Algebra

Lectures by P Vishe
Notes by Ben Napier

2019 Michaelmas Term

Contents

Chapter 1

Rings, fields, and subrings

Lecture 1
On 8/10

Let's start with a rough definition of a ring.

A **ring** is a set of mathematical objects R with the ability to add, multiply, and subtract any numbers $r_1, r_2 \in R$ and still be in the set R. This is not a rigorous definition, but serves as intuition. If we can also divide within a set too, we call it a **field**. Let's look at some examples.

(i) $\mathbb{N}$ is not a ring as $1 - 2 \notin \mathbb{N}$ (and thus not a field).

(ii) $\mathbb{Z}$ is a ring but not a field as $\frac{1}{2} \in \mathbb{Z}$.

(iii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[x]$ are all fields.

(iv) $M_n(\mathbb{R})$ is a ring but not a field, as is $C(\mathbb{R})$.

We now explain more precisely what we mean when we talk about a ring R having the 'ability to add, multiple, and subtract'. We can define addition as

$$+ : R \times R \to R.$$

However, instead of writing $+(1, 4) = 5$ we use the short hand $1 + 4 = 5$. Such functions are called **binary operations** as they only take two elements.

Lecture 2
On 10/10

Let's move forward to a formal definition of a ring.

Definition 1.1 (Ring)**.** A **ring** R is a set with two binary operations called **addition** (usually denoted $+$) and **multiplication** (usually denoted $\cdot$ or $\times$, but not always). A ring must be an **abelian group** under addition and must satisfy:

(i) (identity) $\exists\, 1 \in R : 1 \cdot x = x \cdot 1 = 1$;

(ii) (associativity) $\forall\, a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$; and

(iii) (distributibity) $\forall\, a, b, c \in R$ we have

  (a) $a \cdot (b + c) = a \cdot b + a \cdot c$; and

  (b) $(b + c) \cdot a = b \cdot a + c \cdot a$.

Remark. A few notes on this definition.

(i) Addition is always commutative from the definiition of an abelian group.

(ii) Unlike addition, multiplication does not have to be commutative.

(iii) We call 0 the **additive identity** and 1 the **multipliciative identity**.

(iv) Subtraction is called the **inverse** of addition, so for $a, b \in R$ we have

$$a - b = a + (-b)$$

where $-b$ is such that

$$b + (-b) = 0.$$

Example (Endomorphisms of a vector space)**.** Let V be a complex vector space of dimension n. Then

$$\mathrm{End}\,(V) = \{f : V \to V, f \text{ is linear}\}.$$

We define

$$(f_1 + f_2)(v) := f_1(v) + f_2(v)$$

and

$$(f_1 \circ f_2)(v) = f_1(f_2(v))$$

for all $v \in V$. From previous courses, we have seen that

$$f_1 + f_2, f_1 \circ f_2 \in \mathrm{End}\,(V)$$

and that $\mathrm{End}\,(V)$ is an abelian group under $+$.

(i) (Identity) We define $\mathrm{Id} : V \to V$ such that $\mathrm{Id}\,(v) = v$. This forms the identity element as

$$f \circ \mathrm{Id}\,(v) = f(\mathrm{Id}\,(v)) = f(v) = \mathrm{Id}\,(f(v)) = \mathrm{Id}\,(v) \circ f.$$

(ii) (Associativity) $f, g, h \in \mathrm{End}\,(v)$. We know that $f(v) = Av$ where $A \in M_n(\mathbb{C})$. As matrices are associative, so is f, g, h. That is,

$$\begin{aligned} f \circ (g \circ h)(v) &= f(g \circ h(v)) \\ &= f(g(h(v))) \\ &= A(B(Cv)) \\ &= AB(Cv) \\ &= AB(h(v)) \\ &= (f \circ g)(h(v)). \end{aligned}$$

(iii) (Distributivity) The proof for this property follows the same reasoning as above.

Therefore, the endomorphisms of a complex vector space is a ring using the operations defined above.

Example (Integers modulo n)**.** If we divide any $x \in \mathbb{Z}$ by n then the remainder is in

$$\{0, 1, 2, \ldots, n-1\}.$$

Every integer is associated with its remainder, that is

$$\mathbb{Z}/n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

where $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ are called **residue classes** mod n. The residue class mod n $\bar{i}$ is the set of all numbers that leave a remainder i when divided by n. We also denote $\mathbb{Z}/n$ with $\mathbb{Z}_n$, $\mathbb{Z}/_{n\mathbb{Z}}$, and $\mathbb{Z}/(n)$.

(i) (Identity) $\bar{1} \in \mathbb{Z}/n$ is our identity element as

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}.$$

(ii) (Associativity) Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n$. Then

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} + \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

(iii) (Distributivity) Let $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n$. Then

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a}(\overline{b+c} = \overline{a(b+c)} + \overline{ab+ac} = \overline{ab} + \overline{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}.$$

Hence integers modulo n is a ring under the opeerations defined above.

Example (Integers modulo 3)**.** Let $n = 3$. Then $\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}$. We can look at a table to see how the addition operator works.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

1.1 Subrings

Lecture 3
On 15/10

Definition 1.2 (Subring)**.** A subring S in a ring R is a subset $S \subset R$ such that

(i) (identity) $0, 1 \in S$;

(ii) (closure under addition) $\forall\, a, b \in S,\ a + b \in S$;

(iii) (closure under multiplication) $\forall\, a, b \in S,\ ab \in S$; and

(iv) (addition inverse) $\forall\, a \in S,\ -a \in S$.

Remark. Any subring $S \subset R$ is equipped with the same $+$ and $\cdot$ operators of R.

Example. It can be easily shown that $\mathbb{Q}$ is a subring of $\mathbb{Q}[x]$.

Example. Consider

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subset \mathbb{R}.$$

This may not be immediately obvious, but this is a subring of $\mathbb{R}$.

Example. Consider

$$R = \mathbb{Z}/6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

and

$$S = \{\bar{0}, \bar{2}, \bar{4}\} \subset R.$$

As $\bar{1} \notin S$, it is not a subring of R. This is the only criteria it fails. However, S can be made into a ring itself with $\bar{0}$ as the additive identity and $\bar{4}$ as the multiplicative identity. Even though this is the case, it is not a subring of R as it does not share the same multiplicative identity.

Remark. The above example illustrates an interesting point that rings can be contained with other rings and not be considered a subring.

1.2 Fields

We saw earlier that $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields but we did not formally define the concept.

Definition 1.3 (Field)**.** A ring R is called a **field** if

(i) R is a commutative ring;

(ii) $\forall\, a \in R$ where $a \neq 0$ there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

Example. Consider the commutative ring $\mathbb{Q}$. For all $a, b \in \mathbb{Q}$ where $a, b \neq 0$ we have that

$$\frac{a}{b} \cdot \frac{b}{a} = 1$$

and hence

$$\frac{a}{b} = \left(\frac{b}{a}\right)^{-1};$$

therefore, $\mathbb{Q}$ is a field.

Looking at the example above, we use the notation

$$\frac{a}{b} = ab^{-1}$$

for $a, b \in F$ where F is a field and $b \neq 0$. This operation is called **division** (surely introducted before).

Definition 1.4 (Zero divisor)**.** An element $a \in R$ of a ring R is called a **zero divisor** if there exists $b \in R$ where $b \neq 0$ such that

$$ab = 0.$$

Example. $\bar{2} \in \mathbb{Z}/6$ and $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$ hence $\bar{2}$ is a zero divisor of $\mathbb{Z}/6$. In fact, $\bar{3}$ is too.

Example. Consider

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Q}).$$

As

$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

A is a zero divisor of $M_2(\mathbb{Q})$.

Example. For all rings R, $0 \in R$ is a zero divisor as long as $0 \neq 1$.

