

# Lecture 20 (Constructing Extension Fields)

## The Complex Numbers Revisited

**Reprise** Recall the construction of the complex numbers  $\mathbb{C}$  from the real numbers  $\mathbb{R}$ . Squares in  $\mathbb{R}$  are non-negative. In particular  $x^2 = -1$  has no solution in  $\mathbb{R}$ . Introduce a new number  $i$  which satisfies  $i^2 = -1$ . Let  $\mathbb{C}$  be the set consisting of symbols  $a + bi$  one for each pair  $a, b \in \mathbb{R}$ , called respectively the real and imaginary parts. Add the symbols by adding real parts and imaginary parts:  $(a + ib) + (c + id) = (a + c) + (b + d)i$ . Multiply formally by distributing over addition, assuming commutativity of  $i$  with real and imaginary parts. Then replace  $i^2$  by  $-1$ , and collect real and imaginary parts:

$$(a+bi)(c+di) = (a+bi)c+(a+bi)di = (ac+bc i)+(adi+bdi^2) = (ac-bd)+(ad+bc)i$$

We believe these operations make  $\mathbb{C}$  into a field. The map  $a \mapsto a + 0i$ ,  $a \in \mathbb{R}$  is an embedding (injective homomorphism) of  $\mathbb{R}$  into  $\mathbb{C}$ . By the standard relabelling of  $a + 0i$  as  $a$  for  $a \in \mathbb{R}$  we consider  $\mathbb{R}$  as a subfield of  $\mathbb{C}$ .

**The Complex Numbers as a Quotient Field** The fact the  $x^2 = -1$  has no solution in  $\mathbb{R}$  implies the polynomial  $1 + x^2$  is irreducible in  $\mathbb{R}[x]$ . Hence

$$\mathbb{R}/\langle 1 + x^2 \rangle = \{f(x) + \langle 1 + x^2 \rangle \mid f(x) \in F[x]\}$$

is a field. On division by  $1 + x^2$  any  $f(x) \in \mathbb{R}[x]$  leaves a unique remainder of degree less than 2. So every element of the field  $\mathbb{R}[x]/\langle 1 + x^2 \rangle$  is uniquely expressible in the form  $a + bx + \langle 1 + x^2 \rangle$ ,  $a, b \in \mathbb{R}$ . In terms of these cosets representatives

$$(a + bx + \langle 1 + x^2 \rangle) + (c + id + \langle 1 + x^2 \rangle) = (a + c) + (b + d)x + \langle 1 + x^2 \rangle$$

and multiplying using  $x^2 + \langle 1 + x^2 \rangle = -1 + \langle 1 + x^2 \rangle$ ,

$$\begin{aligned} (a + bx + \langle 1 + x^2 \rangle)(c + dx + \langle 1 + x^2 \rangle) &= (a + bx)(c + dx) + \langle 1 + x^2 \rangle \\ &= ac + (ad + bc)x + bdx^2 + \langle 1 + x^2 \rangle \\ &= (ac - bd) + (ad + bc)x + \langle 1 + x^2 \rangle. \end{aligned}$$

Looking back at the reprise section we see that  $a + bx + \langle 1 + x^2 \rangle \leftrightarrow a + bi$  is bijective map from the field  $\mathbb{R}/\langle 1 + x^2 \rangle$  to the set  $\mathbb{C}$  which respects addition and multiplication and matches  $x + \langle 1 + x^2 \rangle$  with  $i$ . This shows that  $\mathbb{C}$  is indeed a field and it is isomorphic to  $\mathbb{R}[x]/\langle 1 + x^2 \rangle$ .

We now aim to generalise this to arbitrary fields. We first look at the structure of quotient rings of a polynomial ring over a field modulo an arbitrary non-constant polynomial.

**Proposition 20.1** Let  $F$  be a field and  $p(x) \in F[x]$  have degree  $\deg p(x) = d \geq 1$ . Let  $\langle p(x) \rangle = p(x)F[x]$  be the principal ideal generated by  $p(x)$ . Then the following hold for the quotient ring

$$F[x]/\langle p(x) \rangle = \{f(x) + \langle p(x) \rangle \mid f(x) \in F[x]\}.$$

- (i) Every element of the ring  $F[x]/\langle p(x) \rangle$  is expressible uniquely in the form

$$a_0 + a_1x + \cdots + a_{d-1}x^{d-1} + \langle p(x) \rangle$$

with  $a_0, a_1, \dots, a_{d-1} \in F$ , i.e. each coset has a unique representative  $r(x) \in F[x]$  with  $\deg r(x) < d$ .

- (ii) Reduction modulo  $\langle p(x) \rangle$ , restricted to  $a \in F$ ,  $a \mapsto a + \langle p(x) \rangle$ , is an injective homomorphism from  $F$  into  $F[x]/\langle p(x) \rangle$ .

