Leandro Vendramin

Rings and modules

Notes

Saturday 30th October, 2021

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 thirteen two-hours lectures.

The material is somewhat standard. Basic texts on abstract algebra are for example [1], [3] and [4]. Lang's book [5] is also a standard reference, but maybe a little bit more advanced. We based the lectures on representation theory of finite groups on [6] and [7].

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 at every stage of a mathematical career.

Thanks go to Arne van Antwerpen and Geoffrey Jassens.

This version was compiled on Saturday 30th October, 2021 at 19:01.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Rings

We will devote five lectures to basic theory of rings. The topics to cover are: 1) Basic definitions and examples, 2) ideals, homomorphisms and quotient rings, 3) Chinese remainder theorem, 4) noetherian rings and Hilbert's theorem, 5) factorization in commutative rings, 6) Fermat's theorem, and 7) Zorn's lemma and maximal 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

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

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

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

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

Let R be a ring. Some 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 1.6. 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 $ik = i(ij) = -j$. This is the ring of real **quaternions**.

Example 1.7. Let $n \geq 2$. The abelian group $\mathbb{Z}/n = \{0,1,\dots,n-1\}$ 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, $\mathscr{U}(\mathbb{Z}) = \{-1, 1\}$ and $\mathscr{U}(\mathbb{Z}/8) = \{1, 3, 5, 7\}$.

Exercise 1.15. Compute $\mathscr{U}(\mathbb{R}[X])$.

Definition 1.16. 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 1.17. 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 1.18. 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 $(X) = (x_1, \ldots, x_n)$.

xca:ideals_Z **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.

Definition 2.9. 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.

Exercise 2.10. 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 2.11. 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 2.12. 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 2.13. 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 2.14. 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 2.15. Let R be a ring. The map $\mathbb{Z} \to R$, $k \mapsto k1$, is a ring homomorphism.

Example 2.16. 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. Provide an example!

Example 2.17. 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 2.18. 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 2.19. There is no ring homomorphism $\mathbb{Z}/6 \to \mathbb{Z}/15$. Why?

Exercise 2.20. 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. Recall that R/I is the set of cosets $x+I$, where

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

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

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

How can we put a ring structure on R/I? It makes sense to define a multiplication on R/I in such a way 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 2.21. *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. As an example, we show that the left distributive property holds in R/I because it holds in R, that is

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

Example 2.22. 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 2.23 (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 the map $R/I\to f(R)$, $x+I\mapsto f(x)$, is a well-defined bijective ring homomorphism.

Example 2.24. 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 2.25. 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 2.26. 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 2.27. 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 2.28. Are the rings $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ isomorphic?

Exercise 2.29. 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 2.30. 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 2.31. 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 2.32. Prove that $\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/10$.

Exercise 2.33. Prove that there is no ideal I of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

Exercise 2.34. 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 2.35 (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 $R/I \simeq S/J$. □

§3. 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 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. 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 3.2. *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 3.3 (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 3.4. *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

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

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

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

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

xca:gather_people

Exercise 3.6. 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 3.7. Prove that

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

does not have solution.

xca:consecutive

Exercise 3.8. 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 3.9. 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

We now study noetherian rings. We will prove Hilbert's basis theorem. After that we will start our study of factorization in commutative 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 $n \geq m$.

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

Exercise 4.2. 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 $n \in \mathbb{Z}_{>0}$ 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 stabilizes. 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 $I_1 \subsetneq I_2 \subsetneq I$. 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 $I = (x_1, \dots, x_n)$. We may assume that $x_j \in I_{i_j}$ for all j. Let $N = \max\{j_1, \dots, j_n\}$. Then $x_j \in I_N$ for all $j \in \{1, \dots, n\}$ 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. 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 π 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.

Theorem 4.8 (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 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, $n_2 \geq n_1$. 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 $f_i(X) \notin (f_1(X), \dots, f_{i_2}(X))$, 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 lowest degree terms. 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 $f_{m+1}(X) \notin (f_1(X) \ldots, f_n(X))$,

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

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. 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 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 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.

