

## Last lecture

- A **unique factorization domain** is an integral domain  $R$  such that (UF1) every non-zero element of  $R$  can be written in the form  $ua_1 \dots a_k$ , where  $u$  and  $a$  a unit and  $a_1, \dots, a_k$  are irreducible and, (UF2) if  $ua_1 \dots a_k = vb_1 \dots b_l$  then  $k = l$  and  $a_i$  and  $b_i$  are associates after renumbering, if necessary.
- If  $R$  is a UFD then  $a \in R$  is irreducible if and only if it is prime.
- Every principal ideal domain is a unique factorization domain (Theorem 15.7).

### This lecture

A summary of where we have been and where we are going.

## The story so far

In this course the main characters are (commutative) rings, fields, and polynomials over rings and fields.

The main aim is to understand the roots of polynomials over a field.

### Definition 16.1

A **ring** is a set  $R$  equipped with two operations, **addition**  $+$  and **multiplication**  $\cdot$ , such that for  $a, b, c \in R$

- 1  $(R, +)$  is an **additive** (abelian) group:  
 $a + (b + c) = (a + b) + c$ ,  $a + 0 = a = 0 + a$ ,  
 $a + (-a) = 0 = (-a) + a$ ,  $a + b = b + a$
- 2 Multiplication is **associative**:  $a(bc) = (ab)c$
- 3 The two **distributive** laws hold:  
 $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .

That is a ring is a set equipped with an addition and multiplication that 'play well' together!

## Ideals

A **subring** of a ring is a non-empty subset which is itself a ring, using the same operations.

However, just as with groups and normal subgroups, there is a special type of subring which is very important; namely an ideal.

### Definition 16.2

An **ideal** of  $R$  is a subring  $I$  such that  $ra, ar \in I$ , for all  $r \in R$  and  $a \in I$ .

N.B. If  $R$  has a one then an ideal  $I$  contains 1 if and only if  $I = R$ .

Ideals are 'the same' as congruences: define  $x \approx y$  if  $x - y \in I$ .

You can think of ideals this way if you prefer.

The importance of ideals stems from the following construction.

### Definition 16.3

Suppose that  $I$  is an ideal of  $R$ . Then the **quotient ring**  $R/I$  is the set

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

with operations  $(x + I) + (y + I) = (x + y) + I$  and  $(x + I)(y + I) = xy + I$ .

## Ring homomorphisms

When studying rings the useful maps to consider are those functions which preserve the main structure of the ring: addition and multiplication.

### Definition 16.4

Suppose that  $R$  and  $S$  are rings. A **ring homomorphism** is a map  $\varphi : R \rightarrow S$  such that  $\varphi(x + y) = \varphi(x) + \varphi(y)$  and  $\varphi(xy) = \varphi(x)\varphi(y)$ , for all  $x, y \in R$ .

Two rings  $R$  and  $S$  are **isomorphic** if there is a ring homomorphism  $\varphi : R \rightarrow S$  which is a bijection. We write  $R \cong S$ .

Suppose that  $\varphi : R \rightarrow S$  is a ring homomorphism. Then:

- The kernel  $\ker \varphi = \{r \in R : \varphi(r) = 0_S\}$  is an ideal of  $R$ .
- The image  $\text{Im } \varphi = \{\varphi(r) : r \in R\}$  is a subring of  $S$ .
- (**The first isomorphism theorem**)  $R / \ker \varphi \cong \text{Im } \varphi$ .

## Integral domains

Having developed the rudiments of ring theory we now want to think of the elements of rings as being **coefficients** and we want to concentrate on **commutative rings**, so  $rs = sr$  for all  $r, s \in R$ .

Commutative rings are some of the nicest rings that you will meet, unfortunately, nasty things which we cannot avoid happen even in commutative rings.

The first bad thing that can happen is that rings can have **zero divisors**. That is, it is possible that  $ab = 0$  even though  $a \neq 0$  and  $b \neq 0$ .

