Honours Algebra - Week 4 - Rings

Antonio León Villares

February 2022

Contents

Based on the notes by Iain Gordon, Sections 3.1 - 3.4

1 Recap: Groups

A group is a set satisfying 4 conditions under a given operation $*$. The **group axioms** are:

1. **Closure**:
$$g, h \in G \implies g * h \in G$$
2. **Associativity**:
$$g, h, k \in G \implies g * (h * k) = (g * h) * k$$
3. **Identity**:
$$\exists e_G \in G : \forall g \in G, e_G * g = g * e_G = g$$
4. **Existence of Inverse**:
$$g \in G \implies g^{-1} \in G : gg^{-1} = g^{-1}g = e_G$$

A group is called **abelian** if $*$ defines a commutative operation:

$$g * h = h * g$$

2 Rings

2.1 Defining Rings

- **What is a ring?**
  - a special **set** armed with **2 operations**: addition and multiplication
  $$(R, +, \cdot)$$
  - **rings** have the following properties:
    1. $(R, +)$ is an **abelian group**, with identity 0_R
    2. $(R, \cdot)$ is a **monoid**:
       * multiplication is **associative**
       * R contains an identity element 1_R satisfying:
       $$\forall a \in R \ : \ a \cdot 1_R = 1_R \cdot a = a$$
    3. the **distributive law** holds in R:
    $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
    $$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$
- **What is a commutative ring?**
  - a **ring** for which **multiplication** is also **commutative**:
  $$a \cdot b = b \cdot a$$
- **What is the zero ring?**
  - the **ring**:
  $$R = \{0\}$$

  - any ring that is not a zero ring is a **non-zero ring**

- **How do rings differ from vector spaces?**
  - the key difference is that **rings** are defined with a **set multiplication operation**
  - on the other hand, vector spaces define **scalar multiplication over a field**

- **Do elements in rings have inverses?**
  - additively, rings are a group, so there is always an **additive inverse**
  - however, multiplicatively, we only require R to be a monoid, so a **multiplicative inverse** might not exist

- **What is a unital ring?**
  - some definitions treat the above definition as a **unital ring**
  - in said definitions, the set $(R, \cdot)$ is not a **monoid**, but rather a **semigroup**: multiplication is still associative, but an identity element need not exist

2.1.1 Examples: Rings

- $\mathbb{Z}$ is a prime example of a ring, with addition and multiplication defined in the standard way.
  - indeed, $\mathbb{Z}$ is an example of a **commutative ring**
  - it also exemplifies how rings don't require a multiplicative inverse (since for example 2 has no such inverse, as $\frac{1}{2} \notin \mathbb{Z}$)
- standard sets like $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all **commutative rings**, and in fact, have multiplicative inverses
- the set $Mat(n; R)$ of $n \times n$ matrices with entries in the ring R is also a ring (with operations as matrix addition and multiplication)
  - if $n \geq 2$, $Mat(n; R)$ is **not** commutative

2.1.2 Examples: Non-Rings

- $\mathbb{N}$ under standard addition and multiplication is not a ring
  - addition doesn't define an abelian group (for example, 2 has no additive inverse, since $-2 \notin \mathbb{N}$)
- $\mathbb{R}^2$ is not a ring under vector addition and the dot product, since the dot product is a mapping $\mathbb{R}^2 \to \mathbb{R}$
- $\mathbb{R}^3$ is not a ring under vector addition and the cross product, since the cross product doesn't satisfy **associativity**:

$$\left(\begin{pmatrix}1\\0\\0\end{pmatrix} \times \begin{pmatrix}0\\1\\0\end{pmatrix}\right) \times \begin{pmatrix}0\\1\\0\end{pmatrix} = \begin{pmatrix}-1\\0\\0\end{pmatrix} \neq \begin{pmatrix}0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\end{pmatrix} \times \left(\begin{pmatrix}0\\1\\0\end{pmatrix} \times \begin{pmatrix}0\\1\\0\end{pmatrix}\right)$$

2.2 The Integers Modulo m

Most of the following is taken from here: Lecture 11 - Congruence and Congruence Classes

- **When are integers said to be "congruent modulo m"?**
  - let $a, b, m \in \mathbb{Z}$
  - we say that a and b are **congruent modulo** m if m divides $b - a$
  - we write this using:

    $$a \equiv b \ (mod\ m)$$

  - this indicates that a, b have the same **reminder** when divided by m

- **What are the rules of congruences?**

  1. $$a \equiv a \ (mod\ m)$$
  2. $$m \equiv 0 \ (mod\ m)$$
  3. $$a \equiv b \ (mod\ m) \implies b \equiv a \ (mod\ m)$$
  4. $$a \equiv b \ (mod\ m) \ \&\ b \equiv c \ (mod\ m) \implies a \equiv c \ (mod\ m)$$
  5. $$a \equiv b \ (mod\ m) \ \&\ c \equiv d \ (mod\ m) \implies a + c \equiv b + d \ (mod\ m)$$
  6. $$a \equiv b \ (mod\ m) \ \&\ c \equiv d \ (mod\ m) \implies ac \equiv bd \ (mod\ m)$$

- **What is a congruence class?**
  - the set of all integers which are congruent to $a \in \mathbb{Z}$ modulo $m \in \mathbb{Z}$. In other words, the set:

    $$\bar{a} = \{b \mid a \equiv b \ (mod\ m) \iff a - b = kn, k \in \mathbb{Z}\}$$

  - for example, if $m = 2$, then $\bar{0}$ is the set of all **even** numbers; $\bar{1}$ is the set of all **odd** numbers
  - if $\bar{a} = \bar{b}$, then $a \equiv b \ (mod\ m)$
  - using the above rules of congruences, it is easy to see that:

    $$\bar{a} + \bar{b} = \overline{a + b}$$

    $$\bar{a}\bar{b} = \overline{ab}$$

- **What are the integers modulo m?**
  - a **ring** written as:

    $$\mathbb{Z}/m\mathbb{Z}$$

  - $\mathbb{Z}/m\mathbb{Z}$ is the set containing the m congruence classes modulo m:

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

  - this is a ring, since it inherits the properties of the integers

- notice, the following are equivalent notations:

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$$

- **How can we work in this ring?**
  - an example is the **ring of time**:

$$\mathbb{Z}_{12}$$

  - we know that "4 hours after 10 0'clock is 2 o'clock" because:

$$\bar{1}\bar{0} + \bar{4} = \overline{14} = \bar{2}$$

  - similarly "3 periods 8 hours long make up a day" because:

$$\bar{3}\bar{8} = \overline{24} = 0$$

2.3 Proposition: Divisibility by Sum

A natural number is divisible by 3 precisely when the sum of its digits is divisible by 3. The same applies when using 9. [Proposition 3.1.7]

Proof. Let $n \in \mathbb{N}$. If n is a k digit number with digits $a_0, a_1, \ldots, a_{k-1}$, it can be written as:

$$n = \sum_{i=0}^{k-1} a_i \times 10^i$$

Notice:

$$\overline{10^i} \equiv 1 \ (mod\ 3)$$

(and

$$\overline{10^i} \equiv 1 \ (mod\ 9)$$

)

Hence:

$$n \equiv \sum_{i=0}^{k-1} a_i \ (mod\ 3)$$

It follows that n is divisible by 3 (or 9) precisely when the sum of its digits $\sum_{i=0}^{k-1} a_i$ is also divisible by 3 (or 9).

