is **principal** (or a principal domain) if every ideal of R is principal.

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

Example 4.17. 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

$$0 = \deg(1) = \deg(2f(X)+Xg(X)) = \deg(f(X))+\deg(g(X))+1 > 0,$$

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.

Example 4.18. 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 $I = (\alpha)$. 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 $a^2+5b^2 = N(\alpha) = 1$ and hence $\alpha \in \mathscr{U}(R)$. Therefore $I = R$, a contradiction.

Sometimes primes and irreducibles coincide.

Proposition 4.19. *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, $a \in \mathscr{U}(R)$ or $b \in \mathscr{U}(R)$. If $a \in \mathscr{U}(R)$, 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 $b \in \mathscr{U}(R)$, 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 4.20. 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 4.21. Let R be an integral domain. We say that R is an **euclidean domain** if there exists a map $\varphi\colon R \setminus \{0\} \to \mathbb{N}_0$ 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 4.22. $\mathbb{Z}$ is an euclidean domain with $\varphi(x) = |x|$.

Do we have uniqueness in the previous example?

Example 4.23. $\mathbb{R}[X]$ is an euclidean domain with $\varphi(f(X)) = \deg(f(X))$.

The previous examples shows why in the definition of an euclidean domain we consider $\varphi\colon R \setminus \{0\} \to \mathbb{N}_0$.

Example 4.24. Let $R = \mathbb{Z}[i]$. Then R is an euclidean domain with $\varphi(\alpha) = N(\alpha)$. Let $\alpha = a+ib$ and $\beta = c+id \neq 0$. Then

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

for some $r,s \in \mathbb{Z}$. Let $m,n \in \mathbb{Z}$ be such that $|r-m| \leq 1/2$ and $|s-n| \leq 1/2$. If $\delta = m+in$ and $\gamma = \alpha - \beta\delta$, then $\gamma \in R$, $\delta \in R$ and $\alpha = \beta\delta + \gamma$. If $\gamma \neq 0$, then

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

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

Example 4.25. Let $R = \mathbb{Z}[i]$ and $\alpha = -1+i$ and $\beta = 1+2i$. Let $I = (\beta)$ be the ideal of R generated by β. First note that

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

This allows us to draw the lattice of elements of I, that is the lattice formed by the multiples of β, see Figure **??**. Since $\alpha - \gamma \in I = (\beta)$, there are at most four possibilites 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 $-1+3 = \beta_2 i = \beta(1+i)$, then $\gamma = 2i$ and

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

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

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

fig:lattice

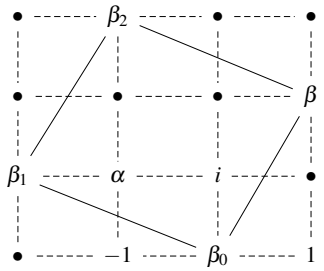

Figure 4.1

Proposition 4.26. *Let R be an 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 4.27. Since $\mathbb{Z}[i]$ is euclidean, then it is principal.

Example 4.28. The rings $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}\left[\sqrt{-3}\right]$ are not principal. 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...

Definition 4.29. 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 has factorization. This fact will be proved in the proof of the following theorem. However, not all these rings with be euclidean domains.

Theorem 4.30. *Let R be a principal domain. Then R is a unique factorization domain.*

Proof. We divide the proof in three steps.

Claim. R is noetherian.

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 $n \in \mathbb{N}$, it follows that $(a_k) \subseteq I = (x) \subseteq (a_n)$ for all $k \in \mathbb{N}$.

Claim. R admits factorizations.

Let $x \in R \setminus \{0\}$ be such that $x \notin \mathscr{U}(R)$. If x is irreducible, there is nothing to prove. If not, $x = x_1 x_2$ with $x_1 \notin \mathscr{U}(R)$ and $x_2 \notin \mathscr{U}(R)$. 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} $\mathscr{U}(R)$ and $x_{12} \notin \mathscr{U}(R)$. 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 $x = c_1 \cdots c_n = d_1 \cdots d_m$. We may assume that $n \leq m$. We proceed by induction on m. If $m = 1$, then $n = 1$ and $c_1 = d_1$. If $m > 1$, then, since c_1 is prime and $c_1 \mid d_1 \cdots d_m$, it follows that $c_1 \mid d_j$ for some j, say $c_1 \mid d_1$ (here is precisely where the permutation σ appears). Since d_1 is irreducible, c_1 and d_1 are associate, that is $c_1 = ud_1$ for some $u \in \mathscr{U}(R)$. 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 by 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 4.31. The ring $\mathbb{Z}[i]$ is a unique factorization domain.

Example 4.32. 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.

We conclude the chapter with the following theorem.

Theorem 4.33 (Fermat). *Let $p \in \mathbb{Z}$ 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, $/Z/p$ 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 $(a-i)(a+i)$. 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 $a+bi \notin \mathscr{U}(\mathbb{Z}[i])$ and $c+di \notin \mathscr{U}(\mathbb{Z}[i])$, 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 $a^2 + b^2 \equiv 2 \bmod 4$. □

Chapter 5
Zorn's lemma

Definition 5.1. 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 5.2. Let R be a poset and $r,s \in R$. Then r and s are **comparable** if either $r < s$ or $s < r$.

