Chapter 3

Ring Theory

In the first section below, a ring will be defined as an abstract structure with a commutative addition, and a multiplication which may or may not be commutative. This distinction yields two quite different theories: the theory of respectively commutative or non-commutative rings. These notes are mainly concerned about commutative rings.

Non-commutative rings have been an object of systematic study only quite recently, during the 20th century. Commutative rings on the contrary have appeared though in a hidden way much before, and as many theories, it all goes back to Fermat's Last Theorem.

In 1847, the mathematician Lamé announced a solution of Fermat's Last Theorem, but Liouville noticed that the proof depended on a unique decomposition into primes, which he thought was unlikely to be true. Though Cauchy supported Lamé, Kummer was the one who finally published an example in 1844 (in an obscure journal, rediscovered in 1847) to show that the uniqueness of prime decompositions failed. Two years later, he restored the uniqueness by introducing what he called "ideal complex numbers" (today, simply "ideals") and used it to prove Fermat's Last Theorem for all $n < 100$ except $n = 37$, 59, 67 and 74.

It is Dedekind who extracted the important properties of "ideal numbers", defined an "ideal" by its modern properties: namely that of being a subgroup which is closed under multiplication by any ring element. He further introduced prime ideals as a generalization of prime numbers. Note that today we still use the terminology "Dedekind rings" to describe rings which have in particular a good behavior with respect to factorization of prime ideals. In 1882, an important paper by Dedekind and Weber developed the theory of rings of polynomials. At this stage, both rings of polynomials and rings of numbers (rings appearing in the context of Fermat's Last Theorem, such as what we call now the Gaussian integers) were being studied. But it was separately, and no one made connection between these two topics. Dedekind also introduced the term

"field" (Körper) for a commutative ring in which every non-zero element has a multiplicative inverse but the word "ring" is due to Hilbert, who, motivated by studying invariant theory, studied ideals in polynomial rings proving his famous "Basis Theorem" in 1893.

It will take another 30 years and the work of Emmy Noether and Krull to see the development of axioms for rings. Emmy Noether, about 1921, is the one who made the important step of bringing the two theories of rings of polynomials and rings of numbers under a single theory of abstract commutative rings.

In contrast to commutative ring theory, which grew from number theory, non-commutative ring theory developed from an idea of Hamilton, who attempted to generalize the complex numbers as a two dimensional algebra over the reals to a three dimensional algebra. Hamilton, who introduced the idea of a vector space, found inspiration in 1843, when he understood that the generalization was not to three dimensions but to four dimensions and that the price to pay was to give up the commutativity of multiplication. The quaternion algebra, as Hamilton called it, launched non-commutative ring theory.

Other natural non-commutative objects that arise are matrices. They were introduced by Cayley in 1850, together with their laws of addition and multiplication and, in 1870, Pierce noted that the now familiar ring axioms held for square matrices.

An early contributor to the theory of non-commutative rings was the Scottish mathematician Wedderburn, who in 1905, proved "Wedderburn's Theorem", namely that every finite division ring is commutative and so is a field.

It is only around the 1930's that the theories of commutative and non-commutative rings came together and that their ideas began to influence each other.

3.1 Rings, ideals and homomorphisms

Definition 3.1. A ring R is an abelian group with a multiplication operation

$$(a, b) \mapsto ab$$

which is associative, and satisfies the distributive laws

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

with identity element 1.

There is a group structure with the addition operation, but not necessarily with the multiplication operation. Thus an element of a ring may or may not be invertible with respect to the multiplication operation. Here is the terminology used.

Definition 3.2. Let a, b be in a ring R. If $a \neq 0$ and $b \neq 0$ but $ab = 0$, then we say that a and b are zero divisors. If $ab = ba = 1$, we say that a is a unit or that a is invertible.

While the addition operation is commutative, it may or not be the case with the multiplication operation.

Definition 3.3. Let R be ring. If $ab = ba$ for any a, b in R, then R is said to be commutative.

Here are the definitions of two particular kinds of rings where the multiplication operation behaves well.

Definition 3.4. An integral domain is a commutative ring with no zero divisor. A division ring or skew field is a ring in which every non-zero element a has an inverse a^{-1}. A field is a commutative ring in which every non-zero element is invertible.

Let us give two more definitions and then we will discuss several examples.

Definition 3.5. The characteristic of a ring R, denoted by char$R$, is the smallest positive integer such that

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n\text{times}} = 0.$$

If there is no such positive integer, we say that the ring has characteristic 0.

We can also extract smaller rings from a given ring.

Definition 3.6. A subring of a ring R is a subset S of R that forms a ring under the operations of addition and multiplication defined in R.

Examples 3.1.

1. $\mathbb{Z}$ is an integral domain but not a field.
2. The integers modulo n form a commutative ring, which is an integral domain if and only if n is prime.
3. For $n \geq 2$, the $n \times n$ matrices $\mathcal{M}_n(\mathbb{R})$ with coefficients in $\mathbb{R}$ are a non-commutative ring, but not an integral domain.
4. The set
$$\mathbb{Z}[i] = \{a + bi,\ a, b \in \mathbb{Z}\},\ i^2 = -1,$$
is a commutative ring. It is also an integral domain, but not a field.
5. Let us construct the smallest and also most famous example of division ring. Take $1, i, j, k$ to be basis vectors for a 4-dimensional vector space over $\mathbb{R}$, and define multiplication by
$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -ij,\ kj = -jk,\ ik = -ki.$$
Then
$$\mathbb{H} = \{a + bi + cj + dk,\ a, b, c, d \in \mathbb{R}\}$$

	commutative	non-commutative
has zero divisor	integers mod n, n not a prime	matrices over a field
has no zero divisor	$\mathbb{Z}$	$\{a+bi+cj+dk,\ a,b,c,d \in \mathbb{Z}\}$
non-zero element invertible	$\mathbb{R}$	$\mathbb{H}$

forms a division ring, called the Hamilton's quaternions. So far, we have only seen the ring structure. Let us now discuss the fact that every non-zero element is invertible. Define the conjugate of an element $h = a+bi+cj+dk \in \mathbb{H}$ to be $\bar{h} = a-bi-cj-dk$ (yes, exactly the same way you did it for complex numbers). It is an easy computation (and a good exercise if you are not used to the non-commutative world) to check that

$$q\bar{q} = a^2 + b^2 + c^2 + d^2.$$

Now take q^{-1} to be

$$q^{-1} = \frac{\bar{q}}{q\bar{q}}.$$

Clearly $qq^{-1} = q^{-1}q = 1$ and the denominator cannot possibly be 0, but if $a = b = c = d = 0$.

6. If R is a ring, then the set $R[X]$ of polynomials with coefficients in R is a ring.

Similarly to what we did with groups, we now define a map from a ring to another which has the property of carrying one ring structure to the other.

Definition 3.7. Let R, S be two rings. A map $f : R \to S$ satisfying

1. $f(a+b) = f(a) + f(b)$ (this is thus a group homomorphism)
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$

for $a, b \in R$ is called ring homomorphism.

We do need to mention that $f(1_R) = 1_S$, otherwise, since a ring is not a group under multiplication, strange things can happen. For example, if $\mathbb{Z}_6$ denotes the integers mod 6, the map $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, $n \mapsto 3n$ satisfies that $f(m+n) = 3(m+n) = 3m+3n = f(m)+f(n)$, and $f(n)f(m) = 3m3n = 3mn = f(mn)$ but $f(1) \neq 1$ and f is not a ring homomorphism. Notice the difference with group homomorphism: from $f(a+b) = f(a)+f(b)$, we deduce that $f(a+0) = f(a)+f(0)$, that is $f(a) = f(a)+f(0)$. Now because $f(a)$ is invertible, it must be that $f(0) = 0$! Once we reach $f(a) = f(a)f(1)$, because $f(a)$ does not have to be invertible, we cannot conclude!

The notion of "ideal number" was introduced by the mathematician Kummer, as being some special "numbers" (well, nowadays we call them groups) having the property of unique factorization, even when considered over more

general rings than $\mathbb{Z}$ (a bit of algebraic number theory would be good to make this more precise). Today only the name "ideal" is left, and here is what it gives in modern terminology:

Definition 3.8. Let $\mathcal{I}$ be a subset of a ring R. Then an additive subgroup of R having the property that

$$ra \in \mathcal{I} \text{ for } a \in \mathcal{I},\ r \in R$$

is called a left ideal of R. If instead we have

$$ar \in \mathcal{I} \text{ for } a \in \mathcal{I},\ r \in R$$

we say that we have a right ideal of R. If an ideal happens to be both a right and a left ideal, then we call it a two-sided ideal of R, or simply an ideal of R.

Example 3.2. The even integers $2\mathbb{Z} = \{2n,\ n \in \mathbb{Z}\}$ form an ideal of $\mathbb{Z}$. The set of polynomials in $\mathbb{R}[X]$ with constant coefficient zero form an ideal of $\mathbb{R}[X]$.

Of course, for any ring R, both R and $\{0\}$ are ideals. We thus introduce some terminology to precise whether we consider these two trivial ideals.

Definition 3.9. We say that an ideal $\mathcal{I}$ of R is proper if $\mathcal{I} \neq R$. We say that is it non-trivial if $\mathcal{I} \neq R$ and $\mathcal{I} \neq 0$.

If $f : R \to S$ is a ring homomorphism, we define the kernel of f in the most natural way:

$$\mathrm{Ker} f = \{r \in R,\ f(r) = 0\}.$$

Since a ring homomorphism is in particular a group homomorphism, we already know that f is injective if and only if $\mathrm{Ker} f = \{0\}$. It is easy to check that $\mathrm{Ker} f$ is a proper two-sided ideal:

- $\mathrm{Ker} f$ is an additive subgroup of R.
- Take $a \in \mathrm{Ker} f$ and $r \in R$. Then

  $$f(ra) = f(r)f(a) = 0 \text{ and } f(ar) = f(a)f(r) = 0$$

  showing that ra and ar are in $\mathrm{Ker} f$.
- Then $\mathrm{Ker} f$ has to be proper (that is, $\mathrm{Ker} f \neq R$), since $f(1) = 1$ by definition.

We can thus deduce the following (extremely useful) result.

Lemma 3.1. *Suppose $f : R \to S$ is a ring homomorphism and the only two-sided ideals of R are $\{0\}$ and R. Then f is injective.*

Proof. Since $\mathrm{Ker} f$ is a two-sided ideal of R, then either $\mathrm{Ker} f = \{0\}$ or $\mathrm{Ker} f = R$. But $\mathrm{Ker} f \neq R$ since $f(1) = 1$ by definition (in words, $\mathrm{Ker} f$ is a proper ideal). □

At this point, it may be worth already noticing the analogy between on the one hand rings and their two-sided ideals, and on the other hand groups and their normal subgroups.

- Two-sided ideals are stable when the ring acts on them by multiplication, either on the right or on the left, and thus

$$rar^{-1} \in \mathcal{I},\ a \in \mathcal{I},\ r \in R,$$

  while normal subgroups are stable when the groups on them by conjugation

$$ghg^{-1} \in H,\ h \in H,\ g \in G\ (H \leq G).$$

- Groups with only trivial normal subgroups are called simple. We will not see it formally here, but rings with only trivial two-sided ideals as in the above lemma are called simple rings.

- The kernel of a group homomorphism is a normal subgroup, while the kernel of a ring homomorphism is an ideal.

- Normal subgroups allowed us to define quotient groups. We will see now that two-sided ideals will allow to define quotient rings.

3.2 Quotient rings

Let $\mathcal{I}$ be a proper two-sided ideal of R. Since $\mathcal{I}$ is an additive subgroup of R by definition, it makes sense to speak of cosets $r + \mathcal{I}$ of $\mathcal{I}$, $r \in R$. Furthermore, a ring has a structure of abelian group for addition, so $\mathcal{I}$ satisfies the definition of a normal subgroup. From group theory, we thus know that it makes sense to speak of the quotient group

$$R/\mathcal{I} = \{r + \mathcal{I},\ r \in R\},$$

group which is actually abelian (inherited from R being an abelian group for the addition).

We now endow $R/\mathcal{I}$ with a multiplication operation as follows. Define

$$(r + \mathcal{I})(s + \mathcal{I}) = rs + \mathcal{I}.$$

Let us make sure that this is well-defined, namely that it does not depend on the choice of the representative in each coset. Suppose that

$$r + \mathcal{I} = r' + \mathcal{I},\ s + \mathcal{I} = s' + \mathcal{I},$$

so that $a = r' - r \in \mathcal{I}$ and $b = s' - s \in \mathcal{I}$. Now

$$r's' = (a + r)(b + s) = ab + as + rb + rs \in rs + \mathcal{I}$$

since ab, as and rb belongs to $\mathcal{I}$ using that $a, b \in \mathcal{I}$ and the definition of ideal. This tells us $r's'$ is also in the coset $rs + \mathcal{I}$ and thus multiplication does not depend on the choice of representatives. Note though that this is true only because we assumed a two-sided ideal $\mathcal{I}$, otherwise we could not have concluded, since we had to deduce that both as and rb are in $\mathcal{I}$.

Definition 3.10. The set of cosets of the two-sided ideal $\mathcal{I}$ given by

$$R/\mathcal{I} = \{r + \mathcal{I},\ r \in R\}$$

is a ring with identity $1_R + \mathcal{I}$ and zero element $0_R + \mathcal{I}$ called a quotient ring.

Note that we need the assumption that $\mathcal{I}$ is a proper ideal of R to claim that $R/\mathcal{I}$ contains both an identity and a zero element (if $R = \mathcal{I}$, then $R/\mathcal{I}$ has only one element).

Example 3.3. Consider the ring of matrices $\mathcal{M}_2(\mathbb{F}_2[i])$, where $\mathbb{F}_2$ denotes the integers modulo 2, and i is such that $i^2 = -1 \equiv 1 \mod 2$. This is thus the ring of 2×2 matrices with coefficients in

$$\mathbb{F}_2[i] = \{a + ib,\ a, b \in \{0, 1\}\}.$$

Let $\mathcal{I}$ be the subset of matrices with coefficients taking values 0 and $1 + i$ only. It is a two-sided ideal of $\mathcal{M}_2(\mathbb{F}_2[i])$. Indeed, take a matrix $U \in \mathcal{I}$, a matrix $M \in \mathcal{M}_2(\mathbb{F}_2[i])$, and compute UM and MU. An immediate computation shows that all coefficients are of the form $a(1+i)$ with $a \in \mathbb{F}_2[i]$, that is all coefficients are in $\{0, 1 + i\}$. Clearly $\mathcal{I}$ is an additive group.