Example. Let F be a field and $a \in F$ be a zero divisor. Let $b \in F$ where $b \neq 0$. Then

$$\begin{aligned} ab &= 0 \\ (ab)b^{-1} &= 0 \cdot b^{-1} \\ a \cdot 1 = a &= 0. \end{aligned}$$

Chapter 2

Integral domains

Lecture 4
On 17/10

Definition 2.1 (Integral domain)**.** A commutative ring R with at least two elements ($0 \neq 1$) is called an **integral domain** if it has no non-zero zero divisor. Alternatively, where R satisfies

$$\forall\, a, b \in R : a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

Example. Any field F has no non-zero zero divisor. Hence any field F where $0 \neq 1$ is an integral domain. So clearly $\mathbb{Q}$, $\mathbb{C}$, and $\mathbb{R}$ are all integral domain over typical operations. $\mathbb{Z}$ is also an integral domain.

Example. Consider

$$\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}.$$

Let's consider the multiplication table.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

It is clear that $\mathbb{Z}/3$ has no non-zero divisor; hence, $\mathbb{Z}/3$ is an integral domain. In fact, $\mathbb{Z}/3$ is a field.

Example. Consider

$$\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

This is not an integral domain as $\bar{2} \cdot \bar{2} = \bar{0}$.

Example. Let R be an integral domain. Let

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x_i : a_i \in R \right\}.$$

$R[x]$ is an integral domain. Let's prove it. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ and $g(x) = b_0 + b_1 x + \ldots + b_m x^m$ such that $a_n \neq 0$ and $b_m \neq 0$.

$$f(x)g(x) = a_0 b_0 + \ldots + a_n b_m x^{n+m} \neq 0$$

hence an integral domain.

2.1 The group of units in a ring

Definition 2.2 (Unit)**.** Let R be a ring. An element $u \in R$ is called a **unit** if there exists u^{-1} such that

$$uu^{-1} = u^{-1}u = 1.$$

Given a ring R,

$$R^{\times} = \{u \in R : u \text{ is a unit}\}$$

is the set of all units in R.

Proposition 2.3. Let R be a ring. $R^{\times}$ is a group under multiplication $(\cdot)$.

Proof. Let $a, b, c \in R^{\times}$. Then

(i) (closure under $\cdot$)

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1;$$

(ii) (multiplicative identity) $1 \in R^{\times}$;

(iii) (associativity)

$$(ab)c = a(bc);$$

(iv) (inverse)

$$aa^{-1} = 1 = a^{-1}a \Rightarrow a^{-1} \in R^{\times}.$$

□

Example. (i) $R = \mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. $\mathbb{R}^{\times} = \{\bar{1}, \bar{3}\}$.

(ii) $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$. $\mathbb{Z}^{\times} = \{\pm 1\}$.

(iii) $M_2(\mathbb{R})^{\times} = \mathrm{GL}_2(\mathbb{R}) =$ all invertible matrices.

Example. Let R be an integral domain. Consider

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_n x^n \in R[x] \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n \in R[x] \end{aligned}$$

where $f(x) \neq 0$ and $g(x) \neq 0$. $f(x)g(x) \neq 1$ for $n \geq 1$, hence if $f(x)$ is a unit then $n = 0$. In fact, $R[x]^{\times} = R^{\times}$.

Proposition 2.4. Let $\bar{x} \in \mathbb{Z}/n$. Then $\bar{x}$ is a unit if and only if

$$\gcd(x, n) = 1.$$

Proof. $\Rightarrow$ Let $\bar{x} \in \mathbb{Z}/n^{\times}$. Then there exists some $y \in \mathbb{Z}/n^{\times}$ such that $\bar{x} \cdot \bar{y} = 1$. Then

$$\begin{aligned}
\overline{x \cdot y} &= \bar{1} \\
\overline{xy - 1} &= \bar{0} \\
n &\mid xy - 1 \\
xy - 1 &= kn, \quad k \in \mathbb{Z} \\
1 &= xy - kn \\
\gcd(x, n) &\mid 1 \\
\gcd(x, n) &= 1
\end{aligned}$$

$\Leftarrow$ Via Euclid's algorithm we have

$$\begin{aligned}
1 &= xy + nz \\
n &\mid xy - 1 \\
\overline{xy - 1} &= \bar{0} \\
\overline{xy} &= \bar{1} \\
\bar{x} &\in \mathbb{Z}/n^{\times}.
\end{aligned}$$

$\square$

Lecture 5
On 22/10

Proposition 2.5.

$$\mathbb{Z}/n \text{ is a field} \iff \mathbb{Z}/n \text{ is an integral domain} \iff n \text{ is prime.}$$

Proof. All fields are integral domains, so $\mathbb{Z}/n$ is a field $\Rightarrow$ $\mathbb{Z}/n$ is an integral domain.

Suppose $n = n_1 n_2$ where $1 < n_1, n_2 < n$. Then

$$\bar{n} = \bar{n}_1 \bar{n}_2 = 0 \Rightarrow \mathbb{Z}/n \text{ is not an integral domain.}$$

Hence, $\mathbb{Z}/n$ is an integral domain $\Rightarrow$ n is prime.

Let n be prime. $\mathbb{Z}/n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$. So

$$\gcd(n, 1) = \gcd(n, 2) = \ldots = \gcd(n, n-1),$$

and hence by an earlier proposition, $1, 2, \ldots, n-1$ are units. With $\mathbb{Z}/n$ being a commutative ring too, it is also a field. $\square$

Chapter 3

Polynomials over a field

Definition 3.1 (Polynomial ring)**.** The **polynomial ring** $F[x]$ in x over the field F is define to be

$$F[x] = \{a_0 + a_1 x + \ldots + a_n x^n : a_i \in F, n \in \mathbb{Z}_{\geq 0}\}.$$

Definition 3.2 (Degree of a polynomial)**.** For any $f = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$, we define the **degree** of f to be

$$\deg f = \begin{cases} \max\{i : a_i \neq 0\} & f(x) \neq 0 \\ -\infty & f(x) = 0. \end{cases}$$

Proposition 3.3 (Properties of the degree of a polynomial)**.** Let $f, g \in F[x]$. Then

(i) $\deg(fg) = \deg f + \deg g$; and

(ii) $\deg(f + g) \leq \max\{\deg f, \deg g\}$ and $\deg(f + g) = \max\{\deg f, \deg g\}$ if $\deg f \neq \deg g$.

Example (Division algorithm in $\mathbb{Z}$)**.** We can find the **quotient** and **remainder** of 200 divided by 22 in $\mathbb{Z}$. Long division gives

$$200 = 22 \cdot 9 + 2,$$

here 9 is the quotient and 2 is the remainder.

We have a similar algorithm that we can apply to polynomials too.

Example (Division algorithm in $F[x]$)**.** Let $f(x) = x^3 + x^2 - 3x - 3$ and $g(x) = x^2 + 3x + 2$. We do the following long division of polynomials.

Terms to eliminate	
x^3	$f_1 = f(x) - xg(x) = -2x^2 - 5x - 3$
$-2x^2$	$f_2 = f_1 + 2g(x) = x - 1$

We stop here as $\deg f_2 < \deg g$. We have

$$\begin{aligned} f(x) &= xg(x) - 2g(x) + x - 1 \\ &= (x-2)g(x) + (x-1) \end{aligned}$$

so our quotient is $x - 2$ and our remainder is $x - 1$.

Proposition 3.4. Given $f, g \in F[x]$ where F is a field and $g(x) \neq 0$, then there are unique polynomials $q(x), r(x) \in F[x]$ such that

$$f(x) = q(x)g(x) + r(x)$$

where $\deg r < \deg g$.