Definition 5.2. 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 5.3. 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 5.4. The integers 2 and -2 are associate in $\mathbb{Z}$.

Example 5.5. 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 5.6. 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 5.7. 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 5.8. 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 $p \mid y$.

Definition 5.9. Let R be an integral domain and $p \in R \setminus \{0\}$. Then p is **prime** if $p \notin \mathscr{U}(R)$ and $p \mid xy$ implies that $p \mid x$ or $p \mid y$.

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

Proposition 5.10. *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 $p \notin \mathscr{U}(R)$. 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 $x \in \mathscr{U}(R)$. □

A square-free integer is an integer which is divisible by no perfect square other than 1.

Exercise 5.11. If N is a square-free integer, then $a + b\sqrt{N} = c + d\sqrt{N}$ if and only if $a = b$ and $c = d$.

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

Lemma 5.12. *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) $\alpha \in \mathscr{U}(\mathbb{Z}[\sqrt{N}])$ *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 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 5.13. 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 $1 - i \notin \mathscr{U}(R)$.

Lecture 4

Example 5.14. 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 5.15. 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 5.16. Let $R = \mathbb{Z}[\sqrt{5}]$. Prove that $1 + \sqrt{5}$ is irreducible and not prime in R.

Definition 5.17. Let R be an integral domain. Then R is **principal** (or a principal 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 5.18. 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.

ca:principal=>noetherian

Exercise 5.19. Let R be a principal domain. Prove that R is noetherian.

Example 5.20. 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 5.21. *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 5.22. 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 5.23. 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 5.24. $\mathbb{Z}$ is an euclidean domain with $\varphi(x)=|x|$.

Do we have uniqueness in the previous example?

Example 5.25. $\mathbb{R}[X]$ 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 $\varphi\colon R\setminus\{0\}\to\mathbb{Z}_{\geq 0}$.

Example 5.26. 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

$$\frac{\alpha}{\beta}=\gamma+\frac{\delta}{\beta}$$

and $\varphi(\delta/\beta)=\varphi(\delta)/\varphi(\beta)<1$. Note that every complex number $z\in\mathbb{C}$ can be written $z=\xi+\eta$, 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 Figure 4.1.

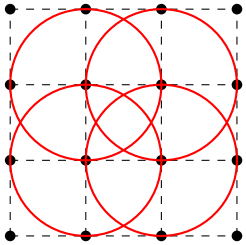


fig:covering

Figure 4.1: $\mathbb{C}$ is covered by open unit disks of radius one and centers in $\mathbb{Z}[i]$.

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 $r,s\in\mathbb{Q}$. 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 5.27. 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 4.2. 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.

Proposition 5.28. *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 5.29. Since $\mathbb{Z}[i]$ is euclidean, then it is principal.

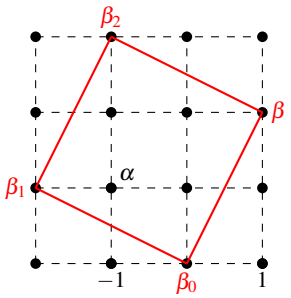


fig:Z[i]

Figure 4.2: Division algorithm in $\mathbb{Z}[i]$.

Example 5.30. 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 for example see [2], [9] or [8].

Definition 5.31. 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. This fact will be proved in the proof of the following theorem. However, not all these rings with be euclidean domains.

Theorem 5.32. *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 $x \notin \mathscr{U}(R)$. 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 $x_{11} \notin \mathscr{U}(R)$ 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 5.33. The ring $\mathbb{Z}[i]$ is a unique factorization domain.

We conclude the lecture with an example of a noetherian domain that is not a unique factorization domain.

Example 5.34. 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.

Lecture 5

In this lecture we prove Fermat's theorem, which concludes our study of factorization in arbitrary commutative rings. Then we present Zorn's lemma and some applications. Finally, we introduce the (complex) group algebra and other basic examples of algebras.