### Definition 16.5

An **integral domain** is a commutative ring with one which does not have any zero divisors (so  $ab = 0 \implies a = 0$  or  $b = 0$ ).

We saw that every integral domain  $R$  embeds into its field of fractions

$$R \hookrightarrow F(R) = \left\{ \frac{a}{b} : a, b \in R \text{ with } b \neq 0 \right\}.$$

Here,  $\frac{a}{b} = \{ (c, d) : c, d \in R \text{ with } d \neq 0 \text{ and } ad = bc \}$ .

## Principal ideal domains and factorization

If  $\alpha_1, \dots, \alpha_n$  are the roots of a polynomial  $f(x) \in \mathbb{R}[x]$  then  $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ , and this factorization is essentially unique (proved later). This makes it clear if we are to understand the roots of polynomials we need to understand how to factorize polynomials.

### Definition 16.6

A **principal ideal domain** is a commutative ring  $R$  with one in which every ideal is principal; that is, every ideal is of the form  $aR$ , for  $a \in R$ .

PIDs are 'nice rings' where factorization 'works'. Making this statement precise is a little involved.

- A **unit** is any element of  $R$  which has an inverse.
- $a$  and  $b$  are **associates** if  $a = bu$  for some unit  $u \in R$ .
- If  $a, b \in R$  then  $a$  **divides**  $b$ , or  $a|b$ , if  $b = at$  for some  $t \in R$ .
- $a$  is **irreducible** if  $a \neq 0$ ,  $a$  is not a unit and  $r|a$  only if  $r$  is either a unit or an associate of  $a$ .
- $p$  is **prime** if  $p \neq 0$ ,  $p$  is not a unit and if  $p|bc$  then either  $p|b$  or  $p|c$ .

## Unique factorization

### Definition 16.7 (slightly informal)

A **unique factorization domain** is an integral domain  $R$  in which every non-zero element can be written in the form  $ua_1 \dots a_k$ , where  $u$  is a unit and  $a_1, \dots, a_k$  are irreducible in  $R$ .

This factorization is unique up to multiplying by units and reordering the factors.

We saw (Theorem 15.7) that every principal ideal domain is a unique factorization domain

$\implies \mathbb{Z}, \mathbb{Z}[i]$  and  $F[x]$ , for  $F$  a field, are unique factorization domains

We will soon see that if  $R$  is a UFD then so is  $R[x]$

$\implies \mathbb{Z}[x]$  is a unique factorization domain

Knowing when factorization works in a ring is interesting in its own right. We will also need this information when we start looking at the roots of polynomials.

## An motivating example using what we already know

### Question

Solve the polynomial equation  $x^2 + 1 = 0$  in  $\mathbb{R}[x]$ .

### First answer

$x^2 + 1$  has no roots in  $\mathbb{R} \iff x^2 + 1$  is **irreducible** in  $\mathbb{R}[x]$

### Second answer

The roots are  $\pm\sqrt{-1} \in \mathbb{C}$  — do we really understand this solution?

### Third answer

Let  $F = \mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x] = \mathbb{R}[x]/I$ , where  $I = (x^2 + 1)\mathbb{R}[x]$ .

**Claim**  $F \cong \mathbb{C}$  !! Let  $\alpha = x + I \in F$  and  $1_F = 1 + I$ .

If  $f(x) \in \mathbb{R}[x] \implies f(x) = (x^2 + 1)q(x) + r(x)$ , where  $\deg r(x) < 2$

$\implies f(x) + I = r(x) + I = r_0 \cdot 1_F + r_1 \cdot \alpha$ , if  $r(x) = r_1x + r_0$

$\implies \{1_F, \alpha\}$  is a basis of  $F$  as a **real** vector space

$\implies$  Further,  $\alpha^2 = (x + I)(x + I) = x^2 + I = -1 + I = -1_F$

$\implies$  There is an isomorphism of fields  $\mathbb{C} \cong F$  given by

$$a + bi \mapsto a \cdot 1_F + b \cdot \alpha.$$