Proof for uniqueness. Let $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$. Then

$$\begin{aligned} (q_1(x) - q_2(x))g(x) + (r_1(x) - r_2(x)) &= 0 \\ \deg(q_1 - q_2) + \deg(g) = \deg(r_2 - r_1) &< \deg(g) \\ q_1 - q_2 &= 0 \\ r_2 - r_1 &= 0; \end{aligned}$$

hence, $q_1 = q_2$ and $r_1 = r_2$. □

Lecture 6
On 24/10

Proof for existence. If $\deg g > \deg f$ then we simply take $q(x) = 0$ and $r(x) = f(x)$. If $\deg g \leq \deg f$ then let

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_m x^m \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n \end{aligned}$$

where $a_m, b_n \neq 0$. Let $d = m - n \geq 0$. We use induction on d. For $d = 0$, we have $m = n$. Set $q(x) = \frac{a_m}{b_n}$ and

$$r(x) = f(x) - q(x)g(x).$$

Here we have a suitable q, r. Now we can move on to the inductive step. Assume the existence of a suitable $q(x), r(x)$ for all $d < k$ for some $k \geq 0$. Now we consider $d = k$. So $m = n + k$. Consider

$$f_1(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x).$$

We now have that $\deg f_1 < \deg f$, so by our assumption there exists a $q_1(x)$ and $r(x)$ such that

$$f_1(x) = q_1(x)g(x) + r(x).$$

So we have

$$f(x) = f_1(x) + \frac{a_m}{b_n}x^{m-n}g(x) = g(x)\left(q_1(x) + \frac{a_m}{b_n}x^{m-n}\right) + r(x)$$

and hence we have a suitable $r(x)$ and $q(x) = q_1(x) + \frac{a_m}{b_n}x^{m-n}$. By induction, this is true for all $d \geq 0$. $\square$

Chapter 4

Greatest common divisors in a ring

Definition 4.1 (Greatest common divisor)**.** Let R be a commutative ring and $a, b \in R$. We call d the **greatest common divisor** of a and b, denoted $d = \gcd(a, b)$ if

(i) d ***divides*** both a and b (that is, there exists $x, y \in R$ such that $a = xd$ and $b = yd$); and

(ii) if $e \in R$ divides a and b then e divides d.

Example. With this definition of the geratest common divisor, we have that 1 and -1 are both greatest common divisors for 2 and 3 in $\mathbb{Z}$; however, we can make the definition unique in rings with total ordering (that is, the $\leq$ and $>$ relations exist) by considering the greatest common divisor as the greatest of the possible. This is typically how we define *the* greatest common divisor. Obviously, we cannot do this in fields such as $\mathbb{C}$ or $\mathbb{Z}[\sqrt{-2}]$ but it does not really matter that the greatest common divisor is not unique in these fields.

Remark. It is actually possible for a two numbers in a ring to not have a greatest common divisor.

Remark. In any ring R, $\gcd(0, 0) = 0$ and is unique.

4.1 The Euclidean algorithm

Example. Let $f(x) = x^2+1$ and $g(x) = x^2+3x+1$ in $\mathbb{Q}[x]$. Find $\gcd(f(x), g(x))$.

Solution. Here we will use the fact that if $f(x) = q(x)g(x) + r(x)$, then

$$\gcd(f(x), g(x)) = \gcd(g(x), r(x)).$$

So,

$$f(x) = g(x) - 3x.$$

Now as our remainder $-3x$ has a lower degree as g, we stop. But now we can perform the same thing with dividing $g(x)$ by $-3x$. So

$$g(x) = \left(-\frac{1}{3}x - \frac{1}{3}\right)(-3x) + 1.$$

Here we are trying to find $\gcd(f(x), g(x)) = \gcd(-3x, 1)$, and

$$-3x = 1 \cdot (-3x) + 0;$$

here we know that $\gcd(f(x), g(x))$ is given by the last non-zero remainder so

$$\gcd(f(x), g(x)) = 1.$$

$\square$

Example. Let $f(x) = x^2 + 7x + 6$ and $g(x) = x^2 - 5x - 6$ in $\mathbb{Q}[x]$. Find $\gcd(f(x), g(x))$.

Solution.

$$\begin{aligned} f(x) &= 1 \cdot g(x) + 12(x+1) \\ g(x) &= \frac{1}{12}x \cdot 12 \cdot (x+1) - 6(x+1) \\ 12(x+1) &= (-2) \cdot (-6) \cdot (x+1) + 0 \end{aligned}$$

So $\gcd(f(x), g(x)) = x + 1$. Even though we have a 12 constant in it, 12 is a unit in $\mathbb{Q}[x]$ meaning it will divide *everything*. $\square$

Remark. A polynomial in $F[x]$ is called **monic** if the leading coefficient is 1. Above we showed that we can find a monic greatest common divisor even though we started with a non-monic one. The following result will show that there is always a monic gcd and it is always unique.

Lemma 4.2 (gcd is unique up to units)**.** Let R be an integral domain. Let $a, b \in R$. Then if $d = \gcd(a, b)$ exists we have that ud is also a $\gcd(a, b)$ for all units $u \in R^\times$.

Proof. $\Rightarrow$ Lets assume that $d = \gcd(a, b)$ and $u \in R^\times$. d divides a hence there exists some $m \in R$ such that $dm = a$. Therefore

$$du(u^{-1}m) = a;$$

hence du divides a. So du divides a and similarily du divides b. Now if there exists $e \in R$ that divides $a, b \in R$ we know that there exists k such that $ek = d$. So $eku = du$ so e divides du and therefore du is a gcd.

$\Leftarrow$ Next we assume that d and d' are two gcds. Then, by definition, both divide a and b and both must divide each other. This means

$$d = d'u, \quad d' = dv,$$

for some $u, v \in R$. Thus $d = duv$. If $d = 0$, then also $d' = 0$, so we may take $u = 1$. If $d \neq 0$, then (since R is an integral domain), we can cancel d and obtain $uv = 1$. Hence u and v are units, so we are done.

$\square$

Lecture 7
On 29/10

Theorem 4.3. Let R be either $\mathbb{Z}$ or $F[x]$, and let $a, b \in R$. Then

(i) $\gcd(a, b)$ exists;

(ii) if $a \neq 0$ and $b \neq 0$ we can compute a $\gcd(a, b)$ by the Euclidean algorithm; and

(iii) if d is a $\gcd(a, b)$, then there exists $x, y \in R$ such that $ax + by = d$.

Chapter 5

Factorisations in rings

A nice (and important) property of the ring of integers is that every positive integer can be uniquely factorised into a product of primes. The situation is not so nice in general rings; however, there still exists relating theorems in the ring $F[x]$ (F field) and the more general class of rings called **unique factorisation domains** (which we will briefly touch on).

5.1 Irreducible polynomials in $F[x]$

Some polynomials can be factored into a product of other polynomials, for example

$$x^3 - x = (x-1)(x^2+x+1) \in \mathbb{Q}[x].$$

Since constantsa re also polynomials, we can also factorise then like

$$13x + 13 = 13(x+1)$$

but this is not *proper* factorisation. Atleast, we don't consider it such as then $7 = 1 \cdot 7 = 1 \cdot 1 \cdot 7$ would start popping up. Polynomails or integers which we can't properly factorise are called irreducible, here is a more formal definition though.

Definition 5.1 (Irreducible)**.** Let R be a commutative ring and $a, b \in R$. An element $r \in R$ is called **irreducible** if

(i) r is not a unit; and

(ii) $r = ab \Rightarrow a$ is a unit or b is a unit.

Example. (i) Let F be a field. Then $f(x) \in F[x]$ is irreducible if it is not constant and cannot be written as the product of two non-constant polynomials in $F[x]$.

(ii) $x^2 + 1 \in \mathbb{R}[x]$ is irreducible, but $x^2 + 1 \in \mathbb{C}[x]$ is not.

Example. Let F be a field and $f(x) \in F[x]$.

(i) If $\deg f = 1$, then it is irreducible.