Theorem 5.35 (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 $a + bi \notin \mathscr{U}(\mathbb{Z}[i])$ 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 $a^2 + b^2 \equiv 2 \bmod 4$. □

§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 $r < s$ or $s < r$.

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 $s \in S$.

Example 6.8. 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 6.9. 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 than a lemma. The reason for calling Zorn's lemma a lemma rather than an axiom is purely historical.

Definition 6.10. 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 6.11. Let R be a commutative ring. Prove that R is a field if and only if $\{0\}$ is a maximal ideal of R.

Exercise 6.12. 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 6.13 (Krull). *Let R be a ring. Each proper ideal I of R is contained in a maximal ideal. In particular, all rings have maximal ideals.*

Proof. Let $X = \{J : J \text{ is an ideal of } R \text{ such that } I \subseteq J \subsetneq R\}$. Since $I \in X$, it follows that X is non-empty. Moreover, X is a poset with respect to the 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 previous theorem it is crucial to consider rings with identity.

Exercise 6.14. 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 6.15. Let R be a principal domain and $p \in R$. Then p is irreducible if and only if (p) is maximal.

Example 6.16. 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.

Example 6.17. 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 6.18. Compute the maximal ideals of $\mathbb{Z}/n$.

Exercise 6.19. Let R be a commutative ring and $J(R)$ be the intertopic 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 lecture with a different application of Zorn's lemma.

Exercise 6.20. Prove that every non-zero vector space has a basis.

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

Exercise 6.21. 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 6.22. Prove that the abelian groups $\mathbb{R}^n$ and $\mathbb{R}$ are isomorphic.

Exercise 6.23. Prove that if G is a group such that $|G| > 2$, then $|\operatorname{Aut}(G)| > 1$.

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

Proof. We leave 1) as an exercise.

Let us prove 2). Let $n_1 = \min\{k \in \mathbb{Z}_{>0} : k1 = 0\}$. Clearly $n \geq n_1$. For $x \in R$, $n_1 x = n_1(1x) = (n_1 1)x = 0x = 0$ and hence $n_1 \geq n$.

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

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

and hence $r1 = 0$ or $s1 = 0$, a contradiction. □

Exercise 7.3. 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 $R \to R$, $x \mapsto x^p$, is a ring homomorphism.

§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

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

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 8.1. Let A be a ring. Then A is an algebra (over the field K) if A is a vector space (over K) 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 a 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 8.2. 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. Moreover, $K[G]$ is a vector space of dimension $\dim K[G] = |G|$.

Example 8.3. 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 $n \geq 2$.

Exercise 8.4. Prove that $\mathbb{R}[C_3] \simeq \mathbb{R} \times \mathbb{C}$.

Example 8.5. Let $G = \{1, g\} \simeq C_2$ be the cyclic group of order two. The product of $\mathbb{C}[G]$ is

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

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 8.6. 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 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 8.7. 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.

Lecture 6

§9. Group representations

We will spend four lectures studying the basics on complex representations of finite groups. The topics to cover are: 1) Basic definitions and examples, 2) characters, 3) Schur's orthogonality relations and applications.

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.

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

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

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 9.3. If G is a group, then $\rho\colon G \to \mathbb{C}^\times$, $g \mapsto 1$, is a representation. This representation is known as the **trivial 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.

Proposition 9.6. *Let G be a finite group and $\rho\colon G \to \mathbf{GL}(V)$ be a representation of finite degree. 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 $m \in \mathbb{Z}_{>0}$. 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. □

In page 35 we will see an alternative proof of the previous proposition.

Definition 9.7. 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 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 9.8. The representations $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are **equivalent** if there exists a bijective map $T\colon V \to W$ invariant with respect to ρ and ψ.

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

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

Example 9.13. 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 invariant subspace of $\mathbb{R}^3$.

Definition 9.14. 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.