□

2.3.1 Exercises (TODO)

1. **Show that a natural number is divisible by 11 if and only if the alternating sum o fits digits is divisible by 11.**
2. **Show that an integer of the form *abcabc* (such as 123123) is always divisible by 7.**
3. **Show that an integer congruent to 3 modulo 4 is never the sum of two squares. Show also that an integer congruent to 7 modulo 8 is nver the sum of three squares.**

2.4 (Re)Defining Fields

- **What is a field?**
  - a **field** is a **non-zero** commutative **ring**
  - every non-zero element in a field has a **multiplicative inverse**:

$$a \in F \implies a^{-1} \in F \ : \ aa^{-1} = a^{-1}a = 1_F$$

2.4.1 Examples

- the ring $\mathbb{Z}_3$ is a field (which we have been calling $\mathbb{F}_3$), since:

$$1 \cdot 1 = 1$$

$$2 \cdot 2 = 1$$

- the ring $\mathbb{Z}_{12}$ is **not** a field, since neither $\bar{3}$ nor $\bar{8}$ have inverses. The proof of this is pretty cool:
  - notice that $\bar{3} \cdot \bar{8} = \overline{24} = \bar{0}$
  - assume $\exists \bar{a} \in \mathbb{Z}_{12}$ such that:

$$\bar{a} \cdot \bar{3} = \bar{1}$$

  - but then we must have:

$$(\bar{a} \cdot \bar{3}) \cdot \bar{8} = \bar{8}$$

  - applying associativity of ring multiplication:

$$(\bar{a} \cdot \bar{3}) \cdot \bar{8} = \bar{a} \cdot (\bar{3} \cdot \bar{8}) = 0$$

  - hence, no such a can exist
  - we can use similar arguments for the right inverse

2.5 Proposition: Integers Modulo as Fields

> *Let $m \in \mathbb{Z}^+$. The **commutative ring** $\mathbb{Z}_m$ is a field **if and only if** m is **prime**. [Proposition 3.1.11]*

Proof. Suppose that $\mathbb{Z}_m$ is a field, and consider $a \in \mathbb{Z} : 1 < a < m$. Since $a \neq 0$, it follows that $\bar{a} \in \mathbb{Z}_m$ has an inverse $\bar{a}^{-1}$. Define:

$$\bar{b} = \bar{a}^{-1}$$

Then:

$$\overline{ab} = \bar{a} \cdot \bar{b} = 1$$

In other words, by properties of congruences:

$$ab - 1 = km \implies ab = km + 1$$

Notice, the LHS and RHS must both be divisible by a. Since a can't divide 1, the RHS can only be divisible by a if a doesn't divide km (if a divided km, $km + 1$ wouldn't be divisible by a). Hence, it must mean that, in particular, a doesn't divide m. Thus, m must be prime, since a was an arbitrary number between 1 and m.

Alternatively, assume that m is prime. Then, for $a \in \mathbb{Z}, 1 < a < m$, we know that:

$$hcf(a, m) = 1$$

By the Euclidean Algorithm (this will be displayed in the exercise below), it follows that $\exists b, c \in \mathbb{Z}$ such that:

$$ab + mc = 1$$

In other words, $ab - 1$ divides m, so:

$$ab \equiv 1 \ (mod \ m) \implies \overline{ab} = \bar{1} \implies \bar{a} \cdot \bar{b} = 1$$

So $\bar{a}$ has an inverse in $\mathbb{Z}_m$.

□

2.5.1 Exercises

1. **Find the inverse of 24 in the field $\mathbb{F}_{37}$**

   Notice, 24 and 37 are coprime, so $hcf(24, 37) = 1$. By the Euclidean Algorithm, we can find $a, b \in \mathbb{Z}$ such that:

   $$37a + 24b = 1$$

   We thus apply the Euclidean Algorithm:

   $$\begin{aligned} 37 &= 24 \times 1 + 13 \\ 24 &= 13 \times 1 + 11 \\ 13 &= 11 \times 1 + 2 \\ 11 &= 2 \times 5 + 1 \end{aligned}$$

   We then backtrack:

   $$\begin{aligned} 11 = 2 \times 5 + 1 &\implies 1 = 11 - 2 \times 5 \\ 13 = 11 \times 1 + 2 &\implies 1 = 11 - (13 - 11) \times 5 = 11 \times 6 - 13 \times 5 \\ 24 = 13 \times 1 + 11 &\implies 1 = (24 - 13) \times 6 - 13 \times 5 = 24 \times 6 - 13 \times 11 \\ 37 = 24 \times 1 + 13 &\implies 1 = 24 \times 6 - (37 - 24) \times 11 = 24 \times 17 - 37 \times 11 \end{aligned}$$

   Hence, we have that:

   $$24 \times 17 - 37 \times 11 = 1$$

   Working in $\mathbb{Z}_{37}$ we get that:

   $$\bar{24} \cdot \bar{17} = \bar{1}$$

   So 17 is the inverse of 24 in $\mathbb{Z}_{37}$.

3 Properties of Rings

This section focuses on deriving the basic properties of rings. Most of the things are common sense, and tedious to prove, so I won't include many of these proofs.

3.1 Lemma: Multiplying by Zero and Negatives

*Let R be a **ring** and let $a, b \in \mathbb{R}$. Then:*

1. $0a = 0 = a0$
2. $(-a)b = -(ab) = a(-b)$
3. $(-a)(-b) = ab$

[Lemma 3.2.1]

3.2 Remark: Consequences of the Distributive Axiom

If R is a ring, and $a, b, c, d \in R$ then:

1. *(a + b)(c + d) = ac + ad + bc + bd*
2. *a(b - c) = ab - ac*

*Notice, since R is a ring we **can't** assume that $ac = ca$: the order of multiplication matters! [Remark 3.2.2.1]*

3.3 Remark: Additive Identity Equal to Multiplicative Identity

*If $0_R = 1_R$, then R is the **zero ring**. [Remark 3.2.2.2]*

Proof.

$$a = a \cdot 1_R = a \cdot 0_R = 0_R$$

So any element in R must be 0_R. □

3.4 Lemma: Rules for Multiples

Let R be a ring, and $a, b \in \mathbb{R}$, with $m, n \in \mathbb{Z}$. Then:

1. $m(a+b) = ma + mb$
2. $(m+n)a = ma + na$
3. $m(na) = (mn)a$
4. $m(ab) = (ma)b = a(mb)$
5. $(ma)(nb) = (mn)(ab)$

[Lemma 3.2.4]

4 Units

4.1 Defining the Unit

- **What is a unit?**
  - let R be a ring
  - $a \in R$ is a unit if $a^{-1} \in R$ exists
  - a is invertible in R

4.1.1 Examples

- in $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ all elements (except 0) are units
- in $\mathbb{Z}$ only 1 and -1 are units (and they are their own inverse)
- for any non-zero ring, 0 is never a unit, since:

$$b \cdot 0 = 0 \neq 1, \quad \forall b \in R$$

4.2 Proposition: Units Form a Group

Let $R^\times$ be the set containing all the units of R. Then, $R^\times$ is a group, called ***the group of units of the ring*** R. *[Proposition 3.2.9]*