(ii) If $\deg f \in \{2, 3\}$, then it is irreducible if and only if it has no roots in F. We will prove this. Let $\alpha' \in F$ be a root of $f(x)$. So we write $f(x) = q(x)(x - \alpha) + r(x)$ with $\deg r \leq 0$ (using an eariler result). Thus, $r(x)$ must be constant. Then

$$0 = f(\alpha) = r(\alpha)$$

but r is constant, so $f(x) = q(x)(x - \alpha)$ and so it is not irreducible. Conversely, if f is not irreducible, then $f(x) = g(x)h(x)$ with $\deg g \geq 1$ and $\deg h \geq 1$. But $\deg f = \deg g + \deg h$, so if $\deg f \in \{2, 3\}$ we must have that either

(a) $\deg g = 1$; or

(b) $\deg h = 1$.

Say that $\deg g = 1$, so $g(x) = ax + b$ for some $a, b \in F$ with $a \neq 0$. Thus

$$0 = g\left(\frac{-b}{a}\right) = f\left(\frac{-b}{a}\right)$$

so f has a root.

(iii) If $\deg f = 4$, then it is irreducible if and only if it has no zeros in F and it is not the product of two quadratic polynomails, the proof for this is similar to above.

Proposition 5.2. Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ with $\deg f \geq 1$. Then if $f\left(\frac{p}{q}\right) = 0$ where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$ then

$$p \mid a_0 \quad \text{and} \quad q \mid a_n.$$

Proof. We have

$$f\left(\frac{p}{q}\right) = a_0 + a_1\left(\frac{p}{q}\right) + \ldots + a_n\left(\frac{p}{q}\right)^n = 0.$$

So if we multiply both sides by q_n and take a factor of p out we get

$$p(a_1 q^{n-1} + a_2 p q^{n-2} + \ldots + a_n p^{n-1}) = -a_0 q^n;$$

hence $p \mid a_n p^n$ but as $\gcd(p, q) = 1$ we have $p \mid a_0$. Simiarly, going back to our first equations and shifting the leading term instead we get

$$q(a_0 q^{n-1} + a_1 p q^{n-2} + \ldots a_{n-1} p^{n-1}) = -a_n p^n$$

and so $q \mid a_n$ as required. ∎

Lecture 8 On 31/10

In general, we will find that is easier to check whether a polynomial in $\mathbb{Q}[x]$ is irreducible than for a polynomial in $\mathbb{Z}[x]$; however, we do need to be a little bit careful. For example, $2x+2$ is irreducible as an element of $\mathbb{Q}[x]$ but not as an element of $\mathbb{Z}[x]$ because $2x+2 = 2(x+1)$ with 2 and $x+1$ not being units in $\mathbb{Z}[x]$.

Lemma 5.3 (Gauss's lemma)**.** A non-constant polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Proof. $\Rightarrow$ Omitted.

$\Leftarrow$ Assume that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$. Let $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. If $\deg g \geq 1$ and $\deg h \geq 1$ then we would also have a proper factorisation in $\mathbb{Q}[x]$, violating irreducibility. Thus we have either $\deg g = 0$ or $\deg h = 0$. Say it is g. Thus $g(x) \in \mathbb{Z}$. If $g(x) \neq \pm 1$ then there will exist a prime number $p \in \mathbb{Z}$ dividing $g(x)$, and thus $f(x)$ and thus violating $\gcd(a_0, a_1, \ldots, a_n) = 1$. Hence $\gcd(x) = \pm 1$ (a unit) so $f(x)$ is irreduible in $\mathbb{Z}[x]$.

$\square$

Corollary 5.4. A polynomial $f(x) \in \mathbb{Z}[x]$ satisfiying $\gcd(a_0, \ldots, a_n) = 1$ factors in $\mathbb{Z}[x]$ if and only if it factors in $\mathbb{Q}[x]$.

Lemma 5.5. If a monic polynomial in $\mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$, then it factors into integer monic polynomials.

Proof. Let $f(x) = a_0 + a_1 x + \ldots + x^n$ as above. As f factors in $\mathbb{Q}[x]$, it factors in $\mathbb{Z}[x]$ hence

$$f(x) = h(x)g(x) = (b_0 + \ldots + b_m x^m)(c_0 + ldots + c_p x^p)$$

where $m+p = n$ and $b_i, c_j \in \mathbb{Z}$. Equating coefficients, we have $b_m c_p = 1$; hence, either $b_m = c_p = 1$ or $b_m = c_p = -1$. Either case, either $f(x) = h(x)g(x)$ or $g(x) = (-h(x))(-g(x))$; both a product of two integer monic polynomials. $\square$

Example. Show that $f(x) = x^4 - 10x^2 - 16$ is irreducible in $\mathbb{Q}[x]$.

Lecture 9 On 5/11

Theorem 5.6 (Eisenstein's criterion)**.** Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}$ with a prime p such that

$$p \nmid a_n, \quad p \mid a_0, \ldots, a_{n-1}, \quad p^2 \nmid a_0$$

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example. Let $p \in \mathbb{Z}$ be a prime number. The polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 = \frac{x^p}{x-1}$$

is called the pth cyclotomic polynomial and it is irreducible (and we will prove it). Set

$$\begin{aligned} f(x) &= \Phi_p(x+1) \\ &= \frac{(x+1)^{p-1}}{(x+1)-1} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \ldots + \binom{p}{1}x + 1 - 1}{x} \\ &= x^{p-1} + px^{p-2} + \ldots + \binom{p}{2}x + p. \end{aligned}$$

Observe that $1 \leq k \leq p-1 \Rightarrow p \mid \binom{p}{k}$. So

$$p \mid a_0, a_1, \ldots, a_{p-2},$$

$a_{p-1} = 1$, $a_0 = p$, and $p^2 \nmid a_0$. So by Eisenstein's criterion we have that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

5.2 Prime elements

Definition 5.7 (Prime element)**.** Let F be a commutative ring. Then $a \in R$ is called a **prime element** if

(i) $a \neq 0$ and a is not a unit; and

(ii) $a \mid xy \Rightarrow a \mid x$ or $a \mid y$.

Proposition 5.8. Let R be an integral domain. If $a \in R$ is prime then it is irreducible.

Proof. So we have $a \in R$ prime. So $a \neq 0$, a is not a unit, and $a \mid bc \Rightarrow a \mid b$ or $a \mid c$. We have

$$a = bc \Rightarrow a \mid bc \Rightarrow a \mid b \text{ or } a \mid c$$

and $a \mid b \Rightarrow b = ax$ for some $b \in R$. So

$$a = axc \Rightarrow a(1 - xc) = 0 \Rightarrow xc = 1;$$

hence, x and c are units. This can be similarly shown that $a \mid c \Rightarrow b$ is a unit. □

Example. Let F be a field. Then $f(x) \in F[x]$ is irreducible if and only if f is prime.

Proof. $\Leftarrow$ Above.

$\Rightarrow$ We have $f(x) \in F[x]$ where F is a field and f is irreducible. Hence $f(x) \neq 0$ and not a unit. Suppose $f \mid hg$. Suppose $f \nmid g$. Then

$$\gcd(f, g) \mid f \Rightarrow \gcd(f, g) = 1.$$

By the Euclidean algorithm there exists f_1 and g_1 such that

$$\begin{aligned} f(x)f_1(x) + g(x)g_1(x) &= 1 \\ f(x)f_1(x)h(x) + g(x)g_1(x)h(x) &= h(x); \end{aligned}$$

hence $f(x) \mid$ LHS and so $f(x) \mid$ RHS.