Example 9.15. 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 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 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 9.16. Let $\rho\colon G \to \mathbf{GL}(V)$ be a degree-two representation. Prove that ρ is irreducible if and only if there is no common eigenvector for the ρ_g, $g \in G$.

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

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

is irreducible.

Example 9.17. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations. One defines the **direct sum** $\rho \oplus \psi$ of ρ and ψ as

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

where $(\rho \oplus \psi)_g\colon V \oplus W \to V \oplus W$ is given by $(v,w) \mapsto (\rho_g(v), \psi_g(w))$.

Definition 9.18. 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 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 9.19. 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 9.20. 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 invariant subspaces of V.

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

Exercise 9.21. Let $\rho\colon G \to \mathbf{GL}(V)$ be a unitary representation. Prove that ρ is either irreducible or decomposable.

Example 9.22. 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 9.23 (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. □

rho_diagonalizable

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 9.24. 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 9.25 (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 $V = S \oplus T$, where S and T are non-zero 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 9.26. Let $G = \mathbb{S}_3$ and $\rho\colon G \to \mathbf{GL}_3(\mathbb{C})$ be the representation given by

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

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

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

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

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

Exercise 9.27. Let G be a finite group. Prove that there is a bijection between degree-one representations of G and degree-one representations of $G/[G,G]$.

Lemma 9.28 (Schur). *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations. If $T\colon V \to W$ is a non-zero invariant map, then T is bijective.*

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

Two applications:

Proposition 9.29. *If $\rho\colon G \to \mathbf{GL}(V)$ 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 λ be an eigenvector of T. Then $T - \lambda \operatorname{id}$ is invariant and it is not bijective. Thus $T - \lambda \operatorname{id} = 0$ by Schur's lemma. □

Proposition 9.30. *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 Schur's lemma, there exists $\lambda_h \in \mathbb{C}$ such that $\rho_h = \lambda_h \mathrm{id}$. If $v \in V \setminus \{0\}$, then $V = \langle v \rangle$, as ρ is irreducible. □

Lecture 7

§10. Characters

This lecture is devoted to study character theory. We prove the first Schur orthogonality relation and present several applications.

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

If a representation ρ 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, χ 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) $|\chi(g)| \leq \chi(1)$.

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 ρ_g is the sum of the eigenvalues of ρ_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 λ_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

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

□

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

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

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

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

where

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

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 $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations, then*

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

Proof. For each $g \in G$ the map ρ_g is diagonalizable. Let $\{v_1, \ldots, v_n\}$ be a basis of eigenvectors of ϕ_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 ψ_g and

$\mu_1,\dots,\mu_m \in \mathbb{C}$ be such that $\psi_g(w_j) = \mu_j w_j$ for all $j \in \{1,\dots,m\}$. Each $v_i \otimes w_j$ is eigenvector of $\phi \otimes \psi$ 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 $(\phi \otimes \psi)_g$. 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.

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 10.7. *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

$$\begin{aligned} T^{\#}\phi_h(v) &= \frac{1}{|G|}\sum_{g\in G}\psi_{g^{-1}}T\phi_g\phi_h(v) = \frac{1}{|G|}\sum_{g\in G}\psi_{g^{-1}}T\phi_{gh}(v) \\ &= \frac{1}{|G|}\sum_{x\in G}\psi_{hx^{-1}}T\phi_x(v) = \frac{1}{|G|}\sum_{x\in G}\psi_h\psi_{x^{-1}}T\phi_x(v) = \psi_h T^{\#}(v). \end{aligned}$$

If $T \in \mathrm{Hom}_{\mathbb{C}[G]}(V,V)$, then

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

for all $v \in V$. □

If $\phi\colon G \to \mathbf{GL}(V)$ 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 $T^{\#} \in \mathrm{Hom}_{\mathbb{C}[G]}(V,W) = \{0\}$ by the previous proposition and Schur's lemma.