We then have a quotient ring

$$\mathcal{M}_2(\mathbb{F}_2[i])/\mathcal{I}.$$

We have seen that $\mathrm{Ker} f$ is a proper two-sided ideal when f is a ring homomorphism. We now prove the converse.

Proposition 3.2. *Every proper two-sided ideal $\mathcal{I}$ is the kernel of a ring homomorphism.*

Proof. Consider the canonical projection π that we know from group theory. Namely

$$\pi : R \to R/\mathcal{I},\ r \mapsto \pi(r) = r + \mathcal{I}.$$

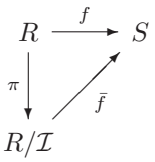
We already know that π is group homomorphism, and that its kernel is $\mathcal{I}$. We are only left to prove that π is a ring homomorphism:

- since $\mathcal{I}$ is two-sided, then $R/\mathcal{I}$ is a ring.
- $\pi(rs) = rs + \mathcal{I} = (r + \mathcal{I})(s + \mathcal{I}) = \pi(r)\pi(s)$.
- $\pi(1_R) = 1_R + \mathcal{I}$ which is indeed the identity element of $R/\mathcal{I}$.

□

We are now ready to state a factor theorem and a 1st isomorphism theorem for rings, the same way we did for groups. It may help to keep in mind the analogy between two-sided ideals and normal subgroups mentioned above.

Assume that we have a ring R which contains a proper two-sided ideal $\mathcal{I}$, another ring S, and $f : R \to S$ a ring homomorphism. Let π be the canonical projection from R to the quotient group $R/\mathcal{I}$:



We would like to find a ring homomorphism $\bar{f} : R/\mathcal{I} \to S$ that makes the diagram commute, namely

$$f(a) = \bar{f}(\pi(a))$$

for all $a \in R$.

Theorem 3.3. (Factor Theorem for Rings). *Any ring homomorphism f whose kernel K contains $\mathcal{I}$ can be factored through $R/\mathcal{I}$. In other words, there is a unique ring homomorphism $\bar{f} : R/\mathcal{I} \to S$ such that $\bar{f} \circ \pi = f$. Furthermore*

1. *$\bar{f}$ is an epimorphism if and only if f is.*
2. *$\bar{f}$ is a monomorphism if and only if $K = \mathcal{I}$.*
3. *$\bar{f}$ is an isomorphism if and only if f is an epimorphism and $K = \mathcal{I}$.*

Proof. Since we have already done the proof for groups with many details, here we will just mention a few important points in the proof.

Let $a + \mathcal{I} \in R/\mathcal{I}$ such that $\pi(a) = a + \mathcal{I}$ for $a \in R$. We define

$$\bar{f}(a + \mathcal{I}) = f(a).$$

This is the most natural way to do it, however, we need to make sure that this is indeed well-defined, in the sense that it should not depend on the choice of the representative taken in the coset. Let us thus take another representative, say $b \in a + \mathcal{I}$. Since a and b are in the same coset, they satisfy $a - b \in \mathcal{I} \subset K$, where $K = \mathrm{Ker}(f)$ by assumption. Since $a - b \in K$, we have $f(a - b) = 0$ and thus $f(a) = f(b)$.

Now that $\bar{f}$ is well defined, it is an easy computation to check that $\bar{f}$ inherits the property of ring homomorphism from f.

The rest of the proof works exactly the same as for groups. □

The first isomorphism theorem for rings is similar to the one for groups.

Theorem 3.4. (1st Isomorphism Theorem for Rings). *If $f : R \to S$ is a ring homomorphism with kernel K, then the image of f is isomorphic to R/K:*

$$\mathrm{Im}(f) \simeq R/\mathrm{Ker}(f).$$

Proof. We know from the Factor Theorem that

$$\bar{f} : R/\mathrm{Ker}(f) \to S$$

is an isomorphism if and only if f is an epimorphism, and clearly f is an epimorphism on its image, which concludes the proof. □

Example 3.4. Let us finish Example 3.3. We showed there that $\mathcal{M}_2(\mathbb{F}_2[i])/\mathcal{I}$ is a quotient ring, where $\mathcal{I}$ is the ideal formed of matrices with coefficients in $\{0, 1+i\}$. Consider the ring homomorphism:

$$f : \mathcal{M}_2(\mathbb{F}_2[i]) \to \mathcal{M}_2(\mathbb{F}_2), M = (m_{k,l}) \mapsto f(M) = (m_{k,l} \mod 1+i)$$

that is f looks at the coefficients of $M \mod 1+i$. Its kernel is $\mathcal{I}$ and it is surjective. By the first isomorphism for rings, we have

$$\mathcal{M}_2(\mathbb{F}_2[i])/\mathcal{I} \simeq \mathcal{M}_2(\mathbb{F}_2).$$

Example 3.5. A less exotic example, which we will study in more details later on, is the following. Consider the map $f : \mathbb{R}[X] \to \mathbb{C}$, $f(p(X)) = p(i)$, that is, f takes a polynomial $p(X)$ with real coefficients, and evaluate this polynomial in i ($i^2 = -1$). This map is surjective (take the polynomial $p(X) = X + (z - i)$, $z \in \mathbb{C}$) and its kernel is formed by polynomials which, when evaluated in i, are giving 0, meaning that i is a root of the polynomial, or equivalently that (X^2+1) is a factor of the polynomial. Thus $\mathrm{Ker}(f) = (X^2+1)\mathbb{R}[X] = \{p(X) = (X^2+1)q(X),\ q(X) \in \mathbb{R}[X]\}$. Using the first isomorphism for rings, we have

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

3.3 The Chinese Remainder Theorem

The name "Chinese Remainder Theorem" supposely comes from the following question: How many soldiers were part of Han Xing's army if, sorted by 3 columns, 2 soldiers were left, sorted by 5 columns, 3 soldiers were left, and sorted by 7 columns, 2 soldiers were left.

The Chinese Remained Theorem is attributed to Sun Zi (in the 3rd century), and was later published by Qin Jiushao (around 1247).

We will prove a "general" Chinese Remainder Theorem, rephrased in terms of rings and ideals.

For that let us start by introducing some new definitions about ideals, that will collect some of the manipulations one can do on ideals. Let us start with the sum.

Definition 3.11. Let $\mathcal{I}$ and $\mathcal{J}$ be two ideals of a ring R. The sum of $\mathcal{I}$ and $\mathcal{J}$ is the ideal

$$\mathcal{I} + \mathcal{J} = \{x + y,\ x \in \mathcal{I},\ y \in \mathcal{J}\}.$$

If $\mathcal{I}$ and $\mathcal{J}$ are right (resp. left) ideals, so is their sum.

Note that the intersection $\mathcal{I} \cap \mathcal{J}$ of two (resp. right, left, two-sided) ideals of R is again a (resp. right, left, two-sided) ideal of R.

Definition 3.12. The product of two left (resp. right) ideals $\mathcal{I}$ and $\mathcal{J}$ is the left (resp. right) ideal

$$\mathcal{I}\mathcal{J} = \{\sum_{i=1}^{n} x_i y_i,\ x_i \in \mathcal{I},\ y_i \in \mathcal{J}\}.$$

Example 3.6. Take $\mathcal{I} = 2\mathbb{Z}$ and $\mathcal{J} = 3\mathbb{Z}$ which are both two-sided ideals of $\mathbb{Z}$. We have

$$\mathcal{I} + \mathcal{J} = \{2x + 3y,\ x, y \in \mathbb{Z}\} = \mathbb{Z},$$

using Bezout identity (since $\gcd(2, 3) = 1$). Also

$$\mathcal{I} \cap \mathcal{J} = 6\mathbb{Z},\ \mathcal{I}\mathcal{J} = \{\sum_{i=1}^{n} 2x_i 3y_i,\ x, y \in \mathbb{Z}\} = 6\mathbb{Z}.$$

We can define a notion of being co-prime for ideals as follows.

Definition 3.13. The two-sided ideals $\mathcal{I}$ and $\mathcal{J}$ of a ring R are relatively prime if

$$\mathcal{I} + \mathcal{J} = R.$$

In a sense, this definition generalizes Bezout identity for rings.

Notice that for a commutative ring, if $\mathcal{I}$ and $\mathcal{J}$ are relatively prime then

$$\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}.$$

(This is also illustrated in the above example.) Indeed, we clearly have that

$$\mathcal{I}\mathcal{J} \subset \mathcal{I} \cap \mathcal{J}$$

since $\mathcal{I}\mathcal{J}$ contains by definition sums of elements xy, $x \in \mathcal{I}, y \in \mathcal{J}$, with $xy \in \mathcal{I}$ and $xy \in \mathcal{J}$ by definition of two-sided ideal. Conversely

$$\mathcal{I} \cap \mathcal{J} \subset \mathcal{I}\mathcal{J}$$

since there exist $x \in \mathcal{I}, y \in \mathcal{J}$ such that $x + y = 1$ by definition of relatively prime, and for every element $a \in \mathcal{I} \cap \mathcal{J}$, we have that

$$a = a(x + y) = ax + ay = xa + ay \in \mathcal{I}\mathcal{J}.$$

For R a non-commutative ring, where $\mathcal{I}, \mathcal{J}$ are two-sided and co-prime, all we can say is that

$$\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J} + \mathcal{J}\mathcal{I}.$$

Indeed, $a(x + y) = ax + ay \in \mathcal{J}\mathcal{I} + \mathcal{I}\mathcal{J}$ since $ax \neq xa$.

Finally, let us extend the notion of "modulo" to ideals.

Definition 3.14. If $a, b \in R$ and $\mathcal{I}$ is an ideal of R, we say that a is congruent to b modulo $\mathcal{I}$ if

$$a - b \in \mathcal{I}.$$

A last definition this time about rings is needed before we can state the theorem.

Definition 3.15. If $R_1, \ldots, R_n$ are rings, the direct product of $R_1, \ldots, R_n$, denoted by $\prod_{i=1}^{n} R_i$, is defined as the ring of n-tuples $(a_1, \ldots, a_n)$, $a_i \in R_i$, with componentwise addition and multiplication. The zero element is $(0, \ldots, 0)$ and the identity is $(1, \ldots, 1)$ where 1 means 1_{R_i} for each i.

This definition is an immediate generalization of the direct product we studied for groups.

Theorem 3.5. (Chinese Remainder Theorem). *Let R be a commutative ring, and let $\mathcal{I}_1, \ldots, \mathcal{I}_n$ be ideals in R, such that*

$$\mathcal{I}_i + \mathcal{I}_j = R, \ i \neq j.$$

1. *If $a_1, \ldots, a_n$ are elements of R, there exists an element $a \in R$ such that*

$$a \equiv a_i \mod \mathcal{I}_i, \ i = 1, \ldots, n.$$

2. *If b is another element of R such that $b \equiv a_i \mod \mathcal{I}_i$, $i = 1, \ldots, n$, then*

$$b \equiv a \mod \cap_{i=1}^{n} \mathcal{I}_i.$$

Conversely, if b satisfies the above congruence, then $b \equiv a_i \mod \mathcal{I}_i$, $i = 1, \ldots, n$.

3. *We have that*

$$R/\cap_{i=1}^{n} \mathcal{I}_i \simeq \prod_{i=1}^{n} R/\mathcal{I}_i.$$

Proof. 1. For $j > 1$, we have by assumption that $\mathcal{I}_1 + \mathcal{I}_j = R$, and thus there exist $b_j \in \mathcal{I}_1$ and $d_j \in \mathcal{I}_j$ such that

$$b_j + d_j = 1, \ j = 2, \ldots, n.$$

This yields that

$$\prod_{j=2}^{n} (b_j + d_j) = 1. \tag{3.1}$$

Now if we look at the left hand side of the above equation, we have

$$(b_2 + d_2)(b_3 + d_3) \cdots (b_n + d_n) = (\underbrace{b_2 b_3 + b_2 d_3 + d_2 b_3}_{\in \mathcal{I}_1} + d_2 d_3) \cdots (b_n + d_n)$$

and all the terms actually belong to $\mathcal{I}_1$, but $c_1 := \prod_{j=2}^n d_j \in \prod_{j=2}^n \mathcal{I}_j$. Thus

$$c_1 \equiv 1 \mod \mathcal{I}_1$$

from (3.1). On the other hand, we also have

$$c_1 \equiv 0 \mod \mathcal{I}_j$$

for $j > 1$ since $c_1 \in \prod_{j=2}^n \mathcal{I}_j$.

More generally, for all i, we can find c_i with

$$c_i \equiv 1 \mod \mathcal{I}_i,\ c_i \equiv 0 \mod \mathcal{I}_j,\ j \neq i.$$

Now take arbitrary elements $a_1, \ldots, a_n \in R$, and set

$$a = a_1 c_1 + \ldots + a_n c_n.$$

Let us check that a is the solution we are looking for. Since $c_j \equiv 0 \mod \mathcal{I}_j$,$j \neq i$, we have for a given i that

$$a \equiv a_i c_i \equiv a_i \mod \mathcal{I}_i$$

using that $c_i \equiv 1 \mod \mathcal{I}_i$.

2. We have just shown the existence of a solution a modulo $\mathcal{I}_i$ for $i = 1, \ldots, n$. We now discuss the question of unicity, and show that the solution is actually not unique, but any other solution than a is actually congruent to $a \mod \cap_{i=1}^n \mathcal{I}_i$.

   We have for all $i = 1, \ldots, n$ that

   $$b \equiv a_i \mod \mathcal{I}_i \iff b \equiv a \mod \mathcal{I}_i \iff b - a \equiv 0 \mod \mathcal{I}_i$$

   which finally is equivalent to

   $$b - a \in \cap_{i=1}^n \mathcal{I}_i.$$

3. Define the ring homomorphism $f : R \to \prod_{i=1}^n R/\mathcal{I}_i$, sending

   $$a \mapsto f(a) = (a + \mathcal{I}_1, \ldots, a + \mathcal{I}_n).$$

   - This map is surjective: take any $(a_1 + \mathcal{I}_1, \ldots, a_n + \mathcal{I}_n) \in \prod_{i=1}^n R/\mathcal{I}_i$, then we must find an $a \in R$ such that $f(a) = (a_1 + \mathcal{I}_1, \ldots, a_n + \mathcal{I}_n)$, that is $a + \mathcal{I}_i = a_i + \mathcal{I}_i$, or equivalently $a_i \equiv a \mod \mathcal{I}_i$, which is true by the first point.
   - Its kernel is given by

   $$\begin{aligned} \mathrm{Ker} f &= \{a \in R,\ f(a) = (\mathcal{I}_1, \ldots, \mathcal{I}_n)\} \\ &= \{a \in R,\ a \in \mathcal{I}_i,\ i = 1, \ldots, n\} \\ &= \prod_{i=1}^n \mathcal{I}_i. \end{aligned}$$

   We conclude using the first isomorphism Theorem for rings.