$\square$

Example (Irreducibility $\not\Rightarrow$ prime)**.** Consider $R = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$. We claim that 2 is irreducible but not prime. Consider $N : \mathbb{R} \to \mathbb{Z}$ defined by

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Let $x_1 = a + b\sqrt{-5}$ and $x_2 = c + d\sqrt{-5}$. Then

$$N(x_1, x_2) = x_1x_2\overline{x_1x_2} = x_1\bar{x}_1x_2\bar{x}_2 = N(x_1)N(x_2)$$

and hence N is multiplicative. Suppose $2 = ab$ where $a, b \in \mathbb{Z}[\sqrt{-5}]$. Then

$$4 = N(2) = N(ab) = N(a)N(b).$$

Let $a = x + y\sqrt{-5}$ and $b = z + w\sqrt{-5}$. Then

$$4 = (x^2 + 5y^2)(z^2 + 5w^2).$$

So

$$x^2 + 5y^2 = \begin{cases} 1 & x = pm1, y = 0 \\ 2 & \text{no solutions} \\ 4 & x = \pm 2, y = 0; \end{cases}$$

hence as when $x = \pm 2, y = 0$, it is irreducible. But 2 is clearly not prime as

$$2 \mid (1 - \sqrt{-5}(1 + \sqrt{-5}) = 6$$

implies that $2x = 1$, which is not possible for $x \in \mathbb{Z}$. So 2 is irreducible but not prime in R.

5.3 Unique factorisation in $F[x]$

Lecture 10
On 7/11

Theorem 5.9. Let F be a field and $f(x) \in F[x]$ with $\deg f \geq 1$. Then $f(x)$ can be factorised uniquely into a product of irreducible elements, up to the order of the factors and multiplication of units.

Proof of existence. We do this by induction. If $\deg f = 1$, we know this is irreducible so we are done. Now assume that the theorem holds for $\deg f < n$. Then we consider $\deg f = n$. If f is irreducible, we are done. If not, then $f(x) = g(x)h(x)$ with $1 \leq \deg g < n$ and $1 \leq \deg f < n$. By assumption, g and h have unique factorisations and then so does f. $\square$

Proof of uniqueness. Suppose $f(x) = p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_2 \cdot \ldots q_n$ where p_i, q_i are irreducibles. We have

$$p_1 \mid q_1, q_2, \ldots, q_n$$

and so $p_1 \mid q_i$ for some i; hence $q_i = p_1 u_1$ for some $u_1 \in F[x]$. As p_1 and q_i are irreducible so u_1 must be a unit. Hence

$$p_1 \cdot p_2 \cdot \ldots \cdot p_m = q_1 \cdot q_i \cdot q_m = q_1 \cdot \ldots \cdot (u_1 p_1) \cdot q_{i+1} \cdot \ldots \cdot q_n,$$

we repeat this process to see that $m = n$ and that the factorisation is unique up to multiplication by units. □

Definition 5.10 (Unique factorisation domain)**.** An integral domain R is called a **unique factorisation domain** (UFD) if every non-zero non-unit element $r \in R$ can be written as a product of irreducible elements and this product is unique up to the order of the factors and multiplication by units.

Example. The following are all UFDs:

(i) $\mathbb{Z}$;

(ii) $F[x]$;

(iii) $\mathbb{Z}[i]$; and

(iv) $\mathbb{Z}[\sqrt{\pm 2}]$.

$\mathbb{Z}[\sqrt{-5}]$ is not an UFD.

Chapter 6

Homomorphisms

Definition 6.1 (Homomorphism)**.** Let R and S be rings. Then a map $f : R \to S$ is called an **homomorphism** if

(i) $f(1_R) = 1_S$;

(ii) $f(a+b) = f(a) + f(b)$ for all $a, b \in R$; and

(iii) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

Remark. In the definition above, we use 1_R and 1_S to denote the identity elements in the rings R and S. We may become relaxed on this and just use the definition $f(1) = 1$, but it means for the respective rings. Context is important in these situations.

Example. We will consider the function $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ given by $a+b\sqrt{2} \mapsto a - b\sqrt{2}$.

(i) $f(1) = f(1 + 0\sqrt{2}) = 1 - 0\sqrt{2} = 1$;

(ii) $f(a+b) = f((a+b)+0\sqrt{2} = (a+b)-0\sqrt{2} = (a-\sqrt{0})+(b-\sqrt{0}) = f(a)+f(b)$; and

(iii) $f(ab) = f((ab) + 0\sqrt{2}) = (ab) - 0\sqrt{2} = (a - 0\sqrt{2})(b - 0\sqrt{2}) = f(a)f(b)$;

hence, f is a homomorphism. Lecture 11 On 12/11

Lemma 6.2. Let R, S be rings and $f : R \to S$ be a homomorphism then

(i) $f(0) = 0$; and

(ii) $f(-a) = -f(a)$.

Proof. (i)

$$0 + 0 = 0 \Rightarrow f(0+0) = f(0) \Rightarrow f(0) + f(0) = f(0) \Rightarrow f(0) = 0.$$

(ii)

$$a+(-a)=0 \Rightarrow f(a+(-a))=f(0) \Rightarrow f(a)+f(-a)=0 \Rightarrow f(-a)=-f(a).$$

$\square$

Definition 6.3 (Kernal and image of a homomorphism)**.** Let $f : R \to S$ be a homomorphism. Then we define the **kernal** of f as

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

and the **image** of f as

$$\operatorname{im} f = \{f(x) : x \in R\} \subset S.$$

Definition 6.4 (Isomorphism)**.** A bijective homomorphism is called an **isomorphism**. If $f : R \to S$ is an isomorphism, then we say that R is isomorphic to S denotes $R \simeq S$.

Example. Define a map $f : \mathbb{Z} \to \mathbb{Z}/m$ where $z \mapsto \bar{z}$. This is surjective but *not* injective; hence, it is not an isomorphism.

Example. Let $R = \mathbb{C}$. We define $S \subset M_2(\mathbb{R})$ as

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R}).$$

This is clearly a subring. Let $f : \mathbb{C} \to S$ defined by

$$f(x+iy) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}.$$

We see that f is a homomorphism and also an isomorphism. Therefore, $\mathbb{C}$ is isomorphic to S.

Remark. An isomorphism between two rings gives us the indication that the rings are effectively the same.

Example.

$$\operatorname{End} V \simeq M_n(\mathbb{R}).$$

Example. (i) Let R, S be rings and define the function $f : R \to \{0\}$ such that $\gamma \mapsto 0$. This is known as the *zero homomorphism.*

(ii) The *identity homomorphism* $\mathrm{Id} : R \to R$ such that $\gamma \mapsto \gamma$ is an isomorphism.

Example. Let R and S be rings. We can construct the *direct product* of R and S denoted $R \times S$. We define its operations as follows

$$(r,s) + (r',s') = (r+r', s+s')$$
$$(r,s)(r',s') = (rr', ss').$$

It is clear that $(1,1) \in R \times S$ is the identity element. The other conditions for being a ring are clear to see. We have two specific surjective homomorphism $p_1 : R \times S \to R$ and $p_2 : R \times S \to S$ defined by

$$p_1(r,s) = r \qquad p_2(r,s) = s$$

for all $(r,s) \in R \times S$. We then see that $\ker p_1 \simeq S$ and $\ker p_2 \simeq R$ and so

$$\ker p_1 \times \ker p_2 \simeq R \times S.$$

Chapter 7

Ideals and quotient rings

Lecture 12
On 14/11

Definition 7.1 (Ideal)**.** A subset I of a ring R is called an **ideal** if it is closed under addition and for every $r \in R$ and $x \in I$ we have $rx \in I$ and $xr \in I$.

We can think of ideals as *black holes*. Once we are in an ideal, we cannot escape it by addition within the ideal or even multiplication with elements outside the ideal. We can also define **left ideals** which are closed under addition and closed only under left multiplications by elements in R and similarly for **right ideals**. When R is commutative, all of the notions coincide (ofcourse).

Remark. Note that if I is an ideal, then $x \in I \Rightarrow (-1)x \in I$. Thus, ideals are *almost* subrings, except that it usually does not contain the identity $1 \in R$.

Example. (i) For any $n \in \mathbb{Z}$, the set $(n) = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is an ideal.

(ii) Let R be a commutative ring. Let $a \in R$. Then

$$(a) := \{ra : r \in R\}$$

is a set which is closed under addition (clearly). For any $x \in R$, we have $x \cdot ra = xra \in (a)$ (so is an ideal). Infact, we call this the **principle ideal** generated by a.