Proof. We check the group axioms. Let $a, b \in R^\times$

1. **Closure**: consider ab. Since R is a ring, it is closed under multiplication, so $ab \in R$. This is a unit in R if and only if it has an inverse in R. Indeed, since a, b are units, then $\exists a^{-1}, b^{-1} \in R$. Moreover, $b^{-1}a^{-1} \in R$ too. But then:
$$(b^{-1}a^{-1})(ab) = b^{-1}b = 1_R$$
$$(ab)(b^{-1}a^{-1}) = aa^{-1} = 1_R$$
So in particular, $b^{-1}a^{-1} \in R$ is the inverse of $ab \in R$, so $ab \in R^\times$. Hence, $R^\times$ is closed under multiplication.
2. **Associativity**: multiplication in a ring R is associative; $R^\times \subseteq R$, so multiplication is associative in $R^\times$ too.
3. **Identity**: since 1_R is always its own inverse, it follows that $1_R \in R^\times$, and 1_R is the identity of $R^\times$.
4. **Existence of Inverse**: trivially, if $a \in R^\times$, its inverse a^{-1} must also be in $R^\times$

□

4.2.1 Examples

- as discussed above, we have:
  - $\mathbb{Z}^\times = \{1, -1\}$
  - $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
- for the ring of $n \times n$ matrices, $Mat(n; R)$ we have:
$$Mat(n; R)^\times = GL(n; R)$$
  the general linear group, composed of the invertible $n \times n$ matrices
- $\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ - this is known as the **Klein Four Group** - a group of four elements which are their own inverse

4.2.2 Exercises (TODO)

1. **Let p be prime. We know that the group of units of the field $\mathbb{F}_p$, $\mathbb{F}_p^\times$, is an abelian group of order $p-1$ (that is, it has p elements). Prove, like Gauss did at age 21, that $\mathbb{F}_p^\times$ is cyclic (that is, it has a group element which generates the group).**

5 Integral Domains

5.1 Zero-Divisors

- **What is a zero-divisor (or a divisor of zero)?**
  - a **non-zero** element in a ring, which when multiplied by another **non-zero** element, is 0:
$$a, b \in R, \quad a, b \neq 0 \implies ab = 0 \ \vee \ ba = 0$$
- **Why are zero-divisors strange?**
  - they challenge intuitive notions (i.e a product is only zero when at least one of its elements is 0)
- **Why are zero divisors interesting in $Mat(n; R)$?**
  - consider $A \in Mat(n; R)$

- if $rank(A) = n$, then A is invertible, so A is a unit
- if $rank(A) < n$, by the rank-nullity theorem, $nullity(A) > 0$
  * what this means is that $\exists \underline{v}$ such that:
  $$A\underline{v} = \underline{0}$$
  * now, define a matrix B, with n column vectors given by $\underline{v}$:
  $$B = \begin{pmatrix} \underline{v} & \underline{v} & \dots & \underline{v} \end{pmatrix}$$
  * then:
  $$AB = \begin{pmatrix} A\underline{v} & A\underline{v} & \dots & A\underline{v} \end{pmatrix}$$
  so AB is the zero matrix
  * this then means that A is a **zero-divisor**
- what this shows is that all the elements in $Mat(n; R)$ are either **units** or **zero-divisors**
- this is truly strange:
  * in $\mathbb{Z}$, there are no zero-divisors, and only 2 units (± 1)
  * in fields, every non-zero element is a unit, and there are no zero-divisors

5.1.1 Examples

- $\mathbb{Z}_m$: for example, in $\mathbb{Z}_6$, $\bar{2}, \bar{3}$ are zero-divisors)
- $Mat(n; R)$: for example,
$$\begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

5.2 Defining Integral Domains

- **What is an integral domain?**
  - an **integral domain** is a **non-zero commutative ring** which contains no **zero-divisors**
  - **integral domains** capture our intuitive notions of how **rings** "should" behave (that is, rings which behave like integers)
- **What intuitive properties do integral domains have?**
  - since there are no zero-divisors, then:
    1. $ab = 0 \implies a = 0 || b = 0$
    2. $a, b \neq 0 \implies ab \neq 0$

5.2.1 Examples

- $\mathbb{Z}$ is an integral domain
- $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are integral domains
- any field is an integral domain, since every element is a unit, so they all have inverses
  - if $\exists a \in F$ then $\exists a^{-1}$
  - if $\exists b \in F \ : \ ab = 0$ then:
  $$(a^{-1}a)b = b$$
  but
  $$a^{-1}(ab) = 0$$

- hence, b must be 0 (since otherwise associativity wouldn't be satisfied), so a can't be a zero-divisor

- as discussed above, $\mathbb{Z}_6$ and $Mat(2; R)$ are **not** integral domains
- $\mathbb{Z}_8$ is also not an integral domain, since $\bar{3} \cdot \bar{8} = \bar{0}$

5.3 Proposition: Cancellation Law for Integral Domains

Let R be an integral domain with $a, b, c \in R$. Then:

$$ab = ac \wedge a \neq 0 \implies b = c$$

This is intuitive if we assume that every element in R has an inverse; however, the cancellation law holds even when a has no inverse in R! [Proposition 3.2.15]

Proof. If $ab = ac$ then $a(b - c) = 0$ by the distributivity of a ring. By the properties of an integral domain, this is true if and only if:

- $a = 0$
- and/or $b = c$

Hence, if $a \neq 0$, we must have that $b = c$.

□

If R isn't an integral domain, this won't hold, since, for example, in $\mathbb{Z}_6$:

$$\bar{3} \cdot \bar{1} = \bar{3}$$

$$\bar{3} \cdot \bar{5} = \overline{15} = \bar{9} = \bar{3}$$

5.4 Proposition: Integers Modulo m as Integral Domains

Recall, a **field** is a non-zero **commutative** ring in which **multiplicative inverses** are defined for every element, so in particular **fields** contain no **zero-divisors**.

Integral domains are non-zero **commutative** rings with no **zero-divisors**

Hence, every **field** is an **integral domain**.

We saw in (2.5) that $\mathbb{Z}_m$ is a field if and only if m is prime. This is a special case of the following proposition:

*$\mathbb{Z}_m$ is an integral domain **if and only if** m is prime. [Proposition 3.2.16]*

Proof. Let m be prime. $\mathbb{Z}_m$ is a commutative ring, since $\mathbb{Z}$ is commutative.

Assume that $\bar{k} \in \mathbb{Z}_m$ is a zero-divisor. By definition:

- $\bar{k} \neq 0$
- $\exists \bar{l} \neq \bar{0} \in \mathbb{Z}_m \ : \ \bar{k}\bar{l} = \bar{0}$

In terms of congruences, we have:

$$kl \equiv 0 \ (mod \ m)$$

Hence, m divides kl. Since m is prime, m must divide either k or l (or both). This then means that:

$$k \equiv 0 \ (mod \ m) \implies \bar{k} = \bar{0}$$

or

$$l \equiv 0 \ (mod \ m) \implies \bar{l} = \bar{0}$$

However, this contradicts the fact that $\bar{k}, \bar{l} \neq 0$, so no zero-divisors must exist in $\mathbb{Z}_m$, so it must be an integral domain.

Alternatively, assume that m is not prime. Then, we can write:

$$m = ab, \qquad 1 < a, b < m$$

In particular, a, b are **not** divisible by m, so:

$$\bar{a}, \bar{b} \neq \bar{0}$$

However, clearly:

$$\bar{a}\bar{b} = \bar{0}$$

So $\bar{a}, \bar{b}$ must be zero divisors. Hence, if m is prime, $\mathbb{Z}_m$ can't be an integral domain.

□

5.5 Theorem: Integral Domains as Fields

According to Iain (and I completely agree), this is one of the coolest, sleekest theorems in this topic.

