

# MATH172 Galois Theory Notes

Xuehuai He  
September 28, 2023

## Contents

<b>Rings! Or why <math>x^2 - 2</math> has roots.</b>	<b>2</b>
Ring . . . . .	2
Phase I: ID, UFD, PID, ED, Fields . . . . .	3
Zero divisors . . . . .	3
Integral domain . . . . .	3
Unit, irreducibles . . . . .	3
Unique factorization domain . . . . .	3
Ideals . . . . .	4
Principal Ideal Domain . . . . .	4
Prime Ideal . . . . .	4
Maximal Ideal . . . . .	4
Noetherian Rings . . . . .	5
Quotient Rings . . . . .	5
Ring homomorphism . . . . .	6
First ring isomorphism theorem . . . . .	6
Quotient by prime ideal is ID . . . . .	6
Quotient by maximal ideal is field . . . . .	7
Euclidean Domain . . . . .	7
Why do we care about Euclidean domains? . . . . .	8
Greatest common divisors & Euclidean algorithm . . . . .	8
Prime elements . . . . .	9
Prime implies irreducible in ID . . . . .	9
Prime implies maximal in PID . . . . .	9
Irreducible implies prime in UFD . . . . .	9
PIDs are UFDs . . . . .	10
Phase I summary . . . . .	11
<b>Field extensions</b>	<b>11</b>
Phase II: Field extensions . . . . .	11
$F[x]/(p(x))$ contains a copy of $F$ . . . . .	12

$F[x]/(p(x))$ field if $p(x)$ irreducible . . . . .	12
Field extension, degree of extension . . . . .	12
To summarize so far! . . . . .	13
Irreducibility – a survey . . . . .	14
Eisenstein’s Criterion . . . . .	15
Gauss’ Lemma . . . . .	15
Algebraic and transcendental . . . . .	16
Algebraic extension . . . . .	16
Finite extensions are algebraic . . . . .	16
Minimal polynomial . . . . .	16

---

## Rings! Or why $x^2 - 2$ has roots.

**Definition 1.** A **ring** is a set  $R$  together with associative binary *operations*  $+$  and  $\times$  s.t.:

← map from  
 $R \times R \mapsto R$

- $(R, +)$  is an **abelian** group with identity  $0$
- There exists  $1 \in R$  s.t.  $r \times 1 = 1 \times r = r$
- $r(s + t) = rs + rt$  and  $(s + t)r = sr + tr \quad \forall s, r, t \in R$

← this is optional

**Proposition 1.**  $0 \times 1 = 0$  (in fact,  $0 \times r = 0 \quad \forall r \in R$ )

*Proof.* Try it! □

**Definition 2.** If  $\times$  is commutative, then  $R$  is a commutative ring.

**Non-example 1.**  $\mathbb{N}$  is not a ring.

**Example 2.**  $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$  are all rings;

- $\mathbb{Z}/n\mathbb{Z}$  is a finite ring
- $M_n(\mathbb{R})$ , the set of  $n \times n$  real matrices, is a **noncommutative** ring
- Polynomial ring:  $\mathbb{Q}[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{Q}\}$  is a commutative ring
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$  is a commutative ring

← square brackets just mean "polynomials in..."

Phase I plan:

$$ID \supsetneq UFD \supsetneq PID \supsetneq ED \supsetneq Fields$$

**Definition 3.** Suppose  $R$  is a ring and  $a, b \in R$  with  $ab = 0$  but  $a, b \neq 0$ ; then  $a, b$  are called **zero divisors**.

**Example 3.**

- In  $\mathbb{Z}/6\mathbb{Z}$ ,  $\bar{4} \times \bar{3} = \bar{0}$
- In  $M_2(\mathbb{R})$ ,  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

**Definition 4.** A commutative ring without zero divisors is called an integral domain (ID)

Why do we want ID? **Cancellation properties.**

- If  $R$  is an ID,  $a, b, c \in R$ ,  $a \neq 0$  and  $ab = ac$ , then

$$ab - ac = 0 \implies a(b - c) = 0 \implies b - c = 0 \implies b = c$$

**Definition 5.** Suppose  $R$  is an ID. An element  $a \in R$  is called a **unit** if  $a \neq 0$  and there exists  $b \in R$  s.t.  $ab = 1$ .

← notation:  $b = a^{-1}$

An element  $r \in R$  is called **irreducible** if  $r \neq 0$ ,  $r$  is NOT a unit, and whenever  $r = ab$  for some  $a, b \in R$  then  $a$  or  $b$  must be a unit.

- If  $r$  and  $s$  are irreducibles with  $r = us$ , then  $r$  and  $s$  are called **associates**.

**Example 4.**

- All “prime integers” are irreducibles in  $\mathbb{Z}$ ;
- $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$  are irreducibles in  $\mathbb{Z}[\sqrt{-5}]$ .
  - Note:  $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$  says that 6 can be factored in more than one way. This means that  $\mathbb{Z}[\sqrt{-5}]$  is NOT an UFD.

**Definition 6.** An integral domain  $R$  is called a unique factorization domain (UFD) if each nonzero, nonunit  $a \in R$  can be written as a product of irreducibles **in a unique way** up to associates.

