Leandro Vendramin

Rings and modules

Notes

Saturday 4th September, 2021

Versión compilada el Saturday 4th September, 2021 a las 21:16.

Leandro Vendramin
Brussels, Belgium

Part I
Rings

Chapter 1
Rings and ideals

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

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

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

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

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

Example 1.4. The set

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

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

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

Let R be a ring. Some facts:

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

Example 1.6. The real vector space $H(\mathbb{R}) = \{a1 + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ with basis $\{1, i, j, k\}$ is a ring with the multiplication induced by the formulas

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

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

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

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

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

Example 1.8. Let $n \geq 1$. The set $M_n(\mathbb{R})$ of real $n \times n$ matrices is a ring with the usual matrix operations. Recall that if $a = (a_{ij})$ and $b = (b_{ij})$, the multiplication ab is given by

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

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

Definition 1.9. Let R be a ring. A **subring** S of R is a subset S such that $(S, +)$ is a subgroup of $(R, +)$ such that $1 \in S$ and if $x, y \in S$, then $xy \in S$.

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

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

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

Example 1.12. If R is a ring, then the **center** $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$ is a subring of R.

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

Exercise 1.13.

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

Definition 1.14. Let R be a ring. An element $x \in R$ is a **unit** if there exists $y \in R$ such that $xy = yx = 1$.

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

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

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

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

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

Exercise 1.17. $\mathbb{Q}[\sqrt{2}]$ is a field. Find the multiplicative inverse of $x + y\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

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

Definition 1.18. Let R be a ring. A **left ideal** of R is a subset I such that $(I,+)$ is a subgroup of $(R,+)$ and such that $RI \subseteq I$, i.e. $ry \in I$ for all $r \in R$ and $y \in I$.

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

Example 1.19. Let $R = M_2(\mathbb{R})$. Then

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

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

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

Definition 1.20. Let R be a ring. An ideal of R is a subset that is both a left and a right ideal of R.

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

Exercise 1.21. Let R be a ring.

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

Example 1.22. Let $R = \mathbb{R}[X]$. If $f(X) \in R$, then the set

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

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

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

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

One proves that

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

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

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

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

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

Definition 1.26. Let R be a ring and I be an ideal of R. Then I is **principal** if $I = (x)$ for some $x \in R$.

The division algorithm shows that every ideal of $\mathbb{Z}$ is principal, see Exercise 1.23.

Exercise 1.27. Prove that every ideal of $\mathbb{R}[X]$ is principal.

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

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

One proves that a field has only two ideals.

Definition 1.29. Let R and S be rings. A map $f : R \to S$ is a **ring homomorphism** if $f(1) = 1$, $f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all $x, y \in R$.

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

Example 1.30. The map $f : \mathbb{Z}/6 \to \mathbb{Z}/6$, $x \mapsto 3x$, is not a ring homomorphism because $f(1) = 3$.

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

Example 1.31. The inclusions $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ are ring homomorphisms.

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

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

Example 1.33. Let $x_0 \in \mathbb{R}$. The evaluation map $\mathbb{R}[X] \to \mathbb{R}$, $f \mapsto f(x_0)$, is a ring homomorphism.

The **kernel** of a ring homomorphism $f\colon R \to S$ is the subset

$$\ker f = \{x \in R : f(x) = 0\}.$$

One proves that the kernel of f is an ideal of R. Moreover, $\ker f = \{0\}$ if and only if f is injective. The image

$$f(R) = \{f(x) : x \in R\}$$

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

Example 1.34. The map $\mathbb{C} \to M_2(\mathbb{R})$, $a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, is an injective ring homomorphism.

Example 1.35. The map $\mathbb{Z}[i] \to \mathbb{Z}/5$, $a+bi \mapsto a+2b \bmod 5$, is a ring homomorphism with $\ker f = \{a+bi : a+2b \equiv 0 \bmod 5\}$.

Exercise 1.36. There is no ring homomorphism $\mathbb{Z}/6 \to \mathbb{Z}/15$. Why?

Exercise 1.37. If $f\colon \mathbb{R}[X] \to \mathbb{R}$ is a ring homomorphism such that the restriction $f|_{\mathbb{R}}$ of f onto $\mathbb{R}$ is the identity, then there exists $x_0 \in \mathbb{R}$ such that f is the evaluation map at x_0.

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

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

and the **canonical map** $R \to R/I$, $x \mapsto x+I$, is a surjective group homomorphism. Recall that R/I is the set of cosets $x+I$, where $x+I = y+I$ if and only if $x-y \in I$. Note that here we only used that I is an additive subgroup of R. We need an ideal to put a ring structure on the set R/I of cosets modulo I. As in the case of integers, we use the following notation. For $x, y \in R$ we write

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

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

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

Since I is an ideal of R, this multiplication is well-defined. In fact, let $x+I = x_1+I$ and $y+I = y_1+I$. We want to show that $xy+I = x_1y_1+I$. Since $x-x_1 \in I$,

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

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

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

as I is a left ideal. Thus

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

Theorem 1.38. *Let R be a ring and I be an ideal of R. Then R/I with*

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

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

We have already seen that the multiplication is well-defined. The rest of the proof is left as an exercise.