□

Example 3.7. If $R = \mathbb{Z}$, the Chinese Remainder Theorem simplifies to say that if $n = \prod_i n_i$ where the n_i are coprime, then

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_i \mathbb{Z}/n_i\mathbb{Z}.$$

In the particular case of Example 3.6, we have

$$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

This version of the Chinese remainder Theorem does not hold in the non-commutative case, because the property that $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$ does not hold anymore, as pointed out earlier. There is though a commutative version if all the co-prime ideals are assumed to be two-sided.

3.4 Maximal and prime ideals

Here are a few special ideals.

Definition 3.16. The ideal generated by the non-empty set X of R is the smallest ideal of R that contains X. It is denoted by $\langle X \rangle$. It is the collection of all finite sums of the form $\sum_i r_i x_i s_i$.

Definition 3.17. An ideal generated by a single element a is called a principal ideal, denoted by $\langle a \rangle$.

Definition 3.18. A maximal ideal in the ring R is a proper ideal that is not contained in any strictly larger proper ideal.

One can prove that every proper ideal is contained in a maximal ideal, and that consequently every ring has at least one maximal ideal. We skip the proof here, since it heavily relies on set theory, requires many new definitions and the use of Zorn's lemma.

Instead, let us mention that a correspondence Theorem exists for rings, the same way it exists for groups, since we will need it for characterizing maximal ideals.

Theorem 3.6. (Correspondence Theorem for rings). *If $\mathcal{I}$ is a two-sided ideal of a ring R, then the canonical map*

$$\pi : R \to R/\mathcal{I}$$

sets up a one-to-one correspondence between

- *the set of all subrings of R containing $\mathcal{I}$ and the set of all subrings of $R/\mathcal{I}$,*
- *the set of all ideals of R containing $\mathcal{I}$ and the set of all ideals of $R/\mathcal{I}$.*

Here is a characterization of maximal ideals in commutative rings.

Theorem 3.7. *Let M be an ideal in the commutative ring R. We have*

$$M \text{ maximal} \iff R/M \text{ is a field.}$$

Proof. Let us start by assuming that M is maximal. Since R/M is a ring, we need to find the multiplicative inverse of $a+M \in R/M$ assuming that $a+M \neq 0$ in R/M, that is $a \notin M$. Since M is maximal, the ideal $Ra + M$ has to be R itself, since $M \subset Ra + M$. Thus $1 \in Ra + M = R$, that is

$$1 = ra + m,\ r \in R,\ m \in M.$$

Then

$$(r + M)(a + M) = ra + M = (1 - m) + M = 1 + M$$

proving that $r + M$ is $(a + M)^{-1}$.

Conversely, let us assume that R/M is a field. First we notice that M must be a proper ideal of R, since if $M = R$, then R/M contains only one element and $1 = 0$.

Let N be an ideal of R such that $M \subset N \subset R$ and $N \neq R$. We have to prove that $M = N$ to conclude that M is maximal.

By the correspondence Theorem for rings, we have a one-to-one correspondence between the set of ideals of R containing M, and the set of ideals of R/M. Since N is such an ideal, its image $\pi(N) \in R/M$ must be an ideal of R/M, and thus must be either $\{0\}$ or R/M (since R/M is a field). The latter yields that $N = R$, which is a contradiction, letting as only possibility that $\pi(N) = \{0\}$, and thus $N = M$, which completes the proof. □

Definition 3.19. A prime ideal in a commutative ring R is a proper ideal P of R such that for any $a, b \in R$, we have that

$$ab \in P \Rightarrow a \in P \text{ or } b \in P.$$

Here is again a characterization of a prime ideal P of R in terms of its quotient ring R/P.

Theorem 3.8. *If P is an ideal in the commutative ring R*

$$P \text{ is a prime ideal} \iff R/P \text{ is an integral domain.}$$

Proof. Let us start by assuming that P is prime. It is thus proper by definition, and R/P is a ring. We must show that the definition of integral domain holds, namely that

$$(a + P)(b + P) = 0 + P \Rightarrow a + P = P \text{ or } b + P = P.$$

Since

$$(a + P)(b + P) = ab + P = 0 + P,$$

we must have $ab \in P$, and thus since P is prime, either $a \in P$ or $b \in P$, implying respectively that either $a + P = P$ or $b + P = P$.

Conversely, if R/P is an integral domain, then P must be proper (otherwise $1 = 0$). We now need to check the definition of a prime ideal. Let us thus consider $ab \in P$, implying that

$$(a + P)(b + P) = ab + P = 0 + P.$$

Since R/P is an integral domain, either $a + P = P$ or $b + P = P$, that is

$$a \in P \text{ or } b \in P,$$

which concludes the proof. □

Corollary 3.9. *In a commutative ring, a maximal ideal is prime.*

Proof. If M is maximal, then R/M is a field, and thus an integral domain, so that M is prime. □

Corollary 3.10. *Let $f : R \to S$ be an epimorphism of commutative rings.*

1. *If S is a field, then* $\mathrm{Ker} f$ *is a maximal ideal of R.*
2. *If S is an integral domain, then* $\mathrm{Ker} f$ *is a prime ideal of R.*

Proof. By the first isomorphism theorem for rings, we have that

$$S \simeq R/\mathrm{Ker} f.$$

□

Example 3.8. Consider the ring $\mathbb{Z}[X]$ of polynomials with coefficients in $\mathbb{Z}$, and the ideal generated by the indeterminate X, that is $\langle X \rangle$ is the set of polynomials with constant coefficient 0. Clearly $\langle X \rangle$ is a proper ideal. To show that it is prime, consider the following ring homomorphism:

$$\varphi : \mathbb{Z}[X] \to \mathbb{Z},\ f(X) \mapsto \varphi(f(X)) = f(0).$$

We have that $\langle X \rangle = \mathrm{Ker}\varphi$ which is prime by the above corollary.

3.5 Polynomial rings

For this section, we assume that R is a commutative ring. Set $R[X]$ to be the set of polynomials in the indeterminate X with coefficients in R. It is easy to see that $R[X]$ inherits the properties of ring from R.

We define the evaluation map E_x, which evaluates a polynomial $f(X) \in R[X]$ in $x \in R$, as

$$E_x : R[X] \to R,\ f(X) \mapsto f(X)|_{X=x} = f(x).$$

We can check that E_x is a ring homomorphism.

The degree of a polynomial is defined as usual, that is, if $p(X) = a_0 + a_1 X + \ldots + a_n X^n$ with $a_n \neq 0$, then $\deg(p(X)) = \deg p = n$. By convention, we set $\deg(0) = -\infty$.

Euclidean division will play an important role in what will follow. Let us start by noticing that there exists a polynomial division algorithm over $R[X]$, namely: if $f, g \in R[X]$, with g monic, then there exist unique polynomials q and r in $R[X]$ such that

$$f = qg + r, \ \deg r < \deg g.$$

The requirement that g is monic comes from R being a ring and not necessarily a field. If R is a field, g does not have to be monic, since one can always multiply g by the inverse of the leading coefficient, which is not possible if R is not a field.

Example 3.9. Take $f(X) = X^2 - 2$ and $g(X) = 2X - 1$. It is not possible to divide $f(X)$ by $g(X)$ in $\mathbb{Z}[X]$. If it were, then

$$f(X) = X^2 - 2 = (q_0 + q_1 X)(2X - 1) + r_0$$

and the coefficient of X^2 is 1 on the left hand side, and $2q_1$ on the right hand side. Now in $\mathbb{Z}$, there is no solution to the equation $2q_1 = 1$. Of course, this is possible in $\mathbb{Q}$, by taking $q_1 = 1/2$!

This gives the following:

Theorem 3.11. (Remainder Theorem). *If $f \in R[X]$, $a \in R$, then there exists a unique polynomial $q(X) \in R[X]$ such that*

$$f(X) = q(X)(X - a) + f(a).$$

Hence $f(a) = 0 \iff X - a \mid f(X)$.

Proof. Since $(X - a)$ is monic, we can do the division

$$f(X) = q(X)(X - a) + r(X).$$

But now since $\deg r < \deg(X - a)$, $r(X)$ must be a constant polynomial, which implies that

$$f(a) = r(X)$$

and thus

$$f(X) = q(X)(X - a) + f(a)$$

as claimed. Furthermore, we clearly have that

$$f(a) = 0 \iff X - a \mid f(X).$$

□

The following result sounds well known, care should be taken not to generalize it to rings which are not integral domain!

Theorem 3.12. *If R is an integral domain, then a non-zero polynomial f in $R[X]$ of degree n has at most n roots in R, counting multiplicity.*

Proof. If f has no root in $R[X]$, then we are done. Let us thus assume that f has a root a_1 in R, that is $f(a_1) = 0$. Then

$$X - a_1 \mid f(X)$$

by the remainder Theorem above, meaning that

$$f(X) = q_1(X)(X - a_1)^{n_1}$$

where $q_1(a_1) \neq 0$ and $\deg q_1 = n - n_1$ since R is an integral domain. Now if a_1 is the only root of f in R, then $n_1 \leq n$ and we are done. If not, consider similarly $a_2 \neq a_1$ another root of f, so that

$$0 = f(a_2) = q_1(a_2)(a_2 - a_1)^{n_1}.$$

Since R is an integral domain, we must have that $q_1(a_2) = 0$, and thus a_2 is a root of $q_1(X)$. We can repeat the process with $q_1(X)$ instead of $f(X)$: since a_2 is a root of $q_1(X)$, we have

$$q_1(X) = q_2(X)(X - a_2)^{n_2}$$

with $q_2(a_2) \neq 0$ and $\deg q_2 = n - n_1 - n_2$. By going on iterating the process, we obtain

$$\begin{aligned} f(X) &= q_1(X)(X - a_1)^{n_1} \\ &= q_2(X)(X - a_2)^{n_2}(X - a_1)^{n_1} \\ &= \dots \\ &= (X - a_1)^{n_1}(X - a_2)^{n_2} \cdots (X - a_k)^{n_k} \cdot c(X) \end{aligned}$$

where $c(X)$ is a polynomial with no root in R, possibly constant, and

$$n \geq n_1 + n_2 + \cdots + n_k.$$

Since R is an integral domain, the only possible roots of f are $a_1, \dots, a_k$, $k \leq n$, and the number of roots counting multiplicity is less than n. □

Example 3.10. Take $R = \mathbb{Z}_8$ the ring of integers modulo 8. Consider the polynomial

$$f(X) = X^3.$$

It is easy to check that is has 4 roots: $0, 2, 4, 6$. This comes from the fact that $\mathbb{Z}_8$ is not an integral domain.

3.6 Unique factorization and Euclidean division

In this section, all rings are assumed to be integral domains.

Let us start by defining formally the notions of irreducible and prime. The elements a, b, c, u in the definitions below all belong to an integral domain R.

Definition 3.20. The elements a, b are called associate if $a = ub$ for some unit u.

Definition 3.21. Let a be a non-zero element which is not a unit. Then a is said to be irreducible if $a = bc$ implies that either b or c must be a unit.

Definition 3.22. Let a be a non-zero element which is not a unit. Then a is called prime if whenever $a \mid bc$, then $a \mid b$ or $a \mid c$.

Between prime and irreducible, which notion is the stronger? The answer is in the proposition below.

Proposition 3.13. *If a is prime, then a is irreducible.*

Proof. Suppose that a is prime, and that $a = bc$. We want to prove that either b or c is a unit. By definition of prime, we must have that a divides either b or c. Let us say that a divides b. Thus

$$b = ad \Rightarrow b = bcd \Rightarrow b(1 - cd) = 0 \Rightarrow cd = 1$$

using that R is an integral domain, and thus c is a unit. The same argument works if we assume that a divides c, and we conclude that a is irreducible. □

Example 3.11. Consider the ring

$$R = \mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3},\ a, b \in \mathbb{Z}\}.$$

We want to see that 2 is irreducible but not prime.

- Let us first check that 2 is indeed irreducible. Suppose that

  $$2 = (a + ib\sqrt{3})(c + id\sqrt{3}).$$

  Since 2 is real, it is equal to its conjugate, and thus

  $$2\overline{2} = (a + ib\sqrt{3})(c + id\sqrt{3})(a - ib\sqrt{3})(c - id\sqrt{3})$$

  implies that

  $$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

  We deduce that $a^2 + 3b^2$ must divide 4, and it cannot possibly be 2, since we have a sum of squares in $\mathbb{Z}$. If $a^2 + 3b^2 = 4$, then $c^2 + 3d^2 = 1$ and $d = 0$, $c = \pm 1$. Vice versa if $c^2 + 3d^2 = 4$ then $a^2 + 3b^2 = 1$, and $b = 0$, $a = \pm 1$. In both cases we get that one of the factors of 2 is unit, namely ± 1.

- We now have to see that 2 is not a prime. Clearly

$$2 \mid (1+i\sqrt{3})(1-i\sqrt{3}) = 4.$$

  But 2 divides neither $1+i\sqrt{3}$ nor $1-i\sqrt{3}$.

We can see from the above example that the problem which arises is the lack of unique factorization.

Definition 3.23. A unique factorization domain (UFD) is an integral domain R satisfying that

1. every element $0 \neq a \in R$ can be written as a product of irreducible factors $p_1, \dots p_n$ up to a unit u, namely:

$$a = up_1 \dots p_n.$$

2. The above factorization is unique, that is, if

$$a = up_1 \dots p_n = vq_1 \dots q_m$$

   are two factorizations into irreducible factors p_i and q_j with units u, v, then $n = m$ and p_i and q_i are associate for all i.

We now prove that the distinction between irreducible and prime disappear in a unique factorization domain.

Proposition 3.14. *In a unique factorization domain R, we have that a is irreducible if and only if a is prime.*

Proof. We already know that prime implies irreducible. Let us show that now, we also have irreducible implies prime.