> *Every **finite** integral domain is a **field**. [Theorem 3.2.17*

Notice, we saw before that every field is an integral domain. This tells us that every (finite) integral domain must be a field!

Proof. Let R be a finite integral domain. For R to be a field, we must show that every element $a \in \mathbb{R}$ has a multiplicative inverse (since R by definition is already commutative).

For the first condition, we need to show that if $a \in R$ i non-zero, then $\exists b \in R$ such that:

$$ab = 1$$

To do this, lets define a mapping:

$$\lambda_a : R \to R$$

where:

$$\lambda_a(b) = ab$$

If we can show that λ_a maps to 1, then since a was an arbitrary element of R, every element of R will have an inverse.

The key insight here is that R is finite. Moreover, λ_a is a mapping between sets of equal cardinality. Hence, if λ_a is shown to be injective, it must mean that every element in R is mapped to a unique element in R, so in particular, the mapping will be surjective. In other words, we will have found $b \in R \; : \; \lambda_a(b) = 1$, as required.

To see that λ_a is injective, notice that:

$$\lambda_a(b_1) = \lambda_a(b_2) \implies ab_1 = ab_2$$

Since R is an integral domain, by the **Cancellation Law**, it must be the case that:

$$b_1 = b_2$$

Hence, λ_a is injective, so it is surjective, and so, we can find $b \in R$ such that $ab = 1$. Moreover, by commutativity of R, we also have that $ba = 1$, so clearly, every $a \in R$ has an inverse in R.

□

6 Polynomials

6.1 Defining Polynomials

- **What is a polynomial?**
  - we define polynomials over a **ring** R as expressions like:

    $$P = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

    where $n \in \mathbb{N}$ and $a_i \in R$
  - the set of all such polynomials is denoted by:

    $$R[X]$$

- **What is the degree of a polynomial?**
  - the largest power of X appearing in P
  - denoted $deg(P)$
- **What is the leading coefficient of a polynomial?**
  - the coefficient a_n of X^n, where $n = deg(P)$
- **When is a polynomial monic?**
  - when the leading coefficient is 1
- **Are polynomials rings?**
  - define addition as:

    $$(a_0 + a_1X + a_2X^2 + \ldots + a_nX^n) + (b_0 + b_1X + b_2X^2 + \ldots + b_nX^m) = (a_0 + b_0) + (a_1 + b_1)X + \ldots$$

    and multiplication as:

    $$(a_0+a_1X+a_2X^2+\ldots+a_nX^n)\cdot(b_0+b_1X+b_2X^2+\ldots+b_nX^m) = a_0b_0+(a_1b_0+a_0b_1)X+\ldots+a_nb_mX^{n+m}$$

- then $R[X]$ defines the **ring of polynomials over** R
- the zero and identity of $R[X]$ are the zero and identity of R

- **What is a constant polynomial?**
  - the polynomial which are R (in other words, polynomials with degree 0)
- **When is $R[X]$ commutative?**
  - by the definition of polynomial multiplication, $R[X]$ is commutative precisely when R is commutative
- **Are polynomials functions?**
  - **no** - it is important that we think of them as rings as of now
  - later on we will see that each polynomial can be associated with a function

6.1.1 Examples

- we can define $X^3 - X \in \mathbb{Z}_3[X]$. Notice, this polynomial is equivalent to $4X^3 - 7X$ in $\mathbb{Z}_3[X]$
- the coefficients of polynomials can also be matrices:

$$(AX)(BX) = (AB)X^2$$

where $A, B \in Mat(2; \mathbb{Q})$

6.2 Lemma: Inheriting Properties from Rings

Let R be a ring, and let $R[X]$ be a ring of polynomials over R. Then:

1. *if R has no **zero-divisors** then $R[X]$ has no **zero-divisors**, and:*

$$deg(PQ) = deg(P) + deg(Q), \qquad P, Q \neq 0 \in R[X]$$

2. *if R is an **integral domain**, so is $R[X]$*

[Lemma 3.3.3]

For the first part, we provide 2 illustrative examples. Consider the polynomials:

$$P = 2X + 4 \qquad Q = 3X + 1$$

In $\mathbb{R}[X]$, we get that:

$$PQ = 6X^2 + 14X + 4$$

In $\mathbb{Z}_6[X]$, we get that:

$$PQ = \bar{6}X^2 + \bar{14}X + \bar{4} = \bar{2}X + \bar{4}$$

As we can see, in the first example, $\mathbb{R}$ has no zero-divisors and:

$$deg(PQ) = 2 = deg(P) + deg(Q)$$

However, in the second example, $\mathbb{Z}_6$ has zero-divisors (namely $\bar{2}, \bar{3}$ and:

$$deg(PQ) = 1 \neq deg(P) + deg(Q)$$

Proof. For the first claim, and as illustrated by the example above, if R has no zero-divisors, then the leading coefficient of PQ is the product of the leading coefficients of P and Q. From this it is easy to see that we will indeed have $deg(PQ) = deg(P) + deg(Q)$. Moreover, it is clear that $PQ \neq 0$ if and only if $P \neq 0 \wedge Q \neq 0$ (since no possible multiplication of coefficients can be 0).

For the second claim, we note that if R is commutative, $R[X]$ is commutative. From the claim above, if R has no zero-divisors, $R[X]$ doesn't either. An integral domain is a commutative ring with no zero-divisors, so if R is an integral domain, so is $R[X]$.

□

6.2.1 Exercises (TODO)

1. **Show that if R is an integral domain, then:**

$$R[X]^{\times} = R^{\times}$$

   Show by counterexample, that this is not the case if R is *not* an integral domain.

6.3 Theorem: Division and Remainder of Polynomials

The following theorem describes how a polynomial can be decomposed into smaller polynomials. It also gives us an understanding of how ***polynomial division*** *can be carried out.*

Let R be an integral domain, and let $P, Q \in R[X]$ where Q is monic (so its leading coefficient is 1).
Then, there exists unique $A, B \in R[X]$ such that:

$$P = AQ + B$$

and:

$$deg(B) < deg(Q)$$

or:

$$B = 0$$

[Theorem 3.34]

Proof. Pick A to minimise $deg(P - AQ)$. This is always possible, since the degree of any polynomial is always non-negative.

Assume that after this:

$$deg(P - AQ) \geq deg(Q)$$

That is, we have:

$$P - AQ = \sum_{i=0}^{r} a_i X^i$$

and $r \geq d = deg(Q)$.

Now consider:

$$P - (A + a_r X^{r-d})Q = P - AQ - a_r X^r + \dots$$

As we can see $deg(P - (A + a_r X^{r-d})Q) = deg(P - AQ) - 1$. This contradicts the fact that our choice of A lead to $deg(P - AQ) \geq deg(Q)$, meaning that we must have $deg(P - AQ) < deg(Q)$.

Thus, we have found A and $B = P - AQ$, with $deg(B) < deg(Q)$ such that:

$$B = P - AQ \implies p = AQ + B$$

as required.

We now show that these choices are indeed unique. Suppose that A', B' also satisfy the conclusions (so $P = A'Q + B'$ and $deg(B') < deg(Q)$. Then:

$$0 = P - P = (A - A')Q + (B - B')$$

Notice:

- $(A - A')Q$ will have degree greater than (or equal to) Q
- $B - B'$ has degree less than Q

But the polynomial should have degree 0. This is only possible if $A - A' = 0 \implies A = A'$ (since B could have degree 0).

But then notice that:

$$B = P - AQ = P - A'Q = B'$$

Thus, the choice of A, B is unique.