Example 5.3. 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 5.4. Let R be a poset and $r \in R$. Then r is **maximal** in R if such that $r \leq t$ implies $r = t$.

Example 5.5. $\mathbb{Z}$ has no maximal elements.

Example 5.6. 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 5.7. 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 $s \in S$.

Example 5.8. Let $S = \{6\mathbb{Z}, 12\mathbb{Z}, 24\mathbb{Z}\}$ be a subset of the set of subgroups of $\mathbb{Z}$. Then $6\mathbb{Z} = 6\mathbb{Z} \cap 12\mathbb{Z} \cap 24\mathbb{Z}$ is an upper bound of S.

Definition 5.9. 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, but it is logically equivalent to a more intuitively 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 that a lemma. The reason for calling Zorn's lemma a lemma rather than an axiom is purely historical.

Definition 5.10. 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 5.11. Let R be a commutative ring. Prove that R is a field if and only if $\{0\}$ is a maximal ideal of R.

Exercise 5.12. 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.

The following application of Zorn's lemma uses the identity of a ring.

Theorem 5.13. *Let R be a ring. Each proper ideal I of R is contained in a maximal ideal. In particular, all rings have maximal ideals.*

Proof. Let $X = \{J \subseteq R : J \text{ is an ideal of } R \text{ such that } I \subseteq J \subsetneq R\}$. Since $I \in X$, it follows that X is non-empty. Moreover, X is a poset with respect to the inclusion. If C is a chain in X, 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 $M \in X$ maximal. We claim that M is a maximal ideal of R. The definition of X implies that M is a proper ideal of R. If M_1 is an 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 $M = M_1$. □

Exercise 5.14. 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 5.15. Let R be a principal domain and $p \in R$. Then p is irreducible if and only if (p) is maximal.

Example 5.16. 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.

Exercise 5.17. Let R be a commutative ring and I be an ideal of R. Then I is maximal if and only if R/I is a field.

Example 5.18. 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 follow that $(f(X))$ is a maximal ideal. Thus R/I is a field.

Exercise 5.19. Compute the maximal ideals of $\mathbb{Z}/n$.

Exercise 5.20. 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 $1 - xy \in \mathscr{U}(R)$ for all $y \in R$. The ideal $J(R)$ is proper and it is known as the **Jacobson radical** of R.

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

Exercise 5.21. Prove that every non-zero vector space has a basis.

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

Exercise 5.22. Prove that there exists a group homomorphism $f\colon \mathbb{R} \to \mathbb{R}$ that is not of the form $f(x) = \lambda x$ for some $\lambda \in \mathbb{R}$.

Exercise 5.23. Prove that the abelian groups $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic.

Exercise 5.24. Prove that if G is a group such that $|G| > 2$, then $|\operatorname{Aut}(G)| > 1$.

Chapter 6
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

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

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

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

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

Definition 6.1. Let A be a ring. Then A is an algebra (over the field K) if A is a vector space and the map $K \to Z(A)$, $k \mapsto k1_A$, is an injective ring homomorphism.

Thus $K[G]$ is an algebra, as it is ring that contains K in its center (or more precisely, the map $K \to Z(K[G])$, $k \mapsto k1$, is an injective ring homomorphism. Other examples of algebras are the polynomial rings $K[X]$ and $K[X,Y]$ and matrix rings $M_n(K)$.

Example 6.2. 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. Moreove, $K[G]$ is a vector space of dimension $\dim K[G] = |G|$.

Example 6.3. 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 $\mathbb{C}[C_n] \simeq \mathbb{C}[X]/(X^n - 1)$ for $n \geq 2$.

Example 6.4. Let K be a field and $G = \{1, g\} \simeq C_2$ be the cyclic group of order two. The product of $K[G]$ is

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

If $K = \mathbb{C}$, then the map $K[G] \to K \times K$, $a1 + bg \mapsto (a+b, a-b)$, is a linear isomorphism of rings.

If $K = \mathbb{Z}/2$, then 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.

Exercise 6.5. Prove that $\mathbb{R}[C_3] \simeq \mathbb{R} \times \mathbb{C}$.

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

Example 6.6. Let $\mathbb{D}_3 = \langle r, s : r^3 = s^2 = 1, srs^{-1} = r^{-1} \rangle$ be the dihedral group of six elements. We claim that

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

Let ω be a primitive 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.

Part II
Representations

Chapter 7
Group representations

Definition 7.1. 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 V will be the dimension of V. Note that if $\dim V = n$, fixing a basis of V we get a **matrix representation** $\rho\colon G \to \mathbf{GL}(V) \simeq \mathbf{GL}_n(V)$ of G.

Example 7.2. 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

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

Thus $\rho_{xy}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ and $\rho_{xy}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. From this the claim follows.

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 7.3. 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.

Example 7.4.

Example 7.5.