Take a to be irreducible and assume that $a \mid bc$. This means that $bc = ad$ for some $d \in R$. Using the property of unique factorization, we decompose d, b and c into products of irreducible terms (resp. d_i, b_i, c_i up to units u, v, w):

$$a \cdot ud_1 \cdots d_r = vb_1 \cdots b_s \cdot wc_1 \dots c_t.$$

Since the factorization is unique, a must be associate to some either b_i or c_i, implying that a divides b or c, which concludes the proof. □

We now want to connect the property of unique factorization to ideals.

Definition 3.24. Let $a_1, a_2, \dots$ be elements of an integral domain R. If the sequence of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

stabilizes, i.e., we have

$$(a_n) = (a_{n+1}) = \dots$$

for some n, then we say that R satisfies the ascending chain condition on principal ideals.

If the same condition holds but for general ideals, not necessarily principal, we call R a Noetherian ring, in honor of the mathematician Emmy Noether.

Figure 3.1: Amalie Emmy Noether (1882-1935)

Examples 3.12. 1. Consider the polynomial ring in infinitely many indeterminates $X_1, X_2, \ldots$ over $\mathbb{R}$. The chain

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \ldots$$

of non-principal ideals is ascending and does not terminate. The ideal generated by all indeterminates is maximal.

2. Consider the polynomial ring $\mathbb{Z} + X\mathbb{Q}[X]$ of all rational polynomials with integral constant term. The chain

$$(X) \subset (X/2) \subset (X/4) \subset \ldots$$

of principal ideals is ascending and does not terminate.

Theorem 3.15. *Let R be an integral domain.*

1. *If R is a UFD, then R satisfies the ascending chain condition on principal ideals.*
2. *If R satisfies the ascending chain condition on principal ideals, then every non-zero element of R can be factored into irreducible (this says nothing about the unicity of the factorization).*
3. *If R is such that every non-zero element of R can be factored into irreducible, and in addition every irreducible element is prime, then R is a UFD.*

Thus R is a UFD if and only if it satisfies the ascending chain condition on principal ideals and every irreducible element of R is prime.

Proof. 1. Recall that in a UFD, prime and irreducible are equivalent. Consider an ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

We have that $a_{i+1} \mid a_i$ for all i. Thus the prime factors of a_{i+1} consist of some (possibly all) prime factors of a_i. Since a_1 has a unique factorization into finitely many prime factors, the prime factors will end up being the same, and the chain will stabilize.

2. Take $0 \neq a_1 \in R$. If a_1 is irreducible, we are done. Let us thus assume that a_1 is not irreducible, that is

$$a_1 = a_2 b_2$$

where a_2 and b_2 are not unit. Since $a_2 \mid a_1$, we have $(a_1) \subseteq (a_2)$, and actually

$$(a_1) \subsetneq (a_2).$$

Indeed, if $(a_1) = (a_2)$, then a_2 would be a multiple of a_1, namely $a_2 = ca_1$ and thus

$$a_1 = a_2 b_2 \Rightarrow a_1 = c a_1 b_2 \Rightarrow a_1(1 - cb_2) = 0$$

implying that $cb_2 = 1$ and thus b_2 is a unit. This contradicts the assumption that a_1 is not irreducible. This computation has shown us that whenever we get a factor which is not irreducible, we can add a new principal ideal to the chain of ideals. Thus, if $a_2 b_2$ is a product of irreducible, we are done. Otherwise, we have that say a_2 is not irreducible, and $a_2 = a_3 b_3$, yielding

$$(a_1) \subsetneq (a_2) \subsetneq (a_3).$$

Since R satisfies the ascending chain condition on principal ideals, this process cannot go on and must stop, showing that we have a factorization into irreducible.

3. We now know that R allows a factorization into irreducible. We want to prove that this factorization is unique, under the assumption that every irreducible is prime. Suppose thus that

$$a = u p_1 p_2 \cdots p_n = v q_1 q_2 \cdots q_m$$

where u, v are units and p_i, q_j are irreducible. p_1 is an irreducible but also a prime by assumption, thus it must divide one of the q_j, say q_1, and we have $q_1 = p_1 d$. Since q_1 is irreducible, d must be a unit, and q_1 and p_1 are associate. We can iterated the process to find that q_i and p_i are associate for all i.

□

We now introduce a notion stronger than being a unique factorization domain.

Definition 3.25. A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Theorem 3.16. *A principal ideal domain R is a unique factorization domain.*

Proof. What we will prove is that if R is a principal ideal domain, then

- R satisfies the ascending chain condition on principal ideals.
- every irreducible in R is also prime.

Having proved these two claims, we can conclude using the above theorem.

Let us first prove that R satisfies the ascending chain condition on principle ideals. Consider the following sequence of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \dots$$

and let $\mathcal{I} = \cup_{i=1}^{\infty}(a_i)$. Note that $\mathcal{I}$ is an ideal of R (be careful, a union of ideals is not an ideal in general!). Indeed, we have that $\mathcal{I}$ is closed under addition: take $a, b \in \mathcal{I}$, then there are ideals (a_j) and (a_k) in the chain with $a \in (a_j)$ and $b \in (a_k)$. If $m \geq \max(j, k)$, then both $a, b \in (a_m)$ and so do $a+b$. To check that $\mathcal{I}$ is closed under multiplication by an element of R, take again $a \in \mathcal{I}$. Then $a \in (a_j)$ for some j. If $r \in R$, then $ra \in (a_j)$ implying that $ra \in \mathcal{I}$.

Now by assumption, $\mathcal{I}$ is a principal ideal, generated by, say b: $\mathcal{I} = (b)$. Since b belongs to $\cup_{i=1}^{\infty}(a_i)$, it must belongs to some (a_n). Thus $\mathcal{I} = (b) \subseteq (a_n)$. For $j \geq n$, we have

$$(a_j) \subseteq \mathcal{I} \subseteq (a_n) \subseteq (a_j)$$

which proves that the chain of ideal stabilizes.

We are left to prove that every irreducible element is also prime. Let thus a be an irreducible element. Consider the principal ideal (a) generated by a. Note that (a) is a proper ideal: if $(a) = R$, then $1 \in (a)$ and thus a is a unit, which is a contradiction.

We have that (a) is included in a maximal ideal $\mathcal{I}$ (this can be deduced from either the ascending chain condition or from the theorem (Krull's theorem) that proves that every ideal is contained in a maximal ideal). Since R is a principal ideal domain, we have that $\mathcal{I} = (b)$. Thus

$$(a) \subseteq (b) \Rightarrow b \mid a \Rightarrow a = bd$$

where a is irreducible, b cannot be a unit (since $\mathcal{I}$ is by definition of maximal ideal a proper ideal), and thus d has to be a unit of R. In other words, a and b are associate. Thus

$$(a) = \mathcal{I} = (b).$$

Since $\mathcal{I}$ is a maximal ideal, it is prime implying that a is prime, which concludes the proof. □

Determining whether a ring is a principal ideal domain is in general quite a tough question. It is still an open conjecture (called Gauss's conjecture) to decide whether there are infinitely many real quadratic fields which are principal (we use the terminology "principal" for quadratic fields by abuse of notation, it actually refers to their ring of integers, that is rings of the form either $\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or $3 \mod 4$ or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ else).

One way mathematicians have found to approach this question is to actually prove a stronger property, namely whether a ring R is Euclidean.

Definition 3.26. Let R be an integral domain. We say that R is a Euclidean domain if there is a function Ψ from $R\backslash\{0\}$ to the non-negative integers such that

$$a = bq + r,\ a, b \in R,\ b \neq 0,\ q, r \in R$$

where either $r = 0$ or $\Psi(r) < \Psi(b)$.

When the division is performed with natural numbers, it is clear what it means that $r < b$. When we work with polynomials instead, we can say that $\deg r < \deg b$. The function Ψ generalizes these notions.

Theorem 3.17. *If R is a Euclidean domain, then R is a principal ideal domain.*

Proof. Let $\mathcal{I}$ be an ideal of R. If $\mathcal{I} = \{0\}$, it is principal and we are done. Let us thus take $\mathcal{I} \neq \{0\}$. Consider the set

$$\{\Psi(b),\ b \in \mathcal{I},\ b \neq 0\}.$$

It is included in the non-negative integers by definition of Ψ, thus it contains a smallest element, say n. Let $0 \neq b \in \mathcal{I}$ such that $\Psi(b) = n$.

We will now prove that $\mathcal{I} = (b)$. Indeed, take $a \in \mathcal{I}$, and compute

$$a = bq + r$$

where $r = 0$ or $\Psi(r) < \Psi(b)$. This yields

$$r = a - bq \in \mathcal{I}$$

and $\Psi(r) < \Psi(b)$ cannot possibly happen by minimality of n, forcing r to be zero. This concludes the proof. □

Example 3.13. Consider the ring

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$$

with

$$\Psi(a + b\sqrt{d}) = |a^2 - b^2 d|.$$

We will show that we have a Euclidean domain for $d = -2, -1, 2$.

Note that $\mathbb{Z}[\sqrt{d}]$ is an integral domain. Take $\alpha, \beta \neq 0$ in $\mathbb{Z}[\sqrt{d}]$. Now we would like to perform the division of α by β to get something of the form

$$\alpha = \beta q + r,\ q, r \in \mathbb{Z}[\sqrt{d}].$$

Since $\mathbb{Z}[\sqrt{d}]$ is not a field, there is no reason for this division to give a result in $\mathbb{Z}[\sqrt{d}]$ (that is, $q, r \in \mathbb{Z}[\sqrt{d}]$), however, we can compute the division in $\mathbb{Q}(\sqrt{d})$:

$$\alpha/\beta = q',$$

with $q' = x + \sqrt{d}y$ with x, y rational. Let us now approximate x, y by integers x_0, y_0, namely take x_0, y_0 such that

$$|x - x_0| \leq 1/2, \ |y - y_0| \leq 1/2.$$

Take

$$q = x_0 + y_0\sqrt{d}, \ r = \beta((x - x_0) + (y - y_0)\sqrt{d}),$$

where clearly $q \in \mathbb{Z}[\sqrt{d}]$, then

$$\begin{aligned} \beta q + r &= \beta(x_0 + y_0\sqrt{d}) + \beta((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \beta(x + y\sqrt{d}) = \beta q' = \alpha, \end{aligned}$$

which at the same time shows that $r \in \mathbb{Z}[\sqrt{d}]$. We are left to show that $\Psi(r) < \Psi(\beta)$. We have

$$\begin{aligned} \Psi(r) &= \Psi(\beta)\Psi((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| \\ &\leq \Psi(\beta)[|x - x_0|^2 + |d||y - y_0|^2] \\ &\leq \Psi(\beta)\left(\frac{1}{4} + |d|\frac{1}{4}\right) \end{aligned}$$

showing that $\mathbb{Z}[\sqrt{d}]$ is indeed a Euclidean domain for $d = -2, -1, 2$.

Below is a summary of the ring hierarchy (recall that PID and UFD stand respectively for principal ideal domain and unique factorization domain):

integral domains $\supset$ UFD $\supset$ PID $\supset$ Euclidean domains

Note that though the Euclidean division may sound like an elementary concept, as soon as the ring we consider is fancier than $\mathbb{Z}$, it becomes quickly a difficult problem. We can see that from the fact that being Euclidean is stronger than being a principal ideal domain. All the inclusions are strict, since one may check that $\mathbb{Z}[\sqrt{-3}]$ is an integral domain but is not a UFD, $\mathbb{Z}[X]$ is a UFD which is not PID, while $\mathbb{Z}[(1 + i\sqrt{19})/2]$ is a PID which is not a Euclidean domain.

ring	ED	PID	UFD	ID
$\mathbb{Z}$	yes	yes	yes	yes
$F[X]$, F a field	yes	yes	yes	yes
$\mathbb{Z}[i]$	yes	yes	yes	yes
$\mathbb{Z}[\sqrt{\pm 2}]$	yes	yes	yes	yes
$\mathbb{Z}[\sqrt{3}]$	yes	yes	yes	yes
$\mathbb{Z}[(1+i\sqrt{19})/2]$	no	yes	yes	yes
$\mathbb{Z}[X]$	no	no	yes	yes
$\mathbb{Z}[\sqrt{-3}]$	no	no	no	yes

Table 3.1: Examples of rings we saw: that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain is done in the exercises, that $\mathbb{Z}[X]$ is not a principal ideal domain is also shown in the exercises, it is enough to show that the ideal $\langle 2, X\rangle$ is not principal. Finally $\mathbb{Z}[\sqrt{-3}]$ is not a unique factorization domain because we saw that 2 is irreducible but not prime.

3.7 Irreducible polynomials

Recall the definition of irreducible that we have seen: a non-zero element a which is not a unit is said to be irreducible if $a = bc$ implies that either b or c is a unit. Let us focus on the case where the ring is a ring of polynomials $R[X]$ and R is an integral domain.

Definition 3.27. If R is an integral domain, then an irreducible element of $R[X]$ is called an irreducible polynomial.

In the case of a field F, then units of $F[X]$ are non-zero elements of F. Then we get the more familiar definition that an irreducible element of $F[X]$ is a polynomial of degree at least 1, that cannot be factored into two polynomials of lower degree.

Let us now consider the more general case where R is an integral domain (thus not necessarily a field, it may not even be a unique factorization domain). To study when polynomials over an integral domain R are irreducible, it is often more convenient to place oneselves in a suitable field that contains R, since division in R can be problematic. To do so, we will now introduce the field of fractions, also called quotient field, of R. Since there is not much more difficulty in treating the general case, that is, when R is a commutative ring, we present this construction.

Let S be a subset of R which is closed under multiplication, contains 1 and does not contain 0. This definition includes the set of all non-zero elements of an integral domain, or the set of all non-zero elements of a commutative ring that are not zero divisors. We define the following equivalence relation on $R \times S$:

$$(a, b) \sim (c, d) \iff s(ad - bc) = 0 \text{ for some } s \in S.$$

It is clearly reflexive and symmetric. Let us check the transitivity. Suppose that

$(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then

$$s(ad - bc) = 0 \text{ and } t(cf - de) = 0$$

for some $s, t \in S$. We can now multiply the first equation by tf, the second by sb and add them

$$stf(ad - bc) + tsb(cf - de) = 0$$

to get

$$sdt(fa - be) = 0$$

which proves the transitivity.