□

6.4 Examples

We illustrate polynomial long division given:

$$P = X^5 - 7X^4 - 16X^3 - 17X + 2$$

$$Q = X^3 - 5X + 4$$

The following was produced using the package `polynom`. The documentation can be found here.

Applying the division:

$$
\begin{array}{r|rrrrrr}
 & & & & X^2 & -7X & -11 \\
\hline
X^3 - 5X + 4 & X^5 & -7X^4 & -16X^3 & & -17X & +2 \\
 & -X^5 & & +5X^3 & -4X^2 & & \\
\cline{2-5}
 & & -7X^4 & -11X^3 & -4X^2 & -17X & \\
 & & 7X^4 & & -35X^2 & +28X & \\
\cline{3-6}
 & & & -11X^3 & -39X^2 & +11X & +2 \\
 & & & 11X^3 & & -55X & +44 \\
\cline{4-7}
 & & & & -39X^2 & -44X & +46
\end{array}
$$

In other words, we have:

$$A = X^2 - 7X - 11$$

$$B = -39X^2 - 44X + 46$$

As we can see, $deg(B) = 2 < 3 = deg(Q)$.

6.5 Evaluating Polynomials

- **Why do we think of polynomials as functions?**
  - because there exists a mapping:
  $$R[X] \to Maps(R, R)$$
  - this mapping is given by **evaluating** a polynomial $P \in R[X]$ at $\lambda \in R$ to produce:
  $$P(\lambda)$$
  - $P(\lambda)$ is obtained by replacing all X in P by λ
- **What is a root of a polynomial?**
  - $\lambda \in R$ such that $P(\lambda) = 0$

6.5.1 Examples

- recall our polynomial $P = X^3 - X \in \mathbb{Z}_3[X]$. Then:
  $$P(\bar{0}) = \bar{0}^3 - \bar{0} = \bar{0}$$
  $$P(\bar{1}) = \bar{1}^3 - \bar{1} = \bar{0}$$
  $$P(\bar{2}) = \bar{2}^3 - \bar{2} = \bar{2} - \bar{2} = \bar{0}$$
  In other words, P can be mapped to the zero function
- the polynomial $P = X^3 + 1 \in \mathbb{C}[X]$ has a roots:
  $$\lambda = -1, e^{i\frac{\pi}{3}}, e^{-i\frac{\pi}{3}}$$

6.5.2 Exercises (TODO)

1. **Show that the mapping $R[X] \to Maps(R, R)$ as described above is not injective when $R = \mathbb{Z}_p$, with p prime. Hint: Fermat's Little Theorem:**
   $$a^p \equiv a \ (mod \ p)$$
   If a is not divisible by p this becomes:
   $$a^{p-1} \equiv 1 \ (mod \ p)$$

6.6 Proposition: Roots of Polynomials

*Let R be a **commutative ring**, with $\lambda in R$ and $P(X) \in R[X]$.*
*λ is a **root** of $P(X)$ **if and only if** $(X - \lambda)$ divides $P(X)$.*

Proof. If $X - \lambda$ divides P, we can write:

$$P = (X - \lambda)Q(X)$$

so:

$$P(\lambda) = 0 \cdot Q(\lambda) = 0$$

so λ is a root.

Alternatively, if λ is a root, we know that:

$$P(X) = \sum_{k=0}^{n} a_k X^k \in RX], \qquad P(\lambda) = 0$$

We can factorise a difference of 2 powers (see here for the proof) via:

$$X^k - \lambda^k = \begin{cases} (X - \lambda) \sum_{j=0}^{k-1} \lambda^j X^{k-j-1}, & k \geq 1 \\ 0, \quad k = 0 \end{cases}$$

Then,

$$\begin{aligned} P(X) &= P(X) - P(\lambda) \\ &= \sum_{k=0}^{n} a_k X^k - \sum_{k=0}^{n} a_k \lambda^k \\ &= \sum_{k=0}^{n} a_k (X^k - \lambda^k) \\ &= \sum_{k=0}^{n} a_k ((X - \lambda) \sum_{j=0}^{k-1} \lambda^j X^{k-j-1}) \\ &= (X - \lambda) \sum_{k=0}^{n} a_k \left(\sum_{j=0}^{k-1} \lambda^j X^{k-j-1} \right) \end{aligned}$$

Thus, $(X - \lambda)$ divides $P(X)$.

□

6.7 Theorem: Number of Roots of Polynomials

A consequence of the above theorem is the following:

> *Let R be an **integral domain**. A non-zero polynomial:*
>
> $$P \in R[X] \setminus \{0\}$$
>
> *has at most $deg(P)$ roots in R. [Theorem 3.3.10]*

Proof. Consider m distinct roots $\lambda_1, \dots, \lambda_m$ of a polynomial P. We know that $X - \lambda_1$ must divide P, such that:

$$P = (X - \lambda_1)A$$

where $A \in R[X], deg(A) = deg(P) - 1$.

This equality holds for $\lambda_i, i \in [2, m]$:

$$P(\lambda_i) = (\lambda_i - \lambda_1)A(\lambda_i)$$

Since λ_i is a root of P, we must have:

$$(\lambda_i - \lambda_1)A(\lambda_i) = 0$$

The roots are distinct, so $(\lambda_i - \lambda_1) \neq 0$. Hence, it follows that $\lambda_2, \dots, \lambda_m$ must be $m-1$ distinct roots of A. Applying induction, the theorem is proven.

□

6.8 Theorem: Fundamental Theorem of Algebra

- **What is an algebraically closed field?**
  - consider a field F and a **non-constant** polynomial:

    $$P \in F[X] \setminus F$$

  - if P has a root in F, then F is **algebraically closed**

> *The field of complex numbers $\mathbb{C}$ is algebraically closed. [Theorem 3.3.13]*

6.8.1 Examples

- $\mathbb{R}$ is **not** algebraically closed, since $X^2 + 1$ has no root in $\mathbb{R}$
- $\mathbb{Z}_2$ is **not** algebraically closed, since $X^2 + X + 1$ has no root in the binary numbers
- any finite field is not algebraically closed. If $F = \{a_1, \dots, a_n\}$ then the polynomial:

  $$1 + \prod_{i=1}^{n}(X - a_i)$$

  has no roots in F

6.9 Theorem: Decomposing a Polynomial Into Linear Factors

*If F is an **algebraically closed** field, then every **non-zero** polynomial:*

$$P \in F[X] \{0\}$$

***decomposes into linear factors**:*

$$P = c(X - \lambda_1)(X - \lambda_2) \dots (X - \lambda_n)$$

where $c \in F^{\times}, n \geq 0, \lambda_i \in F$. This decomposition is unique. [Theorem 3.3.14]

Proof. If P is constant, nothing to do.

F is algebraically closed, so P has a root $\lambda \in F$, so in particular we can write:

$$P = (X - \lambda)A$$

We then apply an inductive argument on A.

□

7 Ring Homomorphisms

7.1 Defining Ring Homomorphisms

- **What is a ring homomorphism?**
  - a mapping between rings R, S satisfying:

$$f(x + y) = f(x) + f(y)$$

$$f(xy) = f(x)f(y)$$

- **Do ring homormophisms preserve the identity?**
  - in general, if $f : R \to S$ is a ring homomorphism, it is not the case that:

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

7.1.1 Examples

- the **inclusion** (i.e a mapping $f(x) = x$ where $x \in A$ and $f(x) \in B$ and $A \subseteq B$) given by:

$$\mathbb{Z} \to \mathbb{Q}$$

  is a ring homomorphism

- the mapping:
$$f : \mathbb{Z} \to \mathbb{Z}_m$$
defined by:
$$f(a) = \bar{a}$$
is a ring homomorphism

- the mapping:
$$f : \mathbb{R} \to Mat(2; \mathbb{R})$$
defined by:
$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$
is a ring homomorphism (just check the properties). This is a prime example of how $f(1_R) \neq 1_S$.