(iii) Similarly, let R be commutative and let $a_1, \ldots, a_n \in R$. Then

$$(a_1, \ldots, a_n) := \{r_1 a_1 + \ldots + r_n a_n : r_i \in R\}$$

is an ideal of R. We say that $(a_1, \ldots, a_n)$ is generated by elements $a_1, \ldots, a_n$. Thus a principle ideal is generated by a single element. It is clear to see that an ideal with contain its generator (consider $1 \in R$).

(iv) Let R be a ring. Let $I \subset R$ be an ideal and suppose that I contains a unit $u \in R^{\times}$. Then $u^{-1}u = 1 \in I$ and so $r \cdot 1 = r \in r$ for any $r \in R$. Thus $R \subset I$ and so $R = I$.

We can go further with this. If F is a field, then any non-zero element is a unit. So an ideal in F is either 0 or F itself.

Lemma 7.2. Let R be a commutative ring. Then the ideals $I_1 = (a_1, \ldots, a_m)$ and $I_2 = (b_1, \ldots, b_n)$ are equal if and only if $a_1, \ldots, a_m \in I_2$ and $b_1, \ldots, b_n \in I_1$.

Proof. It is clear to see that if $I_1 = I_2$, then $a_1, \ldots, a_m \in I_1 = I_2$ and similarly $b_1, \ldots, b_n \in I_2 = I_1$. To prove the other way we look at the definitions of our ideals:

$$I_1 = \{r_1 a_1 + \ldots + r_m a_m : r_i \in R\}$$

and

$$I_2 = \{r_1 b_1 + \ldots + r_n b_n : r_i \in R\}.$$

As $a_1, \ldots, a_m \in I_2$, then for all $r_1, \ldots, r_m \in R$, $a_1 r_1, \ldots, a_m r_m \in I_2$. Using the fact that I_2 is closed under addition we see that $a_1 r_1 + \ldots + a_m r_m \in I_2$. Thus $I_1 \subset I_2$. We can use this argument to prove the other statement, concluding $I_2 \subset I_1 \Rightarrow I_1 = I_2$. $\square$

Example. Let $R = \mathbb{Z}[\sqrt{-5}]$. Prove that $(1 - \sqrt{-5}, 2) = (1 + \sqrt{-5}, 2)$.

Solution. From the last Lemma, it is enough to show that all of the generators exist in the ideal.

$$1 - \sqrt{-5} = (-1)(1 + \sqrt{-5}) + (1)(2) \in (1 + \sqrt{-5}, 2).$$

Similarly,

$$1 + \sqrt{-5} = (1)(2) + (-1)(1 - \sqrt{-5}) \in (1 - \sqrt{-5}, 2)$$

and so $(1 - \sqrt{-5}, 2) = (1 + \sqrt{-5}, 2)$. $\square$

Ideals can also be seen as kernels of some homomorphism.

Lemma 7.3. Let R be a ring and let $I \subset R$ be a subset. Then the following are equivalent:

(i) I is an ideal;

(ii) $I = \operatorname{Ker} f$ for some homomorphism $f : R \to S$.

Proof. Assume that $I = \operatorname{Ker} f$ for some f (homomorphism) and ket $x, y \in I$ and $r \in R$. Then $f(x + y) = f(x) + f(y) = 0$. So $x + y \in I$. Moreover, $f(rx) = f(r)f(x) = 0$ so $rx \in I$ (and similarly for $xr \in I$. We will only be able to prove the converse once we have developed a notoin of quotients of rings modulo ideals. $\square$

Example. (i) For any ring R we have the trivial ideals $0 := \{0\}$ and R itself. The ideal 0 is the kernel of the identity homomorphism and R is the kernel of the zero map.

(ii) $n\mathbb{Z}$ is an ideal of Z for any $n \in \mathbb{Z}$. It is the kernal of the reduction map $\mathbb{Z} \to \mathbb{Z}/n$, $a \mapsto \bar{a}$.

(iii) Consider the *evaluation map* $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ given by $\phi(f(x)) = f(1)$. It is easy to check that ϕ is a homomorphism. It is surjective because for any $a \in \mathbb{Q}$ the constant polynomial $a \in \mathbb{Q}[x]$ maps to a under ϕ. The kernel of ϕ is

$$\operatorname{Ker}\phi = \{f(x) \in \mathbb{Q}[x] : f(1) = 0\} = \{(x-1)g(x) : g(x) \in \mathbb{Q}[x]\};$$

hence, $\operatorname{Ker}\phi$ is the principle ideal $(x-1)$ in $\mathbb{Q}[x]$.

7.1 Quotients of rings by ideals

Lecture 13 On 19/11

Example. Here we will construct quotient rings for $F[x]$ for a field F. Let $f(x) = x^3+1 \in \mathbb{Q}[x]$. Conceptually, $\mathbb{Q}[x]/(f(x))$ consists of all different remainders after dividing $f(x)$. Using the Euclidean algorithm, the set of polynomials ios given by all polynomials of degree less than or equal to 2. Therefore, we define

$$\mathbb{Q}[x]/(f(x)) = \{\overline{\gamma(x)} : \gamma(x) \in \mathbb{Q}[x], \deg\gamma \leq 2\}.$$

So if $g(x) \in \mathbb{Q}[x]$, using the division algorithm

$$g(x) = q(x)f(x) + r(x)$$

where $\deg r \leq 2$. We define

$$\overline{g(x)} = \overline{\gamma(x)}.$$

We associated $g(x)$ with its remainder after dividing by $f(x)$. So, for example, we have $\overline{x^3+1} = \overline{0}$ and $\overline{x^4+x+2} = \overline{x(x^3+1)+2} = \overline{2}$. Moreover, we can define addition and multiplication as before

$$\overline{f_1(x)} + \overline{f_2(x)} = \overline{f_1(x) + f_2(x)}$$
$$\overline{f_1(x)} \cdot \overline{f_2(x)} = \overline{f_1(x) \cdot f_2(x)}.$$

For example,

$$\overline{x+1} + \overline{3x+2} = \overline{4x+3}$$
$$(\overline{x+1}) \cdot (\overline{3x+2}) = \overline{(x+1)(3x+2)}.$$

Lecture 14 On 21/11

Definition 7.4 (Coset)**.** Let $I \subset R$ be an ideal in the ring R. Then given any $x \in R$ we define the **coset** of x to be the set

$$\bar{x} \coloneqq x + I \coloneqq \{x + r : r \in I\} \subset R.$$

x is said to be a **representative** of $x + I$.

The following lemam says that distinct cosets are either disjoint or equal.

Lemma 7.5. Let $x, y \in R$. Then

$$x + I = y + I \iff x + I \cap y + I \neq \emptyset \iff x - y \in I.$$

Proof. The first $\Rightarrow$ is obvious. To prove the second $\Rightarrow$, if $x+I \cap y+I \neq \emptyset$ then this means there exists $r_1, r_2 \in I$ such that

$$x + r_1 = y + r_2 \Rightarrow x - y = r_2 - r_1 \in I.$$

Now for the last (circular) $\Rightarrow$, we know that $x - y \in I$. So $x - y = r'$ for $r' \in I$. So $x = y + r'$. Therefore

$$x + I = \{x + r : r \in R\} = \{y + r' + r : r, r' \in R\} \subset y + I;$$

a similar result can be obtained for $y + I$ to show that $x + I = y + I$. □

We are now going to (roughly) define our quotient ring. We define R/I to be the set of all distinct cosets of R by I, that is

$$R/I \coloneqq \{\bar{x} : x \in R\} = \{x + I : x \in R\}.$$

We can now define addition and multiplication on the cosets by

$$(x + I) + (y + I) \coloneqq (x + y) + I$$
$$(x + I)(y + I) \coloneqq xy + I.$$

Initially, it is not obvious that this is well-defined. That is, independent of representatives. For addition to be well defined we need

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

where $x, y, x', y' \in R$, where x, x' are representatives for $x + I$ and y, y' are representatives for $y + I$. Recall that we have $x + I = x' + I$ means that $x - x' \in I$, so similarly $y - y' \in I$. Since I is an ideal, it is closed under addition so

$$x - x' + y - y' = (x + y) - (x' + y') \in I$$

and so

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

Similarly, for multiplication we have that $x - x' \in I$ and $y - y' \in I$. As I is closed under multiplication for elements in R,

$$(x - x')y \in I \qquad (y - y')x' \in I$$

and by adding these together we get

$$xy - x'y' \in I$$

as required.