What we are trying to do here is to mimic the way we deal with $\mathbb{Z}$. If we take non-zero $a, b, c, d \in \mathbb{Z}$, we can write down $a/b = c/d$, or equivalently $ad = bc$, which is also what $(a, b) \sim (c, d)$ satisfies by definition if we take R to be an integral domain. In a sense, (a, b) is some approximation of a/b.

Formally, if $a \in R$ and $b \in S$, we define the fraction a/b to be the equivalence class of the pair (a, b). The set of all equivalence classes is denoted by $S^{-1}R$. To make it into a ring, we define the following laws in a natural way:

- addition:
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$
- multiplication:
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$
- additive identity:
$$\frac{0}{1} = \frac{0}{s},\ s \in S.$$
- additive inverse:
$$-\frac{a}{b} = \frac{-a}{b}.$$
- multiplicative identity:
$$\frac{1}{1} = \frac{s}{s},\ s \in S.$$

To prove that we really obtain a ring, we need to check that all these laws are well-defined.

Theorem 3.18. *With the above definitions, the set of equivalence classes $S^{-1}R$ is a commutative ring.*

1. *If R is an integral domain, so is $S^{-1}R$.*
2. *If R is an integral domain, and $S = R\backslash\{0\}$, then $S^{-1}R$ is a field.*

Proof. **Addition is well-defined.** If $a_1/b_1 = c_1/d_1$ and $a_2/b_2 = c_2/d_2$, then for some $s, t \in S$, we have

$$s(a_1d_1 - b_1c_1) = 0 \text{ and } t(a_2d_2 - b_2c_2) = 0.$$

We can now multiply the first equation by tb_2d_2 and the second by sb_1d_1 to get

$$tb_2d_2s(a_1d_1 - b_1c_1) = 0 \text{ and } sb_1d_1t(a_2d_2 - b_2c_2) = 0,$$

and adding them yields

$$st[d_2d_1(b_2a_1 + b_1a_2) - b_2b_1(d_2c_1 + d_1c_2)] = 0$$

that is

$$\frac{b_2a_1 + b_1a_2}{b_2b_1} = \frac{d_2c_1 + d_1c_2}{d_2d_1},$$

which can be rewritten as

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{c_1}{d_1} + \frac{c_2}{d_2}$$

and we conclude that addition does not depend on the choice of a representative in an equivalence class.

Multiplication is well-defined. We start as before. If $a_1/b_1 = c_1/d_1$ and $a_2/b_2 = c_2/d_2$, then for some $s, t \in S$, we have

$$s(a_1d_1 - b_1c_1) = 0 \text{ and } t(a_2d_2 - b_2c_2) = 0.$$

Now we multiply instead the first equation by ta_2d_2, the second by sc_1b_1 and we add them:

$$st[a_2d_2a_1d_1 - c_1b_1b_2c_2] = 0.$$

This implies, as desired, that

$$\frac{a_1a_2}{b_1b_2} = \frac{c_1c_2}{d_1d_2}.$$

To be complete, one should check that the properties of a ring are fulfilled, but this follows from the fact that addition and multiplication are carried the usual way.

1. We want to prove that $S^{-1}R$ is an integral domain. We assume that R is an integral domain, and we need to check the definition of an integral domain for $S^{-1}R$. Namely, suppose that $(a/b)(c/d) = 0$ in $S^{-1}R$, that is

$$\frac{a}{b}\frac{c}{d} = \frac{0}{1}.$$

This means that $(ac, bd) \sim (0, 1)$ and $acs = 0$ for some $s \in S$. Now $acs = 0$ is an equation in R, which is an integral domain, and $s \neq 0$, thus $ac = 0$, so either a or c is 0, and consequently either a/b or c/d is zero.

2. To conclude, we want to prove that $S^{-1}R$ is a field, assuming that R is an integral domain, and $S = R\backslash\{0\}$. We consider a/b a non-zero element of $S^{-1}R$, for which we need to find an inverse. Note that a and b are non-zero, thus they are both in S meaning that both a/b and b/a are in $S^{-1}R$ and b/a is the multiplicative inverse of a/b.

□

Definition 3.28. Let R be a commutative ring. Based on the above, the set of equivalence classes $S^{-1}R$ is a commutative ring, called the ring of fractions of R by S. If R is an integral domain, and $S = R\backslash\{0\}$, then $S^{-1}R$ is called the field of fractions or quotient field of R.

Now that we have defined a suitable field, we are left to prove that we can embed an integral domain R in its quotient field.

Proposition 3.19. *A commutative ring R can be embedded in its ring of fractions $S^{-1}R$, where S is the set of all its non-divisors of zero. In particular, an integral domain can be embedded in its quotient field, which is furthermore the smallest field containing R.*

Proof. Consider the following map:

$$f : R \to S^{-1}R,\ a \mapsto f(a) = a/1.$$

It is not hard to check that f is a ring homomorphism. If S has no zero divisor, we have that the kernel of f is given by the set of a such that $f(a) = a/1 = 0/1$, that is the set of a such that $sa = 0$ for some s. Since s is not a zero divisor, we have $a = 0$ and f is a monomorphism. □

Let us get back to the irreducible polynomials, and consider now the case where D is a unique factorization domain. It is not necessarily a field, but we now know how to embed it in a suitable field, namely its field of fractions, or quotient field. Take the polynomial $f(X) = a + abX$, $a \neq 0$ not a unit. Since we can factor it as

$$f(X) = a(1 + bX)$$

where a is not a unit by assumption, this polynomial is not irreducible. But we do not really have a factorization into two polynomials of lower degree. What happens here is that the constant polynomials are not necessarily units, unlike in the case of fields. To distinguish this case, we introduce the notion of primitive polynomial.

Definition 3.29. Let D be a unique factorization domain and let $f \in D[X]$. We call the greatest common divisor of all the coefficients of f the content of f, denoted by $c(f)$. A polynomial whose content is a unit is called a primitive polynomial.

Figure 3.2: Carl Friedrich Gauss (1777-1855)

We can now rule out the above example, and we will prove later that this allows us to say that a primitive polynomial is irreducible if and only if it cannot be factored into two polynomials of lower degree. Be careful however that "primitive polynomial" has a different meaning if it is defined over a field.

The next goal is to prove Gauss lemma, which in particular implies that the product of two primitive polynomials is a primitive polynomial.

We start with a lemma.

Lemma 3.20. *Let D be a unique factorization domain, and consider $f \neq 0, g, h \in D[X]$ such that $pf(X) = g(X)h(X)$ with p a prime. Then either p divides all the coefficients of g or p divides all the coefficients of h.*

Before starting the proof, let us notice that this lemma is somehow a generalization of the notion of prime. Instead of saying that $p|ab$ implies $p|a$ or $p|b$, we have $p|g(X)h(X)$ implies that $p|g(X)$ or $p|h(X)$ (dividing the whole polynomial means dividing all of its coefficients).

Proof. Denote

$$g(X) = g_0 + g_1X + \ldots + g_sX^s,\ h(X) = h_0 + h_1X + \ldots + h_tX^t.$$

Suppose by contradiction that p does not divide all coefficients of g and does not divide all coefficients of h either. Then let g_u and h_v be the coefficients of minimum index not divisible by p. Then the coefficient of X^{u+v} in $g(X)h(X)$ is

$$g_0h_{u+v} + g_1h_{u+v-1} + \ldots + g_uh_v + \ldots + g_{u+v-1}h_1 + g_{u+v}h_0.$$

By definition of u and v, p divides every term but g_uh_v, thus p cannot possibly divide the entire expression, and thus there exists a coefficient of $g(X)h(X)$ not divisible by p. This contradicts the fact that $p|g(X)h(X)$. □

Proposition 3.21. (Gauss Lemma). *Let f, g be non-constant polynomials in $D[X]$ where D is a unique factorization domain. The content of a product of polynomials is the product of the contents, namely*

$$c(fg) = c(f)c(g),$$

up to associates. In particular, the product of two primitive polynomials is primitive.

Proof. Let us start by noticing that by definition of content, we can rewrite

$$f(X) = c(f)f^*(X),\ g(X) = c(g)g^*(X),$$

where $f^*, g^* \in D[X]$ are primitive. Clearly

$$fg = c(f)c(g)f^*g^*.$$

Since $c(f)c(g)$ divides fg, it divides every coefficient of fg and thus their greatest common divisor:

$$c(f)c(g) \mid c(gf).$$

We now prove the converse, namely that $c(gf)| \ |c(g)c(g)$. To do that, we consider each prime p appearing in the factorization of $c(gf)$ and argue that $p \mid c(f)c(g)$. Let thus p be a prime factor of $c(gf)$. Since $fg = c(fg)(fg)^*$, we have that $c(fg)$ divides fg, that is

$$p \mid fg.$$

By the above lemma, either $p \mid f$ or $p \mid g$, say $p \mid f = c(f)f^*$, meaning that either $p \mid c(f)$ or $p \mid f^*$. Since f^* is primitive, p cannot possibly divide f^*, and thus

$$p \mid c(f) \Rightarrow p \mid c(f)c(g).$$

If p appears with multiplicity, we iterate the reasoning with the same p. □

We are now ready to connect irreducibility over a unique factorization domain and irreducibility over the corresponding quotient field or field of fractions.

Proposition 3.22. *Let D be a unique factorization domain with quotient field F. If f is a non-constant polynomial in $D[X]$, then f is irreducible over D if and only if f is primitive and f is irreducible over F.*

For example, this says that f is irreducible over $\mathbb{Z}$ if and only if f is primitive, and f is irreducible over $\mathbb{Q}$.

Proof. First assume that f is irreducible over D.

f **is primitive.** Indeed, if f were not primitive, then we could write

$$f = c(f)f^*,$$

where $c(f)$ denotes the content of f and f^* is primitive. Since we assume f is not primitive, its content cannot be a unit, which contradicts the irreducibility of f over D, and we conclude that f is primitive.

f is irreducible over F. Again assume by contradiction that f is not irreducible over F. Now F is a field, thus reducible means f can be factored into a product of two non-constant polynomials in $F[X]$ of smaller degree:

$$f(X) = g(X)h(X), \ \deg g < \deg f, \ \deg h < \deg f.$$

Since g, h are in $F[X]$, and F is the field of fractions of D, we can write

$$g(X) = \frac{a}{b}g^*(X), \ h(X) = \frac{c}{d}h^*(X), \ a, b, c, d \in D$$

and g^*, h^* primitive. Thus

$$f(X) = \frac{ac}{bd}g^*(X)h^*(X)$$

where g^*h^* is a primitive polynomial by Gauss Lemma. Since we have already proven (in the 1st part) that f is primitive, it must be that $ac/bd = u$ is a unit. But this would mean that

$$f(X) = ug^*(X)h^*(X)$$

which contradicts the fact that $f(X)$ is irreducible over $D[X]$ and we conclude that f is also irreducible over $F[X]$.

We are left to prove the converse. Let then f be a primitive and f be an irreducible polynomial over F. We do it by contraction, and assume that the primitive polynomial f is not irreducible over D:

$$f(X) = g(X)h(X).$$

Since f is primitive, $\deg g$ and $\deg h$ are at least 1. But then neither g not h can be a unit in $F[X]$ (these are units in F) and thus

$$f = gh$$

contradicts the irreducibility of f over F. □

In other words, we have proven that f irreducible over D is equivalent to f primitive and cannot be factored into two polynomials of lower degree in $F[X]$.

To conclude, we present a practical criterion to decide whether a polynomial in $D[X]$ is irreducible over F.

Proposition 3.23. (Eisenstein's criterion). *Let D be a unique factorization domain, with quotient field F and let*

$$f(X) = a_nX^n + \ldots + a_1X + a_0$$

be a polynomial in $D[X]$ with $n \geq 1$ and $a_n \neq 0$.

If p is a prime in D and p divides a_i, $0 \leq i < n$ but p does not divide a_n nor does p^2 divide a_0, then f is irreducible over F.

Figure 3.3: Ferdinand Eisenstein (1823-1852)

Proof. We first divide f by its content, to get a primitive polynomial. By the above proposition, it is enough to prove that this primitive polynomial is irreducible over D.

Let thus f be a primitive polynomial and assume by contradiction it is reducible, that is

$$f(X) = g(X)h(X)$$

with

$$g(X) = g_0 + \ldots + g_r X^r,\ h(X) = h_0 + \ldots + h_s X^s.$$

Notice that r cannot be zero, for if $r = 0$, then $g_0 = g$ would divide f and thus all a_i implying that g_0 divides the content of f and is thus a unit. But this would contradict the fact that f is reducible. We may from now on assume that

$$r \geq 1,\ s \geq 1.$$

Now by hypothesis, $p \mid a_0 = g_0 h_0$ but p^2 does not divide a_0, meaning that p cannot divide both g_0 and h_0. Let us say that

$$p \mid g_0$$

and p does not divide h_0 (and vice-versa).

By looking at the dominant coefficient $a_n = g_r h_s$, we deduce from the assumption that p does not divide a_n that p cannot possibly divide g_r. Let i be the smallest integer such that p does not divide g_i. Then

$$1 \leq i \leq r < n = r + s.$$

Let us look at the ith coefficient

$$a_i = g_0 h_i + g_1 h_{i-1} + \ldots + g_i h_0$$

and by choice of i, p must divide $g_0, \ldots, g_{i-1}$. Since p divides a_i by assumption, it thus must divide the last term $g_i h_0$, and either $p \mid g_i$ or $p \mid h_0$ by definition of prime. Both are impossible: we have chosen p dividing neither h_0 nor g_i. This concludes the proof. □

The main definitions and results of this chapter are

- **(2.1-2.2).** Definitions of: ring, zero divisor, unit, integral domain, division ring, subring, characteristic, ring homomorphism, ideal, quotient ring. Factor and 1st Isomorphism Theorem for rings.
- **(2.3-2.4).** Operations on ideals, Chinese Remainder Theorem, Correspondence Theorem for rings. Definitions of: principal ideal, maximal ideal, prime ideal, the characterization of the two latter in the commutative case.
- **(2.5).** Polynomial Euclidean division, number of roots of a polynomial.
- **(2.6).** Definitions of: associate, prime, irreducible, unique factorization domain, ascending chain condition, principal ideal domain, Euclidean domain. Connections between prime and irreducible. Hierarchy among UFD, PID and Euclidean domains.
- **(2.7).** Construction of ring of fractions. Definitions of: content of a polynomial, primitive polynomial. Gauss Lemma, Eisenstein's criterion.