- the mapping:
$$f : \mathbb{R} \to Mat(2; \mathbb{R})$$
defined by:
$$f(x) = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$$
is **not** a ring homomorphism (just check the properties - it satisfies additive linearity, but not multiplicative)

- the mapping:
$$f : \mathbb{R} \to Mat(2; \mathbb{R})$$
defined by:
$$f(x) = \begin{pmatrix} x^2 & 0 \\ 0 & 0 \end{pmatrix}$$
is **not** a ring homomorphism (it doesn't satisfy additive linearity)

7.1.2 Exercises (TODO)

1. **Let R be a commutative ring, and $\lambda \in R$. The mapping $f : R[X] \to R$ defined by $f(P) = P(\lambda), \quad \forall P \in R[X]$ is a ring homomorphism.**

2. **Let R be a commutative ring, n a positive integer, and $M \in Mat(n; R)$. The mapping $f : R[X] \to Mat(n; R)$ defined by:**
$$f\left(\sum_{i=0}^{t} a_i X^i\right) = \sum_{i=0}^{t} a_i M^i$$
is a ring homomorphism.

7.2 Lemma: Properties of Ring Homomorphisms

The following are properties that follow from the fact that a ring is a group under addition, so any property of group homomorphisms must apply to ring homomorphisms under addition:

1. $f(0_R) = 0_S$ *(preservation of additive identity)*
2. $f(-x) = -f(x)$ *(preservation of additive inverse)*
3. $f(x - y) = f(x) - f(y)$
4. $f(mx) = mf(x)$
5. $f(x^n) = f(x \cdot x \cdot \ldots \cdot x) = (f(x))^n$

[Lemma 3.4.5 & Remark 3.4.6]

8 Ideals and Kernels

Ideals *are the generalisation of* ***kernels*** *for rings. To develop an idea for* ***ideals****, we first note some properties of kernels for* ***ring homomorphisms****.*

Consider the ring homomorphism:

$$f : R \to S$$

Then, the ***kernel*** *of the homomorphism is:*

$$ker(f) = \{r \mid r \in R \ : \ f(r) = 0_S\}$$

Notice that:

1. *the* ***kernel*** *is* ***non-empty*** *since:*

$$f(0_R) = 0_S$$

2. *if $x, y \in ker(f)$:*

$$f(x - y) = f(x) - f(y) = 0_S - 0_S = 0_S$$

   so:

$$x - y \in ker(f)$$

3. *the* ***kernel*** *is* ***closed under multiplication****:*

$$f(xy) = f(x)f(y) = 0_S \cdot 0_S = 0_S$$

4. *more than that, if $x \in ker(f)$ and $r \in R$:*

$$f(xr) = f(x)f(r) = 0_S \cdot f(r) = 0_S$$

$$f(rx) = f(r)f(x) = f(r) \cdot 0_S = 0_S$$

   hence, $xr, rx \in ker(f)$

All these properties are used to define a special subset of a ring, called an ***ideal****. Kernels are just a special type of ideal.*

8.1 Defining Ideals

- **What is an ideal?**
  - a subset I of a ring R
  - satisfies:
    1. $I \neq \emptyset$
    2. I is closed under substraction
    3. $\forall i \in I, \forall r \in R, ri, ir \in I$

- an **ideal** is denoted with:

$$I \trianglelefteq R$$

8.1.1 Examples

- if R is a ring, $\{0\}, R$ are ideals
- $m\mathbb{Z}$ (set of multiples of m) is an ideal of $\mathbb{Z}$: $ma \in m\mathbb{Z}, b \in \mathbb{Z}$ then:

$$b(ma) = m(ba)$$

  and commutativity of integers gives us $(ma)b = m(ba)$

- $$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \right\} \subset Mat(2; \mathbb{R}$$

  is **not** an ideal, since it fails closure under multiplication by elements in $Mat(2; \mathbb{R}$.

  - $ri \in I, \forall i \in I$:

$$\begin{pmatrix} k & l \\ m & n \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & kb + ld \\ 0 & mk + nd \end{pmatrix} \in I$$

  - however, $ir \notin I$, since for example:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin I$$

8.2 Proposition: Generating Ideals

*Let R be a **commutative ring**, and let $T \subseteq R$. Then:*

$${}_R\langle T \rangle$$

*is the **smallest** ideal of R containing T.*
*Here ${}_R\langle T \rangle$ is the **ideal of** R **generated by** T, defined as:*

$${}_R\langle T \rangle = span(T) = \left\{ \sum_{i=1}^{m} r_i t_i \mid r_i \in R, t_i \in T \right\}$$

[Proposition 3.4.14]

Proof. The first step is to show that ${}_R\langle T \rangle$ is an ideal:

1. $0 \in {}_R\langle T \rangle$, so it is non-empty

2. if $t, t' \in {}_R\langle T\rangle$, then subtracting them is equivalent to doing componentwise subtraction, so the result will be in ${}_R\langle T\rangle$ too:

$$\sum_{i=1}^{m} r_i t_i - \sum_{i=1}^{m} r_i' t_i = \sum_{i=1}^{m} (r_i - r_i')t_i \in {}_R\langle T\rangle$$

3. clearly, and using distributivity and commutativity:

$$r \sum_{i=1}^{m} r_i t_i = \sum_{i=1}^{m} (r r_i) t_i \in {}_R\langle T\rangle$$

$$\left(\sum_{i=1}^{m} r_i t_i\right) r = \sum_{i=1}^{m} r_i t_i r = \sum_{i=1}^{m} (r_i r) t_i \in {}_R\langle T\rangle$$

The second step is showing that it is the smallest ideal containing T. This follows from the fact that any ideal I containing $t_1, \dots, t_m \in I$ must contain $\sum_{i=1}^{m} r_i t_i$, as otherwise closure (both under subtraction and over elements of R) would be violated.

□

8.2.1 Examples

- if $m \in \mathbb{Z}$, then ${}_{\mathbb{Z}}\langle m\rangle = m\mathbb{Z}$
- if $P \in \mathbb{R}[X]$, then:

  $${}_{\mathbb{R}[X]}\langle P\rangle = \{AP \mid A \in \mathbb{R}[X]\}$$

  Thinking about this, this is the set of all polynomials in $\mathbb{R}[X]$ which are **divisible** by P.

8.3 The Principal Ideal

- **What is a principal ideal?**
  - an **ideal** generated by a single element in the ring:

    $$I = \langle t\rangle, \qquad t \in R$$

8.3.1 Examples

- 0 is a principal ideal, generated by 0_R
- R is a principal ideal, generated by 1_R

8.4 The Kernel of a Ring homomorphism

- **What is the kernel of a ring homomorphism?**
  - let $f : R \to S$ be a ring homomorphism
  - the **kernel** is an **ideal** of R given by:

    $$ker(f) = \{r \mid r \in R, f(r) = 0_S\}$$

  - for example, if $f : \mathbb{Z} \to \mathbb{Z}_m$ is the homomorphim $f(a) = \bar{a}$ then:

    $$ker(f) = \{a \mid a \in \mathbb{Z}, f(a) = \bar{0}\}$$

    which is nothing but the set of all a divisble by m. In other words:

    $$ker(f) = m\mathbb{Z}$$

We now introduce lemmas derived in a similar way to those derived for the kernel in groups/vector spaces.