Example 1.39. Let $R = (\mathbb{Z}/3)[X]$ and $I = (2X^2+X+2)$ be the ideal of R generated by the polynomial $2X^2+X+2$. If $f(X) \in R$, the division algorithm allows us to write

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

for some $q(X), r(X) \in R$, where either $r(X) = 0$ or $\deg r(X) < 2$. This means that $r(X) = aX+b$ for some $a,b \in R$. Note that $f(X) \equiv aX+b \bmod (2X^2+X+2)$ for some $a,b \in \mathbb{Z}/3$, so the quotient ring R/I has nine elements.

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

Theorem 1.40 (first isomorphism theorem). *If $f\colon R \to S$ is a ring homomorphism, then $R/\ker f \simeq f(R)$.*

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

Example 1.41. The evaluation map $\mathbb{R}[X] \to \mathbb{C}$, $f(X) \mapsto f(i)$, is a surjective ring homomorphism with kernel (X^2+1). Thus

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

by the first isomorphism theorem. In practice, this is how it works. Let $f(X) \in \mathbb{R}[X]$. The division algorithm on $\mathbb{R}[X]$ allows us to write

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

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

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

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

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

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

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

which reminds us the usual multiplication rule of the field of complex numbers.

Example 1.42. Let

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

A direct calculation shows that the map $R \to \mathbb{Q}$, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a$, is a surjective ring homomorphism with $\ker f = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Q} \right\}$. Thus $R/\ker f \simeq \mathbb{Q}$.

Exercise 1.43. Let R be the ring of continuos maps $[0,2] \to \mathbb{R}$. Prove that the set $I = \{f \in R : f(1) = 0\}$ is an ideal of R and that $R/I \simeq \mathbb{R}$.

Exercise 1.44. Let $n \geq 1$. Let R be a ring and I be an ideal of R. Prove that $M_n(I)$ is an ideal of $M_n(R)$ and that $M_n(R)/M_n(I) \simeq M_n(R/I)$.

Exercise 1.45. Let $R = \mathbb{Z}[\sqrt{10}]$ and $I = (2, \sqrt{10})$. Prove that $R/I \simeq \mathbb{Z}/2$.

Exercise 1.46. Prove that $\mathbb{Z}[i]/(1+3i) \simeq \mathbb{Z}/10$.

Exercise 1.47. Prove that there is no ideal I of $\mathbb{Z}[i]$ such that $\mathbb{Z}[i]/I \simeq \mathbb{Z}/15$.

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

Theorem 1.48 (correspondence theorem). *Let $f\colon R \to S$ be a surjective ring homomorphism. There exists a bijective correspondence between the set of ideals of R containing* $\ker f$ *and the set of ideals of S.*

Sketch of proof. Let I be an ideal of R contaning $\ker f$ and let J be an ideal of S. We need to prove the following facts:

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

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

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

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

Chapter 2
Chinese remainder theorem

Note that if R is a commutative ring and I and J are ideals of R, then

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

is an ideal of R.

Definition 2.1. Let R be a commutative ring. The ideals I and J of R are said to be **coprime** if $R=I+J$.

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

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

If I and J are ideals of R, then

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

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

Proposition 2.2. *Let R be a commutative ring. If I and J are coprime ideals, then $IJ=I\cap J$.*

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

Theorem 2.3 (chinese remainder theorem). *Let R be a commutative ring and I and J be coprime ideals. If $u,v\in R$, then there exists $x\in R$ such that*

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

Proof. Since the ideals I and J are coprime, $1 = a+b$ for some $a \in I$ and $b \in J$. Let $x = av + bu$. Then

$$x - u = av + (b-1)u = av - au = a(v-u) \in I,$$

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

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

Proof. Let $\pi_I \colon R \to R/$ and $\pi_J \colon R \to R/J$ be the canonical maps. A straightforward calculation shows that the map $\varphi \colon R \to R/I \times R/J$, $x \mapsto (\pi_I(x), \pi_J(x))$, is an injective ring homomorphism with $\ker \varphi = I \cap J$. The chinese remainder theorem implies that φ is surjective. If $(u+I, v+J) \in R/I \times R/J$, then there exists $x \in R$ such that $x - u \in I$ and $x - v \in J$. This translates into the surjectivity of φ. Now $R/(I \cap J) \simeq R/I \times R/J$ by the first isomorphism theorem. □

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

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

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

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

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

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

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

xca:gather_people

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

xca:no_solution

Exercise 2.7. Prove that

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

does not have solution.

xca:consecutive

Exercise 2.8. Find three consecutive integers such that the first one is divisible by a square, the second one is divisible by a cube and the third one is divisible by a fourth power.

xca:perfect_square

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

Chapter 3
Noetherian rings

In this chapter we will work with commutative rings.