Chapter 4

Exercises on Ring Theory

Exercises marked by (*) are considered difficult.

4.1 Rings, ideals and homomorphisms

Exercise 56. Let R be a ring and $x \in R$. Suppose there exists a positive integer n such that $x^n = 0$. Show that $1 + x$ is a unit, and so is $1 - x$.

Answer. The element $1 - x$ is a unit since

$$(1 - x)(1 + x + \ldots + x^{n-1}) = 1.$$

The element $1 + x$ is a unit since

$$(1 + x)(1 - x + x^2 - x^3 \ldots \pm x^{n-1}) = 1.$$

Exercise 57. Let R be a commutative ring, and I be an ideal of R. Show that

$$\sqrt{I} := \{x \in R \mid \text{ there exists } m \in \mathbb{N}^* \text{ such that } x^m \in I\}$$

is an ideal of R. **Answer.**

- Clearly, $0 \in \sqrt{I}$. If $a \in \sqrt{I}$, then $a^m \in I$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m \in I$, so $-a \in \sqrt{I}$. Now let $a, b \in \sqrt{I}$, so $a^n \in I$ for some $n \geq 1$ and $b^m \in I$ for some $m \geq 1$. Now let us show that $(a + b)^{n+m} \in I$. We have $(a + b)^{n+m} = \sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n + m - j \geq m$, so $b^{n+m-j} \in I$ in this case (since $b^m \in I \Rightarrow b^i \in I$ for $i \geq m$). If $n + 1 \leq j \leq n + m$, we have $j \geq n + 1$, so $a^j \in I$ in this case (since $a^n \in I \Rightarrow a^i \in I$ for $i \geq n$). Therefore all the terms in the previous sum are in I and thus $(a+b)^{n+m} \in I$. Hence $a+b \in \sqrt{I}$. We just proved that $\sqrt{I}$ is an additive subgroup of R.

- Now we have to check the second property. Let $a \in \sqrt{I}$, and $r \in R$. We have $a^n \in I$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n \in I$ and therefore $ar \in \sqrt{I}$. Therefore $\sqrt{I}$ is an ideal of R.

Exercise 58. Determine all rings of cardinality p and characteristic p.

Answer. Let R be a ring of characteristic p. Consider the ring homomorphism: $\varphi : \mathbb{Z} \to R$, the characteristic of R is the natural number p such that $p\mathbb{Z}$ is the kernel of φ. We can now factorize φ in an injective map $\mathbb{Z}/p\mathbb{Z} \to R$. If now we further assume that R has cardinality p, we have that $\mathbb{Z}/p\mathbb{Z}$ and R have same cardinality, and thus we have an isomorphism. This means that the only ring of cardinality and characteristic p is $\mathbb{Z}/p\mathbb{Z}$.

Exercise 59. Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Prove that $Nil(R)$ is an ideal of R.

2. Show that if $r \in Nil(R)$, then $1 - r$ is invertible in R.

3. Show, with a counter-example, that $Nil(R)$ is not necessarily an ideal anymore if R is not commutative.

1. - Clearly, $0 \in Nil(R)$. If $a \in Nil(R)$, then $a^m = 0$ for some $m \geq 1$. Then $(-a)^m = (-1)^m a^m = 0$, so $-a \in Nil(R)$. Now let $a, b \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$ and $b^m = 0$ for some $m \geq 1$. Now let us show that $(a+b)^{n+m} = 0$. We have $(a+b)^{n+m} = \sum_{j=0}^{n+m} \frac{n!}{j!(n+m-j)!} a^j b^{n+m-j}$ (because R is commutative). Now if $0 \leq j \leq n$, we have $n+m-j \geq m$, so $b^{n+m-j} = 0$ in this case (since $b^m = 0 \Rightarrow b^i = 0$ for $i \geq m$). If $n+1 \leq j \leq n+m$, we have $j \geq n+1$, so $a^j = 0$ in this case (since $a^n = 0 \Rightarrow a^i = 0$ for $i \geq n$). Therefore all the terms in the previous sum are 0 and thus $(a+b)^{n+m} = 0$. Hence $a + b \in Nil(R)$. We just proved that $Nil(R)$ is an additive subgroup of R.
   - Now we have to check the second property. Let $a \in Nil(R)$, and $r \in R$. We have $a^n = 0$ for some $n \geq 1$. Now $(ar)^n = a^n r^n$ because R is commutative, so $(ar)^n = 0$ and therefore $ar \in Nil(R)$. Therefore $Nil(R)$ is an ideal of R.

2. If $r \in Nil(R)$, then $r^m = 0$ for some $m \geq 1$. Then $1 + r + r^2 + \cdots + r^{m-1}$ is the inverse of $1 - r$ since

$$(1-r)(1+r+r^2+\cdots+r^{m-1}) = 1+r+r^2+\cdots+r^{m-1}-r-r^2+\cdots+r^m = 1-r^m = 1.$$

3. If $R = M_2(\mathbb{C})$, let $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $a^2 = b^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so $a, b \in Nil(R)$, but $a + b$ does not lie in $Nil(R)$, since $(a + b)^2 = I_2$, and $I_2^n = I_2$ for all $n \geq 1$.

Exercise 60. Determine whether the following maps are ring homomorphisms:

1. $f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_1(x) = x + 1$.
2. $f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ with $f_2(x) = x^2$.
3. $f_3 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_3(x) = 4x$.
4. $f_4 : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ with $f_4(x) = 6x$.

Answer.

1. Since $f_1(0) = 1$, f_1, f cannot be a ring homomorphism.
2. Since $f_2(x + y) = x^2 + y^2 + 2xy \neq x^2 + y^2 = f_2(x) + f_2(y)$, f_2 cannot be a ring homomorphism.
3. Since $f_3(xy) = 4xy \neq xy = f_3(x)f_3(y)$, f_3 cannot be a ring homomorphism.
4. Since $f_4(1) \neq 1$, f_4 cannot be a ring homomorphism!

Exercise 61. Let K be a division ring with center k.

1. Show that the center of the polynomial ring $K[X]$ is $k[X]$.
2. For any a in $K \backslash k$, show that the ideal generated by $X - a$ in $K[X]$ is in fact the whole ring $K[X]$.
3. Show that any ideal $I \subseteq K[X]$ has the form $K[X]h$ where $h \in k[X]$.

Answer.

1. Clearly $k[X]$ is in the center. Conversely, if $f = \sum a_i X^i$ is in the center, then $fa = af$ for all $a \in K$, showing that $a_i \in k$.
2. Fix $b \in K$ such that $ab \neq ba$. Then the ideal generated by $X - a$ contains
$$b(X - a) - (X - a)b = ab - ba \in K$$
since $ab \neq ba$ so $(X - a) = R$.
3. We may assume $I \neq 0$ and fix a monic polynomial of the least degree in I. By the usual Euclidean algorithm argument, we have that $I = K[X]h$. For any $a \in K$, we have $ha \in I = K[X]h$ so $ha = rh$ for some r in $K[X]$. By comparing the leading terms, we see that $r \in K$ and in fact $r = a$. Thus $ha = ah$ for any $a \in K$, which means that $h \in k[X]$.

Exercise 62. Consider the ring $\mathcal{M}_n(\mathbb{R})$ of real $n \times n$ matrices. Are the trace and the determinant ring homomorphisms?

Answer. The trace is not multiplicative, since

$$2 = \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \cdot \mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 4.$$

The determinant is not additive:

$$4 = \det\left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\right) \neq \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) + \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 2.$$

Thus none of them are ring homomorphisms.

4.2 Quotient rings

Exercise 63. Compute the characteristic of the following rings R:

1. $R = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$,
2. $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$,
3. $R = \mathbb{Z}[j]/(2 - 5j)$, where j denotes a primitive 3rd root of unity ($j^3 = 1$ but $j^2 \neq 1$).

Answer. In this exercise, we use the notation $\overline{x}$ to denote an element in the quotient group involved.

1. For $1 \leq m \leq n-1$, we have $m \cdot \overline{1} = \overline{m} \neq 0$, since m is not a multiple of n. But $n \cdot \overline{1} = \overline{n} = \overline{0}$. So $\mathrm{char}(R) = n$ by definition of the characteristic.

2. If $m \in \mathbb{Z}$, we will denote by respectively by $\overline{m}, [m], \tilde{m}$ its class modulo $2, 4$ and 10. Assume that $m(\overline{1}, [1], \tilde{1}) = (\overline{0}, [0], \tilde{0})$. Then we have

$$(\overline{m}, [m], \tilde{m}) = (\overline{0}, [0], \tilde{0}),$$

   which implies that m is a multiple of $2, 4$ and 10. Hence m is a multiple of the lowest common multiple of $2, 4$ and 10, which is 20. Conversely, $20(\overline{1}, [1], \tilde{1}) = (\overline{20}, [20], \tilde{20}) = (\overline{0}, [0], \tilde{0})$. Therefore $\mathrm{char}(R) = 20$.

3. Here we have $(2-5j)(2-5j^2) = 4 - 10(j + j^2) + 25j^3 = 4 + 10 + 25 = 39$. Hence $39 \cdot \overline{1} = \overline{39} = \overline{(2-5j) \cdot (2-5j^2)} = \overline{0}$. Then the characteristic of R is finite and divides 39. Therefore the characteristic of R is $1, 3, 13$ or 39. Now let $c = \mathrm{char}(R) > 0$. Since $c \cdot 1_R$ lies in the ideal $(2 - 5j)$, then $c = (2 - 5j)(a + bj)$ for some $a, b, \in \mathbb{Z}$. Hence $|c|^2 = |2 - 5j|^2 |a + bj|^2$, so

$$c^2 = 39(a^2 + b^2 - ab)$$

   and therefore $39 | c^2$. The only value (among $1, 3, 13$ and 39) for which it is possible is $c = 39$. Thus $\mathrm{char}(R) = 39$.

Exercise 64. Prove the following isomorphisms:

1. $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$.
2. $\mathbb{Z}[X]/(n, X) \simeq \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$.
3. $\mathbb{Z}[X]/(n) \simeq (\mathbb{Z}/n\mathbb{Z})[X]$, $n \geq 2$.

Answer.

1. Consider $\varphi : m \in \mathbb{Z} \mapsto m \cdot 1_R = \overline{m} \in \mathbb{Z}[i]/(1+i)$. This is a ring homomorphism. It is surjective. Indeed, let $\overline{a+bi} \in \mathbb{Z}[i]/(1+i)$. We have $\overline{a+bi} = \overline{(b-a)+a(1+i)} = \overline{b-a}$, so $\overline{a+bi} = \varphi(b-a)$. Now $\ker(\varphi) = c \cdot \mathbb{Z}$, where $c = \mathrm{char}(R)$ by definition of the characteristic. By direct computation, we get $\mathrm{char}(R) = 2$ (since R is not the trivial ring and $(1+i)(1-i) = 2$). Therefore $\ker(\varphi) = 2\,\mathbb{Z}$. Now use the first isomorphism theorem.

2. Let us consider $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P(0)} \in \mathbb{Z}\,/n\,\mathbb{Z}$. This is the composition of the ring homomorphisms $P \in \mathbb{Z}[X] \mapsto P(0) \in \mathbb{Z}$ and $m \in \mathbb{Z} \mapsto \overline{m} \in \mathbb{Z}\,/n\,\mathbb{Z}$, so it is a ring homomorphism. It is surjective: for $\overline{m} \in \mathbb{Z}\,/n\,\mathbb{Z}$, we have $\varphi(m) = \overline{m}$, where $m \in \mathbb{Z} \subset \mathbb{Z}[X]$ is considered as a constant polynomial. Now we have $\ker(\varphi) = \{P \in \mathbb{Z}[X] | P(0) \text{ is divisible by } n\}$, which equals (n, X). Hence $\ker(\varphi) = (n, X)$; now applying the first isomorphism theorem, we get the result.

3. Consider the reduction modulo n, $\varphi : P \in \mathbb{Z}[X] \mapsto \overline{P} \in (\mathbb{Z}\,/n\,\mathbb{Z})[X]$. We have that φ is a ring homomorphism. It is surjective: let $f \in (\mathbb{Z}\,/n\,\mathbb{Z})[X]$, $f = \overline{a}_0 + \cdots + \overline{a}_m X^m, a_i \in \mathbb{Z}$. Then let $P = a_0 + \cdots + a_m X^m \in \mathbb{Z}[X]$. By definition of $\overline{P}$, we have $\varphi(P) = f$. Now let us compute the kernel of φ. Let $P = a_0 + \cdots + a_m X^m$. We have $\varphi(P) = 0 \iff \overline{a}_0 + \cdots + \overline{a}_m X^m = 0$. This is equivalent to say that $\overline{a}_i = \overline{0}$ for all i, which means that $n | a_i$ for all i. This is equivalent to say that $P = n \cdot Q$, for some $Q \in \mathbb{Z}[X]$. Hence $\ker(\varphi) = (n)$. Now apply the first isomorphism theorem.

Exercise 65. Let $A = \mathbb{C}[X; \sigma]$ be the ring of all skew polynomials $\sum a_i X^i$, $a_i \in \mathbb{C}$, where multiplication is defined by $Xa = \sigma(a)X$ for all $a \in \mathbb{C}$, and σ is the complex conjugation on $\mathbb{C}$.

- Show that the center $Z(A)$ of A is $Z(A) = \mathbb{R}[X^2]$.
- Show that $\bar{A} = A/A(X^2+1)$ is a ring.
- Show that $\bar{A}$ is isomorphic to $\mathbb{H}$, the division ring of Hamilton quaternions.

Answer.

- Note that $X^2 a = X\sigma(a)X = \sigma^2(a)X^2$ and more generally

$$(\sum a_i X^i)(\sum b_j X^j) = \sum_i \sum_j a_i \sigma^i(b_j) X^{i+j}.$$

Now if $\sum b_j X^j$ is in the center, then we must have

$$\sum_i \sum_j a_i \sigma^i(b_j) X^{i+j} = (\sum b_j X^j)(\sum a_i X^i)$$

thus X^j must be an even power of X so that when a_i anti-commute with X^j, $\sigma^j(a_i) = a_i$ since σ is of order 2. Furthermore, we must have that $\sigma^i(b_j) = b_j$ for any i, showing that b_j must be real, which shows that the center is $\mathbb{R}[X^2]$. (More formally, one can take a polynomial in the center, say $p(X)$, and compute $p(X)a = ap(X)$ for any $a \in \mathbb{C}$, which shows that $p(X) \in \mathbb{C}[X^2]$, then compute $p(X)X = Xp(X)$ which shows that $p(X) \in \mathbb{R}[X^2]$).