Theorem 10.8 (Ergodic theorem). *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 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

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

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, then ρ_g is the matrix $(\rho_{ij}(g))$ and hence the character of ρ is given by

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

Lemma 10.9. *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations. Then $(E_{ik}^{\#})_{lj} = \langle \rho_{ij}, \psi_{kl} \rangle$.*

Proof. We compute

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

□

Theorem 10.10 (Schur). *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations. Then the following statements hold:*

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

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

Proof. Let us prove the first claim. Since ρ and ψ 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:

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

□

Now we can prove Schur's first orthogonality relation.

Theorem 10.11 (Schur). *Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be irreducible representations. 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

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

□

Schur's theorem has several important corollaries.

If $\rho\colon G \to \mathbf{GL}(V)$ is an irreducible representaion of degree n, then

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

is an orthonormal set.

Corollary 10.12. *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. Since $\dim L(G) = |G|$, it follows that G admits $\le |G|$ equivalence classes of irreducible representations. Let $\rho_1, \dots \rho_r$ be the representatives of the isomorphism classes of the irreducible representations of G. For each k let $n_k = \deg \rho_k$. Since the $n_1^2 + \cdots n_r^2$ maps $\sqrt{n_k}(\rho_k)_{ij}$, $1 \le k \le r$, $1 \le i, j \le n_k$, form an orthonormal set of $L(G)$, it follows that $r \le n_1^2 + \cdots n_r^2 \le |G|$. □

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

$$\rho_1, \dots, \rho_r$$

are *the* irreducible representations of G, where it is assumed that the ρ_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

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

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 δ_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 10.13. *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 ρ is a representation, we write $m\rho = \rho \oplus \cdots \oplus \rho$ (m-times).

Theorem 10.14. *Let $\rho_1, \ldots, \rho_r$ be the irreducible representations of a finite group G. If $\rho = \sum_{i_1}^{r} m_j \rho_j$ where $m_1, \ldots m_r \in \mathbb{Z}_{\geq 0}$, then $m_j = \langle \rho_\rho, \rho_j \rangle$ for all $j \in \{1, \ldots, r\}$.*

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

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

for all $i \in \{1, \ldots, r\}$. □

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

Corollary 10.15. *A representation ρ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.*

Proof. We first decompose ρ 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 10.16. Let $\rho \colon H \to \mathbf{GL}(V)$ be an irreducible representation of H and $f \colon G \to H$ be a surjective group homomorphism. Prove that the composition $\rho \circ f \colon G \to \mathbf{GL}(V)$ is an irreducible representation.

Theorem 10.17. *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 $L_g(g_i) = gg_i$ for all i, the matrix of L_g in the basis $\{g_1, \ldots, g_n\}$ is then

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

Then

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

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 $i \in \{1, \dots, n\}$. □

Now several corollaries.

Corollary 10.18. *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

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

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

$$T^{\#} = \frac{1}{|G|} \sum_{g \in G} (\rho_k)_{g^{-1}} (\rho_k)_x (\rho_k)_g = \frac{1}{|G|} \sum_{g \in G} (\rho_k)(g^{-1} x g) = \frac{1}{\dim V} \chi_k(x) \, \mathrm{id}$$

by the Ergodic theorem and because ρ_k is a group homomorphism. Thus

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

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

In the following exercise, the reader is asked to provide a proof of the second Schur's orthogonality relation.

Exercise 10.19. Let G be a finite group and C and D be conjugacy classes of G. If $g \in C$ and $h \in D$, then

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

Lecture 8

§11. Examples

This chapter contains examples of character tables. Then we study modules over rings, submodules, module homomorphisms and finitely-generated modules.

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 χ_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 χ_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
χ_1	1	1	$\cdots$	1
χ_2	n_2	$\chi_2(g_2)$	$\cdots$	$\chi_2(g_r)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_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 11.1. 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
χ_1	1	1	1	1
χ_2	1	λ	λ^2	λ^3
χ_3	1	λ^2	λ^4	λ^2
χ_4	1	λ^3	λ^2	λ

Exercise 11.2. 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 $\chi_i\colon C_n \to \mathbb{C}^\times$, $g^k \mapsto e^{2\pi ik/n}$, where $i \in \{0,1,\dots,n-1\}$, are the irreducible representations of C_n.