8.5 Lemma: Injectivity and Kernels

*f is injective **if and only if** $ker(f) = \{0\}$. [lemma 3.4.20*

8.6 Lemma: Intersection of Ideals

*The **interesection** of an collection of **ideals** of a ring R is an **ideal** of R. [Lemma 3.4.21]*

8.7 Lemma: Addition of Ideals

*Let I, J be **ideals** of a ring R. Then another **ideal** of R is:*

$$I + J = \{a + b \mid a \in I, b \in J\}$$

9 Subrings and Images

Similarly to how **kernels** are a special type of **ideal**, **images** of ring homomorphisms are a special type of **subring**. We outline properties of subrings by outlining properties of images.

Consider the ring homomorphism:

$$f : R \to S$$

Then, the ***image*** *of the homomorphism is:*

$$im(f) = \{f(r) \mid r \in R\}$$

Notice that:

1. *the* ***image*** *is* ***non-empty*** *since:*

$$f(0_R) = 0_S$$

2. *if $x, y \in im(f)$ then $\exists s, t \in R$ such that:*

$$f(s) = x \qquad f(t) = y$$

So:

$$x - y = f(x) - f(t) = f(s - t)$$

Hence:

$$x - y \in im(f)$$

3. *the* ***kernel*** *is* ***closed under multiplication****:*

$$xy = f(s)f(t) = f(st)$$

so $xy \in im(f)$

4. *unlike with ideals, the image isn't closed under multiplication by elements in R. If $s = f(x) \in im(f)$ and $t \in R$, we ask whether $f(x)t$ or $tf(x)$ are in $im(f)$. This is only the case if $\exists y \in R : f(y) = t$. This is exemplified by:*

$$f : \mathbb{R} \to Mat(2; \mathbb{R})$$

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

Then:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in im(f) \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in R$$

but:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin im(f)$$

9.1 Defining Subrings

- **What is a subring?**
  - a subset R' of a ring R
  - R' itself is a ring under addition and multiplication (as defined in R)

9.1.1 Examples

- $0, R$ are subrings of any ring R
- $Mat(m; F)$ is a subring of $Mat(n; F)$, provided that $m \leq n$ and F is a field. We can think of $Mat(m; F)$ as a zero-padded subset of
$$Mat(n; F)$$

9.2 Proposition: Test for a Subring

*A subset R' of a ring R is a subring **if and only if***

1. *R' has a multiplicative identity*
2. *R' is closed under substraction*
3. *R' is closed under multiplication*

[Proposition 3.4.26]

*The above test thus shows that $im(f)$ is a **subring**.*

Proof. If R' is a subring, the properties hold by properties of a ring.

Assume the 3 conditions hold. The first 2, along the subgroup test tell us that R' is a subgroup of R under addition. Hence, R' is abelian (since subgroups of abelian groups are abelian). Associativity also holds in R', so alongside with (1) and (3), we see that R' is a monoid under multiplication. Distributivity holds in R', since it holds in R. Thus, R' is a ring, and so, a subring.

□

9.2.1 Examples

- ideals are not typically subrings: they tend to fail property (1) (existence of multiplicative identity).
  - as an example, $m\mathbb{Z}$ only has a multiplicative identity with $m = 0$ or $m = 1$
- even if R' is a subring, it can happen that:
$$1_R \neq 1_{R'}$$
  This is shown in the example involving $Mat(m; F)$ and $Mat(n; F)$

9.2.2 Exercises (TODO)

1. **Show that:**

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$. This subring is known as the *Gaussian Integers*.

9.3 Proposition: Properties of Subrings

Let R, S be rings, with:

$$f : R \to S$$

*a **ring homomorphism**. Then:*

1. *if R' is a subring of R, $f(R')$ is a subring of S*
2. *if*
   - $f(1_R) = f(1_S)$
   - *x is a unit in R*

   then:
   - *$f(x)$ is a unit in S*
   - $(f(x))^{-1} = f(x^{-1})$
   - *f is restricted to a group homomorphism:*

$$f : R^\times \to S^\times$$

[Proposition 3.4.28]

Proof. The first part follows by using the properties of a ring homomorphism, alongside the test for a subring.

For the second part, if $x \in R^\times$, by definition x is a unit, so x^{-1} exists. Hence:

$$f(x)f(x^{-1}) = f(1_R) = 1_S$$

Similarly,

$$f(x^{-1})f(x) = f(1_R) = 1_S$$

In other words, $f(x)$ must be a unit, with inverse $f(x^{-1})$, and so, $f(x) \in S^\times$

□

9.4 Remark: Intersection of Subrings

> *Unlike with ideals, the* ***intersection*** *of* ***subrings*** *doesn't result in a* ***subring****. [Remark 3.4.29]*

Proof. We can show by counterexample. Let:

$$R' = \left\{ \begin{pmatrix} a & b & 0 \\ 0 & a & 0 \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

$$R' = \left\{ \begin{pmatrix} c & d & d \\ 0 & c & f \\ 0 & 0 & c \end{pmatrix} \right\}$$

with $a, b, c, d, e, f \in \mathbb{Q}$. Clearly, R', R'' are subrings of $Mat(3; \mathbb{Q})$, but their intersection can't be a subring, since it doesn't contain the identity.

□

10 Workshop

1. **True or False. The group of units** $(\mathbb{Z}_m)^\times$ **is cyclic.**

> *Beyond intuition about this being false, I can't think of a "smart" way of proving this, other than finding a counterexample by trial and error.*

Field	Group of Units	Cyclic?
$\mathbb{Z}_1$	$\{1\}$	yes
$\mathbb{Z}_2$	$\{1\}$	yes
$\mathbb{Z}_3$	$\{1, 2\}$	yes
$\mathbb{Z}_4$	$\{1, 3\}$	yes
$\mathbb{Z}_5$	$\{1, 2, 3, 4\}$	yes
$\mathbb{Z}_6$	$\{1, 5\}$	yes
$\mathbb{Z}_7$	$\{1, 2, 3, 4, 5, 6\}$	yes
$\mathbb{Z}_8$	$\{1, 3, 5, 7\}$	no

$(\mathbb{Z}_8)^\times$ is not cyclic, since each element is its own inverse, so they can't generate the whole group.

As tips when filling the table:

- *the units of $\mathbb{Z}_p$ are precisely all of $\mathbb{Z}_p$, since $\mathbb{Z}_p$ is a field, and so all of its elements are invertible*
- *if n is even, then the units of $\mathbb{Z}_n$ will have to be odd. This is because a is a unit in $\mathbb{Z}_n$ if it can be written as:*

$$kn + 1, \qquad k \in \mathbb{N}$$

Since n is even, $kn + 1$ will be odd

2. **True or False. The ring of integers $\mathbb{Z}$ is a field, because every nonzero element has a multiplicative inverse. For example, the inverse of 6 is $\frac{1}{6}$.**

   This is false, because $\frac{1}{6} \notin \mathbb{Z}$. That is, all the elements of $\mathbb{Z}$ have inverses in $\mathbb{Q}$, but not necessarily in $\mathbb{Z}$.