Definition 3.1. A ring R is said to be **noetherian** if every (increasing) sequence $I_1 \subseteq I_2 \subseteq \cdots$ of ideals of R stabilizes, that is $I_n = I_m$ for some $m \in \mathbb{N}$ and all $n \geq m$.

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

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

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

For $n \in \mathbb{N}$ let $I_n = \{f \in R : f|_{[0,1/n]} = 0\}$. Then each I_n is an ideal of R and the sequence $I_1 \subsetneq I_2 \subsetneq \cdots$ does not stabilizes. Thus R is not noetherian.

Definition 3.3. Let R be a ring. An ideal I of R is said to be **finitely generated** if $I = (X)$ for some finite subset X of R.

The zero ideal is always finitely generated.

Proposition 3.4. *Let R be a ring. Then R is noetherian if and only if every ideal of R is finitely generated.*

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

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

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

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

Proposition 3.6. *Let I be an ideal of R. If R is noetherian, then R/I is noetherian.*

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

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

and hence J is finitely generated. $\square$

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

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

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

Proof. We need to show that every ideal of $R[X]$ is finitely generated. Assume that there is an ideal I of $R[X]$ that is not finitely generated. In particular, $I \neq \{0\}$. Let $f_1(X) \in I \setminus \{0\}$ be of minimal degree. For $i > 1$ let $f_i(X) \in I$ be of minimal degree such that $f_i(X) \notin (f_1(X), \dots, f_{i-1}(X))$ (note that such an $f_i(X)$ exists because I is not finitely generated). For each i let a_i be the leading coefficient of $f_i(X)$, that is

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

where the dots denote lowest degree terms. Note that $a_i \neq 0$. Let $J = (a_1, a_2, \dots)$. Since R is noetherian, the sequence

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

stabilizes, so J is finitely generated, say $J = (a_1, \dots, a_m)$ for some $m \in \mathbb{N}$. There exist $u_1, \dots, u_m \in R$ such that

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

Let

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

The leading coefficient of $g(X)$ is $\sum_{i=1}^{m} u_i a_i = a_{m+1}$ and, moreover, the degree of $g(X)$ is n_{m+1}. Thus $\deg(g(X)) < n_{m+1}$. Since $f_{m+1}(X) \notin (f_1(X) \dots, f_n(X))$,

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

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

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

Example 3.9. Since $\mathbb{Z}$ is noetherian, so is $\mathbb{Z}[X]$ by Hilbert's theorem. Now $\mathbb{Z}[\sqrt{N}]$ is noetherian, as $\mathbb{Z}[\sqrt{N}] \simeq \mathbb{Z}[X]/(X^2-N)$ and quotients of noetherian rings are noetherian.

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

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

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

Chapter 4
Factorization

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

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

Definition 4.2. Let R be an integral domain and $x, y \in R$. Then x **divides** y if $y = xz$ for some $x \in R$. Notation: $x \mid y$ if and only if x divides y. If x does not divide y one writes $x \nmid y$.

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

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

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

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

Example 4.5. Let $R = \mathbb{Z}[i]$.

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

Example 4.6. Let $R = \mathbb{R}[X]$ and $f(X) \in R$. Then $f(X)$ and $\lambda f(X)$ are associate in R for all $\lambda \in \mathbb{R}^\times$.

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

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

Example 4.8. Let $R = \mathbb{R}[X]$ and $f(X) \in R \setminus \{0\}$. Then $f(X)$ is irreducible if $\lambda \in \mathbb{R}^\times$ or $\lambda f(X)$ for $\lambda \in \mathbb{R}^\times$ are the only divisors of $f(X)$.

The irreducibles of $\mathbb{Z}$ are the prime numbers.

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

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

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

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

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

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

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

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

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

satisfies the following properties:

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

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

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

1) $\mathscr{U}(R) = \{-1, 1, i, -i\}$.
2) 3 is irreducible in R. In fact, if $3 = \alpha\beta$, then $9 = N(\alpha)N(\beta)$. This implies that $N(\alpha) \in \{1, 3, 9\}$. Write $\alpha = a + bi$ for $a, b \in \mathbb{Z}$. If $N(\alpha) = 1$, then $\alpha \in \mathscr{U}(R)$ by the lemma. If $N(\alpha) = 9$, then $N(\beta) = 1$ and hence $\beta \in \mathscr{U}(R)$ by the lemma. Finally, if $N(\alpha) = 3$, then $a^2 + b^2 = 3$, which is a contradiction since $a, b \in \mathbb{Z}$.
3) 2 is not irreducible in R. In fact, $2 = (1+i)(1-i)$ and since $N(1+i) = N(1-i) = 2$, it follows that $1 + i \notin \mathscr{U}(R)$ and $1 - i \notin \mathscr{U}(R)$.

Chapter 5
Zorn´s lemma

Chapter 6
Some solutions

Rings and ideals

Chinese remainder theorem

Noetherian rings

Factorization

Zorn´s lemma

References

Index