2) Let λ 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}
χ_1	1	1	1	$\cdots$	1
χ_2	1	λ	λ^2	$\cdots$	λ^{n-1}
χ_3	1	λ^2	λ^4	$\cdots$	λ^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_n	1	λ^{n-1}	λ^{n-2}	$\cdots$	λ

Exercise 11.3. Let A and B be abelian groups. We write $\mathrm{Irr}(A) = \{\rho_1,\dots,\rho_r\}$ and $\mathrm{Irr}(B) = \{\phi_1,\dots,\phi_s\}$. 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 11.4. The character table of the group $C_2 \times C_2 = \{1,a,b,ab\}$ is

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Clearly, the order in which the computer returns the irreducible characters is not necessarily the same we used!

Example 11.5. 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)
χ_1	1	1	1
χ_2	1	-1	1
χ_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 11.6. Compute the character table of $\mathbb{S}_4$.

Example 11.7. 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 χ 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 χ_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)
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

Example 11.8. Let $Q_8 = \{-1, 1, i, -i, j, -j\}$ be the quaternion group. Let us compute the character table of Q_8. The group Q_8 is generated by $\{i, j\}$ and the map $\rho\colon Q_8 \to \mathbf{GL}_2(\mathbb{C})$,

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

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 ρ:

	1	-1	i	j	k
χ_ρ	2	2	0	0	0

Then ρ 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
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_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 11.9. Compute the character table of the dihedral group of eight elements.

§12. Modules

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

Definition 12.1. Let R be a ring. A **module** (over R) is an abelian group M with a map $R \times M \to M$, $(x,m) \mapsto x \cdot m$, 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, so they will be referred simply as modules.

Example 12.2. A module over a field is a vector space.

Example 12.3. Every abelian group is a module over $\mathbb{Z}$.

Example 12.4. 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 be denoted by ${}_R R$.

Example 12.5. 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 12.6. 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 12.7. If $f\colon R \to S$ is a ring homomorphism and M is a module (over S) wih $(s,m) \mapsto sm$, then M is also a module (over R) with $r \cdot m = f(r)m$ for all $r \in R$ and $m \in M$. In fact,

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

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

Example 12.8. Let $R = \mathbb{R}[X]$ and $T\colon \mathbb{R}^n \to \mathbb{R}^n$ be a linear map. 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 12.9. If $\{M_i | i \in I\}$ is a family of 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 a 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 12.10. If $\{M_i | i \in I\}$ is family of 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 a 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 12.11. 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 $\mathbb{Z}/6$).

Definition 12.12. 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 12.13. 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 12.14. 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 12.15. 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 12.16. If V is a vector space and $T : V \to V$ is a linear map, then V is a module (over $\mathbb{R}[X]$) with

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

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

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

Exercise 12.17. 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 12.18. 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 12.19. 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 12.20. 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 $g, h \in \mathrm{Hom}_R(V,M)$, $f\circ g = f\circ h \implies g = h$.
4) For every module V and every $g \in \mathrm{Hom}(V,M)$, $f\circ g = 0 \implies g = 0$.

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

Example 12.21. Let $R = \begin{pmatrix} \mathbb{R} & 0 \\ 0 & \mathbb{R} \end{pmatrix}$. We claim that $\begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix} \not\cong \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix}$ as modules over R, where the module structure is given by the usual matrix multiplication. Assume that they are isomorphic. Let $f\colon \begin{pmatrix} 0 \\ \mathbb{R} \end{pmatrix} \to \begin{pmatrix} \mathbb{R} \\ 0 \end{pmatrix}$ be an isomorphism of modules and let $x_0 \in \mathbb{R}\setminus\{0\}$ be such that $f\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_0 \\ 0 \end{pmatrix}$. Thus

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

a contradiction, as f is injective.