- For this quotient to be a ring, we need the ideal $A(X^2+1)$ to be two-sided. This is the case since $X^2 + 1$ belongs to the center by the point above.

- We can express the ring of Hamilton quaternions $\mathbb{H}$ in the form $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$, and define

$$\varphi : A \to \mathbb{H},\ \varphi(X) = j,\ \varphi(a) = a,\ a \in \mathbb{C}.$$

Since $ja = \sigma(a)j$ in $\mathbb{H}$ for any $a \in \mathbb{C}$, φ gives a ring homomorphism from A to $\mathbb{H}$. This induces a ring homomorphism $\bar{\varphi} : \bar{A} \to \mathbb{H}$ since $\varphi(X^2 + 1) = j^2 + 1 = 0$. Since

$$\bar{\varphi}(\overline{a + bX}) = a + bj,$$

$\bar{\varphi}$ is an isomorphism. (This is the first isomorphism theorem for rings.)

4.3 The Chinese Remainder Theorem

Exercise 66. Show that the following rings are isomorphic:

$$\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \simeq \mathbb{Z}/36\mathbb{Z} \times 168\mathbb{Z}.$$

Answer. We have that $72 = 8 \cdot 9$ and $\gcd(8, 9) = 1$, thus $\mathbb{Z}_{72} \simeq \mathbb{Z}_8 \times \mathbb{Z}_9$. Similarly $\mathbb{Z}_{84} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7$, $\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \times \mathbb{Z}_9$ and $\mathbb{Z}_{168} \simeq \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7$. Thus

$$\begin{aligned} \mathbb{Z}_{72} \times \mathbb{Z}_{84} &\simeq \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \\ &\simeq \mathbb{Z}_8 \times \mathbb{Z}_{36} \times \mathbb{Z}_3 \times \mathbb{Z}_7 \\ &\simeq \mathbb{Z}_{36} \times \mathbb{Z}_{128}. \end{aligned}$$

Exercise 67. Show that $10^{99} + 1$ is a multiple of 247.

Answer. We have that

$$100 = 12 \cdot 8 + 4$$

thus

$$10^{100} = (10^{12})^8 \cdot 10^4 \equiv 10^4 \equiv (-3)^4 \equiv 3 \equiv -10 \mod 13$$

where the second equality uses that $a^{p-1} \equiv 1 \mod p$. Similarly ($100 = 18 \cdot 6 - 8$)

$$10^{100} \equiv 10^{-8} \equiv 2^8 \equiv 9 \equiv -10 \mod 19.$$

By the Chinese Theorem, we deduce that

$$10^{100} \equiv -10 \mod 247.$$

Since $\gcd(10, 247) = 1$, we can simplify by a factor of 10, and get

$$10^{99} \equiv -1 \mod 247$$

and thus $247 \mid 10^{99} + 1$.

Exercise 68. The battle of Hasting (October 14, 1066). "The men of Harold stood well, together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter thier redoubts; for a single blow of a saxon warhatched would break his lance and cut through his coat of mail... When Harold threw himself into the fray the Saxon were one mighty square of men, shouting the battle-cries 'Ut!', 'Olicross!', 'Godemite!'."

How many men were there in the army of Harald Hardrada? (This exercise is courtesy of C. Wuthrich).

Answer. The men of Harald formed thirteen squares, that is $13x^2$, when Harold threw himself into the battle $(+1)$, they were one mighty square of men (y^2). This gives the equation

$$y^2 = 13x^2 + 1.$$

We then have to look for the smallest integer solution. Using field theory instead, one can rewrite this equation as

$$1 = (y - \sqrt{13}x)(y + \sqrt{13}).$$

We are thus looking for an element $y + \sqrt{13}x$ of $K = \mathbb{Q}(\sqrt{13})$ which satisfies this equation. One can show that $\eta = \frac{3+\sqrt{13}}{2}$ satisfies this equation up to a sign -1, thus η with an even power satisfies it, and η and its powers are actually the only elements in K to satisfy it. We thus need to take an even power of η which will give us an element in the ring $\mathbb{Z}[\sqrt{13}]$. We find that $\eta^6 = 649 + 180\sqrt{13}$ is the first power to satisfy this condition. Finally, the smallest integer solution to the equation $y^2 = 13x^2 + 1$ is $x = 180$ and $y = 649$, that is, there were 421'200 men with Harald Hardrada. It is however known that his army was instead containing about 7'500 men.

4.4 Maximal and prime ideals

Exercise 69. Show that a non-zero principal ideal is prime if and only if it is generated by a prime element.

Answer. If p is prime then consider the principal ideal $pR = \{pr,\ r \in R\}$. To show that pR is prime, we have to show that if $ab \in pR$ then either a or b is in pR. If $ab \in pR$, then $ab = pr$ for some $r \in R$. Since p is prime, it has to divide either a or b, that is either $a = pa'$ or $b = pb'$. Conversely, take a principal ideal cR which is prime, thus if $ab \in cR$, either $a \in cR$, that is $a = ca'$, or $b \in cR$, that is $b = cb'$. We have thus shown that if $c|ab$, then $c|a$ or $c|b$.

Exercise 70. Are the ideals $(X, X+1)$, $(5, X^2+4)$ and $(X^2+1, X+2)$ prime/maximal in $\mathbb{Z}[X]$?

Answer.

- $I = (X, X+1) = \mathbb{Z}$ since $1 = (X+1) - X$, thus I is not a proper ideal and cannot be prime.
- Consider $\mathbb{Z}[X]/(5, X^2+4) \simeq \mathbb{Z}_5[X]/(X^2+4)$, and $(X^2+4) = (X-\bar{1})(X+\bar{1})$ is reducible modulo 5, thus this quotient is not an integral domain and thus the ideal is not prime.
- $I = (X^2+1, X+2) = (X+2, 5)$ since $(X+2)^2 - 4(X+2) + 5 = X^2+1$, then $\mathbb{Z}[X]/I \simeq \mathbb{Z}_5[X]/(X+\bar{2})$ where $X+\bar{2}$ is irreducible in $\mathbb{Z}_5[X]$ thus the quotient is a field and I is maximal.

Exercise 71.

1. Consider the ring $R = \mathbb{Z}[i]$ and the ideal $I = (1+i)$ in R. Is I prime? Is I maximal?
2. Consider the ring $R = \mathbb{Z}[j]$ and the ideal $I = (2 - rj)$ in R. Is I prime? Is I maximal? (j is a primitive 3rd root of unity.)
3. Consider the ring $R = \mathbb{Z}[X]$ and the ideal $I = (n)$ in R. Is I prime? Is I maximal?

Answer.

1. We have $\mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}/2\mathbb{Z}$, which is a field, so $(1+i)$ is maximal (hence prime).
2. The characteristic of $\mathbb{Z}[j]/(2-5j)$ is 39 which is not a prime number (see Exercise 63), so $\mathbb{Z}[j]/(2-5j)$ is not an integral domain. Hence $(2-5j)$ is not prime and therefore not maximal.
3. We have $\mathbb{Z}[X]/(n) \simeq \mathbb{Z}/n\mathbb{Z}[X]$. We have that $\mathbb{Z}/n\mathbb{Z}[X]$ is an integral domain if and only if $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. Hence (n) is a prime ideal if and only if n is a prime number. It is never maximal since $\mathbb{Z}/n\mathbb{Z}[X]$ is not a field for any n (X has no inverse).

Exercise 72. Consider the ring $R = K[X]$ and the ideal of R given by $I = (X-a)$, where K is a field, and $a \in K$. Is I maximal? Is I prime?

Answer. Let $\varphi : P \in K[X] \mapsto P(a) \in K$. This is a ring homomorphism, which is surjective: indeed, if $\lambda \in K$, then $\varphi(\lambda) = \lambda$, where $\lambda \in K \subset K[X]$

is viewed as a constant polynomial. We now determine the kernel of φ. Let $P \in K[X]$. We can write $P = Q(X).(X-a)+c$, for some $Q \in K[X]$ and $c \in K$. (Indeed, it suffices to proceed to the division of P by $X-a$. The remainder is either zero or has degree < 1, that is degree 0, which means that the remainder is a constant.) Then we have $P(a) = Q(a).(a-a)+c = c$. Therefore, $\varphi(P) = 0 \iff c = 0 \iff P$ is a multiple of $X-a$. Hence $\ker(\varphi) = (X-a)$ (the principal ideal generated by $X-a$). Using the first isomorphism theorem, we get that $K[X]/(X-a) \simeq K$. Since $K[X]/(X-a) \simeq K$, and K is a field, then $K[X]/(X-a)$ is a field as well and $(X-a)$ is maximal (hence prime).

Exercise 73. Let R be a commutative ring. Let

$$Nil(R) = \{r \in R | \exists n \geq 1, r^n = 0\}.$$

1. Show that $Nil(R)$ is contained in the intersection of all prime ideals of R.
2. Show that $Nil(R/Nil(R)) = 0$.

Answer.

1. Let $a \in Nil(R)$, so $a^n = 0$ for some $n \geq 1$. Assume that there is a prime ideal $\mathfrak{p}$ for which $a \notin \mathfrak{p}$. We have $a^n = 0 \in \mathfrak{p}$. Since $a^n = a^{n-1}.a$ and $\mathfrak{p}$ is a prime ideal, then $a^{n-1} \in \mathfrak{p}$ or $a \in \mathfrak{p}$. By assumption on a, we have $a \notin \mathfrak{p}$, so necessarily $a^{n-1} \in \mathfrak{p}$. But $a^{n-1} = a^{n-2}.a \in \mathfrak{p}$, so $a^{n-2} \in \mathfrak{p}$ for the same reasons, and by induction we get $a \in \mathfrak{p}$, a contradiction. Therefore a lies in all the prime ideals of R.
2. Let $\overline{a} \in Nil((R/Nil(R)))$, so $\overline{a}^n = \overline{0}$ for some $n \geq 1$. Then $\overline{a^n} = \overline{0}$, which means that $a^n \in Nil(R)$ by definition of the quotient ring. Therefore, there exists $m \geq 1$ such that $(a^n)^m = 0$, so $a^{nm} = 0$, which means that $a \in Nil(R)$. Hence $\overline{a} = \overline{0}$.

Exercise 74. Let $R = \mathbb{Z}[X]$, and let $n \geq 1$.

- Show that the ideal (n, X) is given by

$$(n, X) = \{p(X) \in \mathbb{Z}[X],\ p(0) \text{ is a multiple of } n\}.$$

- Show that (n, X) is a prime ideal if and only if n is a prime number.

Answer.

- Let $P \in (n, X)$, so $P = n.Q_1 + X.Q_2$ for some $Q_1, Q_2 \in \mathbb{Z}[X]$. Then $P(0) = n.Q_1(0) \in n\,\mathbb{Z}$ (we have $Q_1(0) \in \mathbb{Z}$ since $Q_1 \in \mathbb{Z}[X]$), that is $P(0)$ is a multiple of n. Conversely, assume that $P \in \mathbb{Z}[X]$ is such that $P(0)$ is a multiple of n, and write $P = a_nX^n + \cdots + a_1X + a_0$. Then $P(0) = a_0$, so by assumption $a_0 = n.m$ for some $m \in \mathbb{Z}$. Now we get $P = n.m + X.(a_nX^{n-1} + \cdots + a_2X + a_1)$, so $P \in (n, X)$.

- If n is not a prime number, then we can write $n = n_1.n_2, 1 < n_1, n_2 < n$. Now consider $P_1 = n_1, P_2 = n_2 \in \mathbb{Z}[X]$ (constant polynomials). We have $P_1.P_2 = n_1.n_2 = n \in (n, X)$, but P_1 and P_2 are not elements of (n, X). Indeed, $P_1(0) = n_1$ and $P_2(0) = n_2$, but n_1, n_2 are not multiples of n by definition. Hence (n, X) is not a prime ideal. Now assume that n is equal to a prime number p. First of all, $(p, X) \neq \mathbb{Z}[X]$, because $1 \notin (p, X)$ for example. Now let $P_1, P_2 \in \mathbb{Z}[X]$ such that $P_1.P_2 \in (p, X)$. Then $(P_1.P_2)(0)$ is a multiple of p by the previous point, that is $p|P_1(0).P_2(0)$. Since p is a prime number, it means that $p|P_1(0)$ or $p|P_2(0)$, that is $P_1 \in (p, X)$ or $P_2 \in (p, X)$. Hence (p, X) is a prime ideal.

4.5 Polynomial rings

Exercise 75. Set

$$E = \{p(X) \in \mathbb{Z}[X] \mid p(0) \text{ is even }\},\ F = \{q(X) \in \mathbb{Z}[X] \mid q(0) \equiv 0(\text{mod } 3)\}.$$

Check that E and F are ideals of $\mathbb{Z}[X]$ and compute the ideal $E + F$. Furthermore, check that $E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] | p(0) \equiv 0 \text{ (mod 6) }\}$.

Answer. If $p(X) = \sum_{k=0}^{n} p_k X^k$, then

$$E = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z}\} \quad \text{and} \quad F = \{q(X) \in \mathbb{Z}[X] \mid q_0 \in 3\mathbb{Z}\}.$$

Thus E and F are ideals of $\mathbb{Z}[X]$ since $2\mathbb{Z}$ and $3\mathbb{Z}$ are ideals of $\mathbb{Z}$. If $\sum_k c_k X^k = \left(\sum_k p_k X^k\right) \cdot \left(\sum_k q_k X^k\right)$, then $c_0 = p_0 q_0$ and thus

$$E \cdot F \subseteq \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z} \cdot 3\mathbb{Z}\} = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 6\mathbb{Z}\}.$$

Similarly,

$$E + F = \{p(X) \in \mathbb{Z}[X] \mid p_0 \in 2\mathbb{Z} + 3\mathbb{Z}\} \underbrace{=}_{\text{Bezout}} \{p(X) \in \mathbb{Z}[X] \mid p_0 \in \mathbb{Z}\} = \mathbb{Z}[X].$$

Exercise 76. Show that if F is a field, the units in $F[X]$ are exactly the nonzero elements of F.