### Proof

- (i) By the division algorithm for polynomials every  $f(x) \in F[x]$  can be expressed uniquely in the form  $f(x) = q(x)p(x) + r(x)$  with  $q(x), r(x) \in F[x]$  and  $\deg r(x) < \deg p(x) = d$ . Hence every coset modulo  $\langle p(x) \rangle$  has a unique representative of degree less than  $d$ .
- (ii) From part (i),  $a \mapsto a + \langle p(x) \rangle$  is an injection of  $F$  into the quotient ring  $F[x]/\langle p(x) \rangle$ . By definition of quotient ring  $a \mapsto a + \langle p(x) \rangle$  is an injective ring homomorphism.  $\square$

We should also note that the injection  $F$  into  $E$  takes the unit element of  $F$  to the unit element of the ring, since for arbitrary rings an injection might not take an identity element to an identity element. For fields, or more generally for ring homomorphism between integral domains this is automatic. See Tutorial 3, Q3.

**Theorem 20.2** Let  $F$  be a field and  $p(x) \in F[x]$  be irreducible. Then there is an extension field  $E$  of  $F$  isomorphic  $F[x]/\langle p(x) \rangle$  in which  $p(x)$  has a root  $\alpha$  and each element of  $E$  is uniquely expressible in the form  $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ , for some  $a_0, a_1, \dots, a_{d-1} \in F$ .

**Proof** Let  $E \supseteq F$  be a copy of the field  $F[x]/\langle p(x) \rangle$  in which each  $a \in F$  is matched with  $a + \langle p(x) \rangle \in F[x]/\langle p(x) \rangle$ . Then the field structure on  $F[x]/\langle p(x) \rangle$  pulls back to give a field structure on  $E$ . By the last Theorem (ii) this is the given field structure on  $F$ . So  $F$  a subfield of  $E$ . Suppose  $x + \langle p(x) \rangle$  is matched to  $\alpha \in E$ . Then for each  $f(x) \in F[x]$ ,  $f(x) + \langle p(x) \rangle$  is matched to  $f(\alpha) \in E$ . Further by (i) every element of  $E$  is uniquely expressible in the form  $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$  for some  $a_0, a_1, \dots, a_{d-1} \in F$ . Lastly because  $p(x) \in \langle p(x) \rangle$ ,  $p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$  in  $F[x]/\langle p(x) \rangle$  and this implies  $p(\alpha) = 0$  in  $E$ .  $\square$

**Longer Proof** Let  $X$  be a set of the same cardinality as the complement of  $Y = \{a + \langle p(x) \rangle \mid a \in F\}$  in  $F[x]/\langle p(x) \rangle$ . Let  $\eta : Y \rightarrow X$  be a bijection. By (ii) in the Proposition 20.1 we can extend  $\eta$  to bijection from  $F[x]/\langle p(x) \rangle$  to  $E = X \dot{\cup} F$  by setting  $\eta(a + \langle p(x) \rangle) = a$  for  $a \in F$ . Then for  $a, b \in E$  defining  $a + b = \eta(\eta^{-1}a + \eta^{-1}b)$  and  $ab = \eta((\eta^{-1}a)(\eta^{-1}b))$  puts a ring structure on  $E$  such that  $\eta$  is a ring isomorphism. So  $F[x]/\langle p(x) \rangle$  a field implies  $E$  is a field. For  $a, b \in F$ ,

$$a + b = \eta((a + \langle p(x) \rangle) + (b + \langle p(x) \rangle)) = \eta(a + b + \langle p(x) \rangle) = a + b,$$

and

$$ab = \eta((a + \langle p(x) \rangle)a + \langle p(x) \rangle) = \eta(ab + \langle p(x) \rangle) = ab.$$

Thus  $F$  is a subfield of  $E$ .

Now set  $\alpha = \eta(x + \langle p(x) \rangle)$ . For arbitrary  $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ ,  $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in E$  and

$$\begin{aligned} \eta(f(x) + \langle p(x) \rangle) &= \eta(a_0 + a_1x + \cdots + a_nx^n + \langle p(x) \rangle) \\ &= \eta(a_0) + \eta(a_1)\eta(x) + \cdots + \eta(a_n)\eta(x)^n \\ &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= f(\alpha). \end{aligned}$$

So from (ii) of Proposition 20.1 we can conclude every element of  $E$  is uniquely expressible in the form  $a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$ , for some  $a_0, a_1, \dots, a_{d-1} \in F$ . Lastly because  $p(x) \in \langle p(x) \rangle$ ,  $p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle$ ,

$$p(\alpha) = \eta(p(x) + \langle p(x) \rangle) = \eta(0 + \langle p(x) \rangle) = 0 \in E. \quad \square$$