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

Example 12.22. If $M = \mathbb{R}^2$ as 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 12.23. 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 $nm = 0$.

xca:projector

Exercise 12.24. 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 $p \circ i = \mathrm{id}_N$. 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 12.25. 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 intertopic $\cap_{i \in I} N_i$ is also a submodule of M.

xca:submodules

Exercise 12.26. 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) $T(x,y) = (y,x)$.

xca:commuting

Example 12.27. 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.

xca:Hom

Exercise 12.28. Prove that $\mathrm{Hom}_R(M,N)$ is a module over $Z(R)$.

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

Example 12.30. Let R be a commutative ring. We claim that

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

Since R is commutative, it follows that $\mathrm{Hom}_R({}_RR, M)$ is a module, see Exercise 12.28. Let $\varphi\colon M \to \mathrm{Hom}_R({}_RR, M)$, $m \mapsto f_m$, where $f_m\colon R \to M$, $r \mapsto r \cdot m$. To show that φ is well-defined it is enough to see that $\varphi(m) \in \mathrm{Hom}_R({}_RR, M)$, that is

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

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

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

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

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

Moreover,

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

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

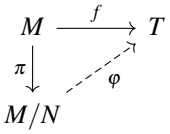
$$\begin{aligned} \varphi(r \cdot m)(s) &= f_{r \cdot m}(s) = s \cdot (r \cdot m) = (sr) \cdot m \\ &= (rs) \cdot m = f_m(rs) = \varphi(m)(rs) = (r \cdot \varphi(m))(s). \end{aligned}$$

It remains to show that φ is bijective. We first prove that φ is injective. If $\varphi(m) = 0$, then $r \cdot m = \varphi(m)(r) = 0$ for all $r \in R$. In particular, $m = 1 \cdot m = 0$. We now prove that φ is surjective. If $f \in \mathrm{Hom}_R({}_RR, M)$, 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 12.31. 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 second 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 12.32. 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 12.33. 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 W and every $g,h \in \mathrm{Hom}_R(N,T)$, $g \circ f = h \circ f \implies g = h$.
4) For every module T and every $g \in \mathrm{Hom}_R(N,T)$, $g \circ f = 0 \implies g = 0$.

xca:mod_iso_max

Exercise 12.34. 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 9

Definition 12.35. 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 12.36. 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 12.37. 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 12.38. 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.

Proposition 12.39. *Let R be a ring and M be a module over R. Then M is finitely-generated if and only if M is isomorphic to a quotient of R^k for some k.*

Proof. Assume first that $M = (m_1, \ldots, m_k)$ is finitely-generated. A routine calculation shows that the map

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

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 12.40. 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 $k \in \mathbb{Z}_{>0}$, $r_1,\dots,r_k \in R$ and $m_1,\dots,m_k \in X$ 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.

Examples 12.41.

1) $\{2,3\}$ is a linear 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 linearly independent subset of M. Is $y \in M \setminus \{x\}$, then $\{x,y\}$ is linearly dependent.

Examples 12.42. 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 linearly independent.

Exercise 12.43. 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 12.44. 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 12.45.

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

Exercise 12.47. 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.

Example 12.48. $\mathbb{R}[X]$ is a free module (over $\mathbb{R}$) with basis $\{1, X, X^2, \dots\}$.

Exercise 12.49. 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 $ad - bc \in \{-1, 1\}$.

Some hints

Lecture 2

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

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

Some solutions

Lecture 4

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

References

1. M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.
2. O. A. Cámpoli. A principal ideal domain that is not a Euclidean domain. *Amer. Math. Monthly*, 95(9):868–871, 1988.
3. D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.
4. T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
5. S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.
6. J.-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.
7. B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.
8. J. C. Wilson. A principal ideal ring that is not a Euclidean ring. *Math. Mag.*, 46:34–38, 1973.
9. 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