Answer. Let $f(X) \in F[X]$ of degree n, $f(X)$ is a unit if and only if there exists another polynomial $g(X) \in F[X]$ of degree m such that $f(X)g(X) = 1$. Because F is a field (thus in particular an integral domain), $f(X)g(X)$ is a polynomial of degree $n + m$, thus for the equality to hold, since 1 is a polynomial of degree 0, we need $n + m = 0$, thus both f and g are constant, satisfying $fg = 1$, that is they are units of F, that is nonzero elements since F is a field.

Exercise 77. There exists a polynomial of degree 2 over $\mathbb{Z}/4\mathbb{Z}$ which has 4 roots. True or false? Justify your answer.

Answer. Take the polynomial $2X(X - 1)$.

Exercise 78. Let R be a ring, and let $a \neq 0 \in R$ such that there exists an integer n with $a^n = 0$. Show that $R^* \subset (R[X])^*$ and $R^* \neq R[X]^*$, where R^* and $R[X]^*$ denote respectively the group of units of R and $R[X]$.

Answer. Clearly $R^* \subseteq R[X]^*$. We need to show that the inclusion is strict, that this, there exists an element in $R[X]^*$ which is not in R^*. Take $f(X) = 1 - aX$. We have

$$(1 - aX)(1 + aX + (aX)^2 + \ldots + (aX)^{n-1}) = 1,$$

and f does not belong to R^*.

Exercise 79. Let K be a field. Consider the ring $K[X, Y]$ of polynomials in indeterminates X and Y with coefficients in K.

1. Is $K[X, Y]$ an integral domain?
2. What are the units of $K[X, Y]$?
3. Consider the ideals $\mathcal{I}_1 = (X)$ and $\mathcal{I}_2 = (X, Y)$. Are they prime ideals of $K[X, Y]$?
4. Show that $\mathcal{J} = \{f \in K[X, Y],\ f(0, 0) = 0\}$ is an ideal.
5. Deduce using $\mathcal{J}$ that $K[X, Y]$ cannot be a principal ideal domain.

Answer.

1. Yes it is. It is a commutative ring (since K is a field). Furthermore, it has no zero divisor, since K as none.
2. So units of $K[X, Y]$ are polynomials $f \in K[X, Y]$ such that there exist $g \in K[X, Y]$ with $fg = 1$. Thus the degree of the polynomial fg is 0, and both f, g must be constant polynomials (since K is a field). Thus the units are those of K.
3. Both of them are for the same reason: $K[X, Y]/\mathcal{I}_1 \simeq K[Y]$ and $K[X, Y]/\mathcal{I}_2 \simeq K$, both of them are integral domains, thus both ideals are prime.
4. Take $f, g \in \mathcal{J}$, then $f - g$ belongs to $\mathcal{J}$, and if h is in $K[X, Y]$, we also have that $hf \in \mathcal{J}$.
5. Assume there exists $f \in K[X, Y]$ such that $(f) = \mathcal{J}$. Note that both X and Y belong to $\mathcal{J}$. Thus there must exist $g, h \in K[X, Y]$ such that $X = f(X, Y)g(X, Y)$ and $Y = f(X, Y)h(X, Y)$. Since X is of degree 1, and Y is of degree 1, we should have $f(X, Y) = aX + bY$. But now, if $a \neq 0$, $Y = h(X, Y)(aX + bY)$ is not possible, and if $b \neq 0$, $X = f(X, Y)g(X, Y)$ is not possible either.

4.6 Unique factorization and Euclidean division

Exercise 80.

Show that the ideal generated by 2 and X in the ring of polynomials $\mathbb{Z}[X]$ is not principal.

Answer. We have that

$$\langle 2, X\rangle = \{2r(X) + Xs(X),\ r(X), s(X) \in \mathbb{Z}[X]\},$$

and assume there exists $f(X) \in \mathbb{Z}[X]$ such that $\langle 2, X\rangle = (f(X))$. Since $2 \in (f(X))$, then $f(X) = \pm 2$. Since $X \in (f(X))$, we should have $X = \pm 2g(X)$, a contradiction.

Exercise 81. Let R be an integral domain in which every decreasing chain of ideals is finite. Show that R is a field.

Answer. Let $x \in R$, $x \neq 0$. Then $(x) \supset (x^2) \supset (x^3) \supset \ldots$ is a decreasing chain of ideals. It thus stabilizes at some point by assumption, that is, there is a k in $\mathbb{N}$ such that $(x^k) = (x^{k+1})$. In particular, there is an element $a \in R$ such that $ax^{k+1} = x^k$. Since R is an integral domain, we have $ax = 1$, and thus x is invertible, showing that R without the 0 element is a field.

Exercise 82. Show that if R is a unique factorization domain, then $R[X]$ is also a unique factorization domain.

Answer. Let us write $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, $a_j \in R$. Recall that $c(f)$ is the content of f defined as $\gcd(a_0, \ldots, a_n)$. We need to check that a factorization exists, and that it is unique.

- Existence: if $p \in R$ is irreducible, then p is also irreducible in $R[X]$. If $f(X) \in R[X]$, we can write $f(X) = d\tilde{f}(X)$ be factoring the content d, so that $c(\tilde{f}) = 1$. We can factor d into a product of irreducible in R. Now either $\tilde{f}$ is irreducible in $R[X]$, or it factors properly into a product of lower degree polynomials ($c(\tilde{f}) = 1$). All the factors will also have content 1, and we can only lower degree of factors finitely often, so we get a factorization of $\tilde{f}$, and thus one for f as product of irreducibles in $R[X]$.
- Uniqueness: by Theor 2.15, it suffices to prove that each irreducible element is prime, which we can do by proving that each irreducible element generates a prime ideal in $R[X]/$ If $p \in R$ is irreducible, then $R[X]/pR[X] = (R/p)[X]$ which is an integral domain.

Exercise 83. Let F be a field, let $f(X), g(X) \in F[X]$, and let $d(X)$ be a greatest common divisor of $f(X)$ and $g(X)$. Show that there are polynomials $u(X), v(X) \in F[X]$ such that

$$d(X) = u(X)f(X) + v(X)g(X).$$

When does Bezout identity hold more generally?

Answer. Bezout identity works for general PID as follows (and thus in particular for $F[X]$). Take $a, b \in R$, where R is a PID. Consider the corresponding principal ideals aR and bR, we have that

$$aR + bR = cR$$

simply because R is a PID. Since $aR \subset cR$, $c|a$ and for the same reason $c|b$. Now consider $d = \gcd(a, b)$, then $d|a$ and $d|b$, and thus conversely dR contains aR and bR and thus cR, showing that $d|c$. But c must also divide d, showing that $c = d$, that is

$$aR + bR = \gcd(a, b)R,$$

in words, $\gcd(a, b)$ is some linear combination of a and b using coefficients in R. This does not work for arbitrary UFDs. For example, in $\mathbb{Z}[X]$, the polynomials X and 2 are coprime, but no linear combination of 2 and X gives 1. For more generalization of this notion, check the definition of Bezout domain.

Exercise 84. Show that $\mathbb{Z}[\sqrt{3}]$ is a Euclidean domain. (Hint: use the same technique as the one seen for $\mathbb{Z}[\sqrt{2}]$.)

Answer. Consider the ring

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3},\ a, b \in \mathbb{Z}\}$$

with

$$\Psi(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

Take $\alpha, \beta \neq 0$ in $\mathbb{Z}[\sqrt{3}]$, and compute the division in $\mathbb{Q}(\sqrt{3})$:

$$\alpha/\beta = q',$$

with $q' = x + \sqrt{3}y$ with x, y rational. Let us now approximate x, y by integers x_0, y_0, namely take x_0, y_0 such that

$$|x - x_0| \leq 1/2,\ |y - y_0| \leq 1/2.$$

Take

$$q = x_0 + y_0\sqrt{3},\ r = \beta((x - x_0) + (y - y_0)\sqrt{3}),$$

where clearly $q \in \mathbb{Z}[\sqrt{3}]$, then

$$\begin{aligned} \beta q + r &= \beta(x_0 + y_0\sqrt{3}) + \beta((x - x_0) + (y - y_0)\sqrt{3}) \\ &= \beta(x + y\sqrt{3}) = \beta q' = \alpha, \end{aligned}$$

which at the same time shows that $r \in \mathbb{Z}[\sqrt{3}]$. So far this is exactly what we did in the lecture. We are also left to show that $\Psi(r) < \Psi(\beta)$. We have

$$\begin{aligned} \Psi(r) &= \Psi(\beta)\Psi((x - x_0) + (y - y_0)\sqrt{d}) \\ &= \Psi(\beta)|(x - x_0)^2 - d(y - y_0)^2| \\ &\leq \Psi(\beta)[|x - x_0|^2 + |d||y - y_0|^2] \\ &\leq \Psi(\beta)\left(\frac{1}{4} + |3|\frac{1}{4}\right) \end{aligned}$$

though here we notice that we get $\frac{1}{4}+|3|\frac{1}{4}=1$. So this is not good enough! But let us see what this means to get 1: this happens only if $|x-x_0|^2=|y-y_0|^2=1/4$, otherwise we do get something smaller than 1. Now if $|x-x_0|^2=|y-y_0|^2=1/4$, we have from the second equation that

$$\Psi=\Psi(\beta)|(x-x_0)^2-d(y-y_0)^2|=\Psi(\beta)|\frac{1}{4}-\frac{3}{4}|<1$$

and we are done.

Exercise 85. The goal of this exercise is to show that a principal ideal domain is a unique factorization domain in which every prime ideal is maximal. (Hint: To show that every prime is maximal, take a prime ideal $\mathcal{I}$ and a maximal ideal $\mathcal{M}$, and see what it means for $\mathcal{I}$ to be included in $\mathcal{M}$ in a PID). Note that the converse is true.

Answer. If we have a PID, it is a UFD (this is far from obvious, this was shown in the notes). We have to show that every prime ideal is maximal. Take $\mathcal{I}$ a prime ideal, and $\mathcal{M}$ a maximal ideal. Thus $\mathcal{I}\subseteq\mathcal{M}$ by maximality of $\mathcal{M}$. Now since we have a PID, we can write $\mathcal{I}=(a)$, $\mathcal{M}=(m)$ and $(a)\subseteq(m)$ showing that $m|a$. Thus $a=md$ for some d. But now a is prime (this follows from (a) being prime, see Exercise 69) thus it is irreducible (in a UFD, irreducible and prime are equivalent). Since a is irreducible, either m or d is a unit, and m cannot be (otherwise $\mathcal{M}$ would be R, which is impossible by definition of maximal ideal), thus d is a unit. Then a and m are associate, so they generate the same principal ideal, and $\mathcal{I}=\mathcal{M}$.

4.7 Irreducible polynomials

Exercise 86. Prove whether the following polynomials are reducible/irreducible over F.

1. t^2-2, $F=\mathbb{Q}$.
2. $\frac{2}{9}t^5+\frac{5}{3}t^4+t^3+\frac{1}{3}$, $F=\mathbb{Q}$.
3. t^4+15t^3+7, $F=\mathbb{Z}$, *hint: think of modulo.*
4. $t^{16}+t^{15}+t^{14}+\ldots+t^3+t^2+t+1$, $F=\mathbb{Q}$, *hint: this needs a trick.*

Answer.

1. Use Eisenstein's criterion with $p=2$.
2. This polynomial is irreducible if and only if
$$9f(t)=2t^5+15t^4+9t^3+3$$
is irreducible over $\mathbb{Q}$. Here Eisenstein's criterion can be applied with $p=3$, showing that f is irreducible.

3. Modulo 5, $f(t) \equiv t^4 + 2$. If this is reducible, then either it has a a factor of degree 1 (not possible, it is easy to try the 5 values), or it is a product of two factors of degree 2. The latter can be checked explicitly: if

$$t^4 + 2 = (t^2 + at + b)(t^2 + ct + d)$$

then $a + c = 0$, $ac + b + d = 0$, $bd = 2$. One can check all possible values and see that this is not possible either. Hence $t^4 + 2$ is irreducible modulo 5, and therefore the original polynomial was irreducible over $\mathbb{Z}$.

4. Notice that $f(t)$ is irreducible if and only if $f(t + 1)$ is. By expanding $f(t + 1)$, one can use Eisenstein's criterion with $q = 17$.

Exercise 87. True/False.

Q1. Let R be a ring, and let r be an element of R. If r is not a zero divisor of R, then r is a unit.

Q2. A principal ideal domain is a euclidean domain.

Q3. Hamilton's quaternions form a skew field.

Q4. The quotient ring $\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i]$ is a field.

Q5. A field is a unique factorization domain.

Q6. The ideal $(5, i)$ in $\mathbb{Z}[i]$ is principal.

Q7. The polynomial $3x^4 + 15X^2 + 10$ is irreducible over $\mathbb{Q}$.

Q8. Let R be a ring, and M be a maximal ideal, then R/M is an integral domain.

Answer.

Q1. This cannot be true in general! Take $\mathbb{Z}$ for example. It has no zero divisor, but apart 1 and -1, no other element is a unit! Actually, in an integral domain, there is no zero divisor, which does not mean it is an field.

Q2. A euclidean domain is a principal ideal domain. The converse is not true. Take for example $\mathbb{Z}[(1 + i\sqrt{19})/2]$. It is a principal ideal domain, but it is not a euclidean domain.

Q3. A skew field is non-commutative field. Hamilton's quaternions are non-commutative, and we have seen that every non-zero quaternion is invertible (the inverse of q is its conjugate divided by its norm).

Q4. It is actually a field. You can actually compute the quotient ring explicitly, this shows that $\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i]$ is isomorphic to the field of 2 elements $\{0, 1\}$.This can be done using the first isomorphism for rings.

Q5. It is true since every non-zero element is a unit by definition.

Q6. It is true! With no computation, we know it from the theory: We know that $\mathbb{Z}[i]$ is a euclidean domain, and thus it is a principal domain, so all ideals including this one are principal.

Q7. It is true! Use for example Eisenstein's criterion with $p = 5$.

Q8. Who said the ring R is commutative? The statement seen in the class is about commutative rings. It is not true for non-commutative rings. Here is an example: take $R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$ (ring of quaternions with integer coefficients), pR is a maximal ideal of R (p odd prime) but R/pR is actually isomorphic to $M_2(\mathbb{Z}/p\mathbb{Z})$ and thus is not an integral domain.