Definition 7.6 (Quotient)**.** Let R be a ring and $I \subset R$ be an ideal. Then the ring R/I is called the **quotient** of R by I, or $R \bmod I$. Its elements $x + I$ for $x \in R$ are called **residue classes** $(\bmod\, I)$, and are sometimes denoted $\bar{x}$.

Now lets look at an example to try and make this look a little bit less abstract.

Example. Let $R = \mathbb{Z}[i]$ and $I = (2-i)$. Let's work out what the quotient R/I looks like. First, we need to find representatives of its elements. Every element in R/I is of the form

$$a + bi + (2-i), \qquad a, b \in \mathbb{Z}$$

but when are two such elements equal in R/I? We have

$$\overline{a+bi} = \overline{c+di}$$

if and only if

$$2 - i \mid (a+bi) - (c+di).$$

So, for example, $2 - i + (2-i) = 0 + (2-i)$ (as $2 - i \mid 2 - i - 0$), so

$$\overline{2-i} = \overline{0}$$

and so

$$\overline{2} = \overline{i}.$$

Hence

$$\overline{a+bi} = \overline{a} + \overline{2b} = \overline{a+2b}$$

and so every element in R/I has a representative in $\mathbb{Z}$. We can restrict the distinct equivalence classes $\bmod I$ further. Namely, squaring both sides of $\overline{2} = \overline{i}$ we get

$$\overline{4} = \overline{-1}$$

and so $\overline{5} = \overline{0}$. Thus, the equivalence classes are only different $\bmod 5$, that is, we have at most five elements in R/I:

$$0 + I, 1 + I, 2 + I, 3 + I, 4 + I.$$

Now, is it possible to reduce this further? We assume that $a, b \in \mathbb{Z}$ are such that $\overline{a} = \overline{b}$. That is,

$$a - b \in (2-i) \Rightarrow a - b = (x + iy)(2-i)$$

for some $x, y \in \mathbb{Z}$. This is equivalent to

$$a - b = 2x + y + (2y - x)i$$

and so

$$2x + y = a - b, \quad 2y - x = 0.$$

These equations imply that $5y = a - b$, that is $a = b \bmod 5$; so our representatives are indeed distinct.

Lecture 15
On 5/12

We previously defined $\mathbb{Q}[x]/(x^3+1)$, now we will make the idea of quotients of polynomial rings more rigorous.

Theorem 7.7 (Quotients of polynomial rings)**.** Let F be a field and $f(x) \in F[x]$ where $\deg f \geq 0$. Then

$$F[x]/(f(x)) = \{\overline{a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}} : a_i \in F\}.$$

Moreover, all above cosets are *distinct*.

Lecture 16
On 10/12

Proof. This theorem is equivalent to saying that $F[x]/(f(x))$ is a vector space over F with basis

$$B = \{\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}\}$$

where $\deg f = n$. It is clear that $F[x]/(f(x))$ as it is an abelian group with scalar multiplication given by

$$\alpha \cdot (g(x)) = \alpha g(x)$$

for $\alpha \in F$ and $g(x) \in F[x]$. Now we must show that B spans $F[x]/(f(x))$. By long division, for any $g(x) \in F[x]$ with $\deg g \geq 0$ we have

$$g(x) = q(x)f(x) + r(x)$$

where $\deg r < n$; hence,

$$\overline{g(x)} = \overline{r(x)} \Rightarrow g(x) - r(x) \in (f(x))$$

as B spans all polynomials in $\bar{x}$ up to degree $n-1$ it will contain $\overline{r(x)}$ and so $\overline{g(x)}$. If $\sum_{i=0}^{n-1} a_i \bar{x}^i = \bar{0}$ then $\sum_{i=0}^{n-1} a_i x^i \in (f(x))$ and so $f(x)$ divides $\sum_{i=0}^{n-1} a_i x_i$ hence $\deg f = n \leq n-1$; a contradiction. Therefore, $a_0 = a_1 = \ldots = 0$ and so B is a basis. □

Example. Consider $\mathbb{Q}[x]$ with ideal $I = (x^2 + x + 1)$. By the above theorem

$$\mathbb{Q}[x]/(f(x)) = \{\overline{r(x)} = \deg(r(x)) \leq 1\}.$$

Then, for example, $\overline{x^2 + x + 1} = \bar{0}$ then $\bar{x}^2 = \overline{-x-1}$. Suppose $p(x) = x^4 - 3x^2 + 2$. We have that

$$\bar{x}^4 = (\bar{x}^2)^2 = (\overline{-x-1})^2 = \overline{x^2 + 2x + 1} = \overline{x^2 + x + 1} + \bar{x} = \bar{x}.$$

It can easily be shown from that $4x+5$ is the coset representation of $x^4 - 3x^2 + 2$ as $\overline{p(x)} = \overline{4x+5}$.

Example. Let $R = \mathbb{Z}/3[x]$ and $I = (x^4 + x + 1)$. Then R/I is a $\mathbb{Z}/3$ vector space over $\{\bar{1}, \bar{x}, \bar{x}^2, \bar{x}^3\}$. Hence

$$R/I = \left\{ \sum_{i=0}^{3} \overline{a_i x^i} : a_i \in \mathbb{Z}/3 \right\}.$$

Remark. Consider the quotient ring R/I. R/I can be commutative or non-commutative. If R is commutative, so is R/I. R/R is isomorphic to the zero ring, which is commutative. On the other side of things, $R/0$ is isomorphic to R (clearly).

Example (Quotient map)**.** Let R be a ring and I be an ideal. We have that the map $f : R \to R/I$ such that

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

By construction we have that

$$\ker f = I \qquad \text{and} \qquad \operatorname{im} f = R/I.$$

Hence, we have proved that all ideals are the kernal of a homomorphism.

Example. Let $R = \mathbb{Z}[i]$. Consider $I = (2)$.

(i) Show that R/I has exactly 4 elements.

(ii) Give the tables for addition and multiplication in R/I.

(iii) Is R/I isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ or $\mathbb{Z}/4$ as a ring?

Solution. (i) Let $\alpha = a + bi \in \mathbb{Z}[i]$. We have that

$$a = 2k + a' \qquad \text{and} \qquad b = 2l + b'$$

where $a', b' \in \{0, 1\}$. Then

$$\alpha = (2k + a') + (2l + b')i = (a' + b'i) + 2(k + li).$$

Therefore, $\bar{\alpha} = (a' + b'i) \in R/I$. Hence, there at at most 4 elements in R/I. Now we just need to show that they are distinct. We assume that $\overline{a' + b'i} = \overline{c' + d'i}$ where $a', b', c', d' \in \{0, 1\}$. So

$$\begin{aligned}
\overline{(a' + b'i) - (c' + d'i)} &= \bar{0} \\
\overline{(a' - c') + (b' - d')i} &= \bar{0} \\
\overline{(a' - c') + (b' - d')i} &\in I = (2) \\
(a' - c') + (b' - d')i &= 2(e + fi)
\end{aligned}$$

for some $e, f \in \mathbb{Z}$. However, $a' - c' \in \{0, \pm 1\}$ so $a' = c'$. Similarly, $b' = d'$.