3. **Let F be a field, and $R = F[X]$, the ring of polynomials over F. Show that $R^\times = F^\times$, the set of non-zero constant polynomials.**

   Since F is a field, each of its elements has an inverse, so $F^\times = F$. This means that:

$$F^\times \subseteq R^\times$$

   since $F \subseteq R$.

   Now, consider $P \in R$, such that $P \in R^\times$. Say that $deg(P) = n$. Since P is a unit, $\exists Q \in R$ such that $PQ = 1_F$, where $deg(Q) = m$.

   By Lemma 3.3.3 of the notes, part i), since F has no zero-divisors (since it is a field) it follows that:

$$deg(PQ) = deg(P) + deg(Q) \implies 0 = m + n$$

   since $deg(1_F) = 0$. But now, since $m, n \geq 0$, this is only possible if $m = n = 0$. In other words, any unit of R must be a constant polynomial, so $P \in F^\times$. Hence we have that:

$$R^\times \subseteq F^\times$$

   and so:

$$F^\times = R^\times$$

4. **We now consider how to construct fields from rings.**

   (a) **By using the test for a subring, plus something, or otherwise, show that the following subset of $Mat(2; \mathbb{R})$ is a field:**

$$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

   Recall the test for a subring:

*A subset R' of a ring R is a subring **if and only if***

1. *R' has a multiplicative identity*
2. *R' is closed under substraction*
3. *R' is closed under multiplication*

[Proposition 3.4.26]

and the definition of a field:

*A **field** is a **non-zero, commutative** ring in which every non-zero element has a **multiplicative inverse**. [Definition 3.1.8]*

Hence, we just "follow our nose", verifying the properties of a subring, and then showing that R is non-zero, commutative, and that each element has an inverse.

(1) **Existence of Multiplicative Identity**

Using $a = 1, b = 0$ we get that $I_2 \in R$, so the identity is in R.

(2) **Closure Under Subtraction**

Let $a, b, c, d \in \mathbb{R}$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} c & d \\ -d & d \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -b+d & a-c \end{pmatrix}$$

so if $x = a - c \in \mathbb{R}, y = b - d \in \mathbb{R}$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} c & d \\ -d & d \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in R$$

so we have closure under subtraction.

(3) **Closure Under Multiplication**

Let $a, b, c, d \in \mathbb{R}$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & d \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix}$$

so if $x = ac - bd \in \mathbb{R}, y = ad + bc \in \mathbb{R}$:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & d \end{pmatrix} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \in R$$

so we have closure under multiplication.

Now, we check for the requirements of a field:

① **Commutativity**

We have already computed

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & d \end{pmatrix}$$

so we just need to check if:

$$\begin{pmatrix} c & d \\ -d & d \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

gives the same result:

$$\begin{pmatrix} c & d \\ -d & d \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{pmatrix}$$

so commutativity is satisfied.

② **Inverse for Non-Zero Element**

Consider a non-zero:

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

This means that at least one of a, b is non-zero. It's inverse will then be defined, since $det(A) = a^2 + b^2$ so:

$$A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

which is clearly in R.
Thus, R is a field.

(b) **Construct a ring homomorphism from $\mathbb{R}[X]$ to $\mathbb{C}$ that is surjective. Calculate its kernel.**

Here I had the right intuition, but missed the crucial step. We want a homomorphism, which maps a polynomial to a complex number. This indicates that we want to somehow create a representation of a polynomial in the form $a +$ 🙃b so that we can map:

$$a + 🙃b \to a + \sqrt{-1}b$$

On top of this, we should pick such a representation so that if allows a function as an homomorphism (so it should be somewhat linear).
This immediately indicates factorising a polynomial via:

$$A = PQ + R$$

If we pick Q to be of second degree, then R will have the form $aX + b$.

We can decompose any polynomial $A \in \mathbb{R}[X]$ as:

$$A = PQ + R$$

where $deg(Q) = 2$ and $deg(R) < 2$. In particular, let:

$$Q = X^2 + 1 \qquad R = a + bX$$

Define a ring homomorphism:

$$f : \mathbb{R}[X] \to \mathbb{C}$$

by:

$$f(P) = P(\sqrt{-1})$$

That is, we evaluate P at $\sqrt{-1}$.
This is clearly an homomorphism, since if $A, B \in \mathbb{R}[X]$ then:

$$f(A + B) = (A + B)(\sqrt{-1}) = A(\sqrt{-1}) + B(\sqrt{-1}) = f(A) + f(B)$$
$$f(AB) = (AB)(\sqrt{-1}) = A(\sqrt{-1})B(\sqrt{-1}) = f(A)f(B)$$

But notice, $\sqrt{-1}$ is a root of Q so:

$$f(P) = f(R) = a + \sqrt{-1}b \in \mathbb{C}$$

Hence, f must be surjective.
If $A \in ker(f)$ then that means that $a = b = 0$ so in particular A must have $X^2 + 1$ as a factor. In particular, $ker(f)$ must be the ideal generated by the polynomial $X^2 + 1$.

(c) **What do the constructions above have in common?**

This links to the work which will be done next week, in which quotient rings will be introduced. The above tells us that the quotient ring $\mathbb{R}[X]/ker(f)$ is **isomorphic** to $\mathbb{C}$.
In fact, it can be shown that the ring R introduced above is also isomorphic to $\mathbb{C}$ via:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \to a + \sqrt{-1}b$$

Thus, we have found 2 ways of defining the field $\mathbb{C}$ from 2 very different rings!

5. **Define the *quaternions*:**

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \,\middle|\, z, w \in \mathbb{C} \right\}$$

(a) **Show that $\mathbb{H}$ is a subring of $Mat(2; \mathbb{C})$**

*A subset R' of a ring R is a subring **if and only if***

1. *R' has a multiplicative identity*
2. *R' is closed under subtraction*
3. *R' is closed under multiplication*

[Proposition 3.4.26]

① **Existence of Multiplicative Identity**

Picking $z = 1, w = 0$ we see that $I_2 \in \mathbb{H}$, so it contains the multiplicative identity.

② **Closure Under Subtraction**

Let $z, w, a, b \in \mathbb{C}$. Then:

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} - \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} z-a & w-b \\ -\bar{w}+\bar{b} & \bar{z}-\bar{a} \end{pmatrix} = \begin{pmatrix} z-a & w-b \\ -\overline{(w-b)} & \overline{z-a} \end{pmatrix} \in \mathbb{H}$$

③ **Closure Under Multiplication**

Let $z, w, a, b \in \mathbb{C}$. Then:

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} za-\bar{b}w & zb-\bar{a}w \\ -a\bar{w}+\bar{z}\bar{b} & \bar{z}\bar{a}-\bar{b}w \end{pmatrix} = \begin{pmatrix} za-\bar{b}w & zb-\bar{a}w \\ -\overline{(zb-\bar{a}w)} & \overline{za-\bar{b}w} \end{pmatrix} \in \mathbb{H}$$

(b) **Show that $\mathbb{H}$ is a division ring (i.e every non-zero element is a unit), and that it is not a field**

We can easily define the inverse, since the determinant is non-zero:

$$det(A) = z\bar{z} + w\bar{w} = |z|^2 + |w|^2 > 0$$

(provided that $z \neq 0$ or $w \neq 0$)
Then:

$$A^{-1} = \frac{1}{|z|^2 + |w|^2} \begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix}$$

However, it is not a field, since it isn't commutative. Indeed:

$$\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1-i & 1+i \\ -1+i & 1+i \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} 1+i & 1+i \\ -1+i & 1-i \end{pmatrix}$$