Proposition 7.6. *Let G be a finite group and $\rho\colon G \to \mathbf{GL}(V)$ be a representation. Then each ρ_g is diagonalizable.*

Proof. Let $n = \dim V$. Fix a basis of the finite-dimensional vector space V and consider a matrix representation $\rho\colon G \to \mathbf{GL}_n(V)$. Since g is finite, $g^m = 1$ for some $m \in \mathbb{N}$. This means that ρ_g is a root of $X^m - 1 \in \mathbb{C}[X]$. Since the roots of the polynomial $X^m - 1$ are all different and $X^m - 1$ factorizes linearly on $\mathbb{C}[X]$, it follows that the minimal polynomial of ρ_g also factorizes linearly in $\mathbb{C}[X]$. Hence ρ_g is diagonalizable. □

Definition 7.7. 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 G-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, i.e. $\psi_g T = T\rho_g$ for all $g \in G$.

Definition 7.8. The representations $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are **equivalent** if there exists a bijective G-invariant map $T\colon V \to W$.

Example 7.9. 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 7.10. Let $\rho\colon G \to \mathbf{GL}(V)$ a representation. A subspace W of V is said to be G-invariant (with respect to ρ) 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 G-invariant, then the map $\rho|_W\colon G \to \mathbf{GL}(W)$, $g \mapsto (\rho_g)|_W$, is a representation.

Definition 7.11. Let $\rho\colon G \to \mathbf{GL}(V)$ a representation. A **subrepresentation** of ρ is a representation of the form $\rho|_W\colon G \to \mathbf{GL}(W)$ for some G-invariant subspace W of V.

Example 7.12. Let $G = \langle g : g^3 = 1 \rangle$ be the cyclic group of order three and

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

The subspace

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

is a G-invariant subspace of $\mathbb{R}^3$.

Definition 7.13. A representation $\rho \colon G \to \mathbf{GL}(V)$ is **irreducible** if $\{0\}$ and V are the only G-invariant subspaces of V.

Clearly, degree-one representations are irreducible.

Example 7.14. Let $G = \langle g : g^3 = 1 \rangle$ be the cyclic group of order three and

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

We claim that the G-invariant subspace

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

is irreducible. Let S be a non-zero G-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 $S = W$.

Exercise 7.15. Let $\rho \colon G \to \mathbf{GL}(V)$ be a degree-two representation. Prove that ρ is irreducible if and only if there is no common eigenvector for the ρ_g, $g \in G$.

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

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

is irreducible.

Definition 7.16. A representation $\rho\colon G \to \mathbf{GL}(V)$ is **completely irreducible** if V can be decomposed as $V = V_1 \oplus \cdots \oplus V_n$, where each V_i is a G-invariant subspace of V and each $\rho|_{V_i}$ is irreducible.

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 7.17. 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 $v,w \in V$.

Definition 7.18. A representation $\rho\colon G \to \mathbf{GL}(V)$ is **decomposable** if V can be decomposed as $V = S \otimes T$ where S and T are non-zero G-invariant subspaces of V.

Exercise 7.19. Let $\rho\colon G \to \mathbf{GL}(V)$ be a unitary representation. Prove that ρ is either irreducible or decomposable.

Example 7.20. 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.

Proposition 7.21 (Weyl's trick). *Every representation of a finite group is equivalent to a unitary representation.*

Proof. Let $\rho\colon G \to \mathbf{GL}(V)$ and $V \times V \to \mathbb{C}$, $(v,w) \mapsto \langle v,w\rangle_0$ be an inner product on V. A straighforward 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 ρ is unitary. □

Weyl's trick has several interesting corollaries. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation of a finite group G. Then 1) every non-zero representation is either irreducible or decomposable, and 2) every ρ_g is diagonalizable (as unitary operators are diagonalizable).

Exercise 7.22. If G is an infinite group it is not longer true that every non-zero representation is either irreducible or decomposable. Find an example.

Recall that we only consider finite-dimensional representations of finite groups.

Theorem 7.23 (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 $\leq n$. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation of degree $n+1$. If ρ is irreducible, we are done. If not, write $V = S \otimes T$, where S and T are non-zero G-invariant subspaces. Since $\dim S < \dim V$ and $\dim T < \dim V$, it follows from the inductive hypothesis that both S and T are completely irreducible. Thus V is completely irreducible. □

Example 7.24. Let $G = \mathbb{S}_3$ and $\rho\colon G \to \mathbf{GL}_3(\mathbb{C})$ be the representation given by

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

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

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

are irreducible G-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 7.25. Let G be a finite group. Prove that there is a bijection between degree-one representations of G and degree-one representations of $G/[G,G]$.

Part III
Modules

Chapter 8
Modules and submodules

Chapter 9
Some hints

Rings and ideals

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

1.49 Use the ring homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}[i] \xrightarrow{\pi} \mathbb{Z}[i]/(1+3i)$, where π is the canonical map.

Chapter 10
Some solutions

Rings and ideals

Chinese remainder theorem

Noetherian rings

Factorization

Zorn's lemma

References

Index