(ii)

$+$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{1+i}$	$\bar{i}$
$\bar{i}$	$\bar{i}$	$\overline{1+i}$	$\bar{0}$	$\bar{1}$
$\overline{1+i}$	$\overline{1+i}$	$\bar{i}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{i}$	$\overline{1+i}$
$\bar{i}$	$\bar{0}$	$\bar{i}$	$\bar{1}$	$\overline{1+i}$
$\overline{1+i}$	$\bar{0}$	$\overline{1+i}$	$\overline{1+i}$	$\bar{0}$

(iii) $x \in R/I \Rightarrow \overline{x + x} = \bar{0}$ (which is preserved by a ring isomorphism) and in $\mathbb{Z}/4$ we have that $\bar{1} + \bar{1} = \bar{2} \neq \bar{0}$. Hence, R/I is not isomorphic to $\mathbb{Z}/4$. In $\mathbb{Z}/2 \times \mathbb{Z}/2$ we have that $\overline{x}^2 = \overline{x}$ which is preserved by a ring isomorphism which is clearly not held in R/I; therefore, R/I is also not ismorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

□

Lecture 17
On 11/12

Theorem 7.8 (First isomorphism theorem)**.** Let $\varphi : R \to S$ be a ring homomorphism. Then the map

$$\bar{\varphi} : R/\ker\varphi \to \operatorname{im}\varphi$$

defined by

$$\bar{x} \to \varphi(x)$$

(that is, $\overline{\varphi}(\bar{x}) = \varphi(x)$) is a well-defined isomorphism. That is,

$$R/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. First, we must show that $\bar{\varphi}$ is well-defined. Let $x, x' \in R$ such that $\bar{x} = \overline{x'}$. Then $x - x' \in \ker\varphi$ and so

$$\varphi(x - x') = 0.$$

As φ is a homomorphism, we have that $\varphi(x) = \varphi(x')$ and so

$$\overline{\varphi}(\overline{x}) = \overline{\varphi}(\overline{x'});$$

hence $\bar{\varphi}$ is well-defined. It is clear that $\bar{\varphi}$ is a homomorphism as

$$\overline{\varphi}(\overline{x} + \overline{y}) = \overline{\varphi}(\overline{x + y}) = \varphi(x + y) = \varphi(x) + \varphi(y) = \overline{\varphi}(\overline{x}) + \overline{\varphi}(\overline{y}).$$

Now, we must show that it is bijective and thus a isomorphism. The kernal of $\overline{\varphi}$ is zero as

$$\overline{\varphi}(\overline{x}) = 0 \Longleftrightarrow \varphi(x) = 0 \Longleftrightarrow x \in \ker\varphi \Longleftrightarrow \bar{x} = \bar{0}$$

and so $\overline{\varphi}$ is injective. $\overline{\varphi}$ is surjective as for all $y \in \operatorname{im}\varphi$ there exists an $x \in R$ such that $\varphi(x) = y$; therefore,

$$\overline{\varphi}(\overline{x}) = y$$

as required. ☐

Example. Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be the evaluation map

$$\varphi(f(x)) = f(i)$$

where $i^2 = -1$. If i is a root, then so is its conjugate $-i$ (this is a property of real polynomials). Hence, if $f(i) = 0$ then $f(x)$ has a factor $x^2 + 1$, and so

$$\ker\varphi = (x^2 + 1).$$

Since φ is surjective, the first isomorphism theorem yields

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C};$$

we could have *defined* $\mathbb{C}$ to be $\mathbb{R}/(x^2 + 1)$!

7.2 Prime and maximal ideals

Lecture 18
On 12/12

We have two main types of ideals of importance in ring theory.

Definition 7.9 (Prime ideal)**.** An ideal I of a commutative ring R is **prime** if

(i) for all $a, b \in R$ such that $ab \in I$ we have $a \in I$ or $b \in I$; and

(ii) $I \neq R$.

Example. (i) The set of real numbers is a prime ideal of $\mathbb{Z}$.

(ii) $I = (2, x)$ is a prime ideal of $\mathbb{Z}[x]$.

(iii) Let $p \in \mathbb{Z}$. Then p is prime iff $(p) = p\mathbb{Z}$ is a non-zero prime ideal.

(iv) (2) is *not* a prime ideal of $\mathbb{Z}[i]$ as $(1-i)(1+i) = 2 \in (2)$ *but* $1 \pm i \notin (2)$.

There is a similarity between prime elements and prime ideals, which may be seen in the above examples. If $x \in R$ is a prime element, then $I = (x) \subset R$ is a prime ideal. Conversely, if $I = (x) \subset R$ is a prime ideal then $x \in R$ is a prime element; however, there exists prime ideals that are not principal. Therefore, prime ideals are more general then prime elements. We also see that

$$x \in (a) \iff (x) \subset (a) \iff x \mid a.$$

Definition 7.10 (Maximal ideal)**.** An ideal I of a ring R is **maximal** if

(i) the only ideals of R containing I are R and I; and

(ii) $I \neq R$.

Example. (i) If F is a field, the only maximal ideal is $\{0\}$.

(ii) In the ring $\mathbb{Z}$, the maximal ideals are the principal ideals generated by a prime number.

Proposition 7.11. Let I be an ideal of a commutative ring R. Then

(i) I is prime iff R/I is an integral domain; and

(ii) I is maximal iff R/I is a field.

Proof. (i) First let us prove that I is prime $\Rightarrow$ R/I is an integral domain. Assume I is prime. Let $\overline{a}, \overline{b} \in R/I$. Then if $\overline{ab} = \overline{0}$ then $ab \in I$. So either $a \in I$ or $b \in I$. Hence $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. Therefore, R/I is an integral domain. Now, let us prove that R/I is an integral domain $\Rightarrow$ I is prime. Assume that R/I is an integral domain. Now let $a, b \in R$ such that $ab \in I$. Then $\overline{ab} = \overline{0}$. So $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. Therefore $a \in I$ or $b \in I$; and so I is prime.

(ii) First, we will prove that I being maximal $\Rightarrow R/I$ field. Assume that I is maximal. Then we have a representation x for every non-zero element in R/I such that $x \notin I$ (clearly). So we have

$$(I, x) = R = (1).$$

It is clearly closed under addition and multiplication by $r \in R$, so there exists $y \in R$ and $m \in I$ such that

$$xy + m = 1.$$

Hence $\overline{xy} = \overline{1}$ and so R/I is a field. Now to prove the other direction. Assume that R/I is a field and let $x \in R$ such that $x \notin I$ (that is, $\overline{x} \neq \overline{0}$). Then there exists $\overline{y} \in R/I$ such that

$$\overline{xy} = \overline{1}.$$

Hence

$$xy = 1 + m$$

for some $m \in I$. So we have $1 \in (x, I)$. Hence, $(x, I) = R$. Now let J be some other ideal such that $I \subset J$ and $I \neq J$. Now, there must exist some $x \in J$ such that $x \notin I$. Hence

$$I \subset (I, x) \subset J$$

but as $R = (I, x)$, we have that $J = R$ and so I is maximal.

□

Lemma 7.12. If an ideal R of a ring R is maximal, then it is prime.

Proof. $I \subset R$ is maximal $\iff R/I$ is a field $\iff R/I$ is an integral domain $\iff$ I is prime. □

Example. (i) Recall that $R[x]/(x^2 + 1) \cong \mathbb{C}$. As $\mathbb{C}$ is a field, $(x^2 + 1)$ is maximal.

(ii) Let $R = \mathbb{Z}[i]$ and $I = (2)$. $(\overline{1+i})(\overline{1+i}) = \overline{0}$, so R/I is *not* an integral domain, so I is not maximal.

(iii) Let $R = \mathbb{Z}[i]$ and $I = (2 - i)$. It can be shown that $R/I \cong \mathbb{Z}/5$. As 5 is prime, $\mathbb{Z}/5$ is a field and so I is a maximal ideal of R.