If  $a$  is a nonzero, nonunit element of UFD  $R$  and  $a = r_1 r_2 \dots r_m = s_1 \dots s_n$  where  $r_i, s_j$  are irreducible, then after reordering  $r_i = u_i s_i$  for any  $i$  and units  $u_i$ , and  $m = n$ .

← After reordering, there are the same amounts of factors and all factors are the same up to units.

**Definition 7.** Suppose  $R$  is a comm ring. A subset  $I \subseteq R$  is called an **ideal** if  $(I, +) \leq (R, +)$  and  $ir, ri \in I$  for all  $i \in I$  and for all  $r \in R$ .

Why do we want ideals? Such that  $R/I$  is a well-defined ring.

**Example 5.**  $\{0\}$  and  $R$  are ideals of  $R$ .

**Example 6.** If  $R$  is commutative and  $a \in R$ , then  $(a) = \{ar \mid r \in R\}$  is called the **principal ideal** generated by  $a$ .

← Prove this (be convinced)!  
Also known as  $aR$ .

**Definition 8.** A **principal ideal domain** is an integral domain where all ideals are principal ideals.

**Example 7.** The only ideals of  $(\mathbb{Z}, +)$  are of the form  $n\mathbb{Z} = (n)$ .

← Ideals generated by  $n$

**Non-example 8.**  $\mathbb{Z}[x]$  is a UFD but NOT a PID because the ideal  $(2, x) = \{2r + xs \mid r, s \in \mathbb{Z}[x]\}$  is not principal.

← Observe that  $(2, x)$  is an ideal made of polynomials with even constant terms. This cannot be principal, since if we only have 2 and not  $x$ , we do not have nonzero polynomials with zero constant terms.

**Lemma 2.** If  $I \subseteq R$  is an ideal and  $1 \in I$ , then  $I = R$ .

*Proof.* Try it!

**Proposition 3.** If  $I \subseteq R$  is an ideal containing a unit of  $R$  then  $I = R$ .

*Proof.* If  $u \in I$  is a unit then  $u^{-1} \in R$ , so  $uu^{-1} = 1 \in I$ . Then the result follows from Lemma 2.  $\square$

**Definition 9.** A **field** is a commutative ring whose each nonzero element is a unit.

**Corollary 4.** If  $R$  is an ID whose ideals are  $(0)$  and  $R$ , then  $R$  is a **field**.

← The converse is also true. **The only ideals in a field are 0 and the field.**

*Proof.* Suppose  $a \in R \setminus \{0\}$  and consider  $(a)$ . Since  $a \in (a)$ ,  $(a) = R$ . Hence, we must have that  $1 \in (a)$ , which means  $1 = ar$  for some  $r \in R$ .  $\square$

**Definition 10.** Suppose  $R$  is an integral domain. A *proper* ideal  $P \subsetneq R$  is called **prime** if whenever  $ab \in P$  for some  $a, b \in R$ , then  $a$  or  $b \in P$ .

**Non-example 9.**  $(6)$  is not a prime ideal of  $\mathbb{Z}$  since  $2 \times 3 \in (6)$  but neither  $2, 3 \in (6)$ .

**Non-example 10.**  $(2)$  is not a prime ideal of  $\mathbb{Z}[\sqrt{-5}]$  since  $6 \in (2)$ , but we observe that  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$  while  $1 \pm \sqrt{-5} \notin (2)$ .

← Observe that in  $\mathbb{Z}[\sqrt{-5}]$ , we have  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3$ , so it is not a UFD!

**Example 11.**  $(2)$  is a prime ideal of  $\mathbb{Z}$ .

**Definition 11.** A proper ideal  $M \subsetneq R$  is called **maximal** if whenever  $I \subseteq R$  such that  $M \subseteq I \subseteq R$  is an ideal containing  $M$ , then either  $I = M$  or  $I = R$ .

**Proposition 5.** Every proper ideal is contained in a maximal ideal.

← This might not be unique in non-local rings.

*Proof.* TBD. □

**Proposition 6.** Suppose  $R$  is a commutative ring.

- $(0)$  is prime *if and only if*  $R$  is an integral domain.
- $(0)$  is maximal *if and only if*  $R$  is a field.

← By def of prime, if  $ab = 0$ , then either  $a = 0$  or  $b = 0$ , which means there are NO zero divisors.

*(The following is kind of on a tangent)*

**Definition 12.** A commutative ring  $R$  with unity is called **Noetherian** if, whenever  $I_1 \subseteq I_2 \subseteq \dots$  is an ascending sequence of (proper) ideals of  $R$ , there exists an  $n > 0$  such that  $I_n = I_{n+1} = \dots$  are the same ideals thereafter.

← The chain stops ascending!

**Theorem 7.**  $R$  is Noetherian *if and only if* all ideals of  $R$  are finitely generated.

**Corollary 8.** All Principal Ideal Domains are Noetherian.

← Since all ideals are generated by 1 elt.

*(Tangent ends here)*

**Definition 13.** Suppose  $R$  is a commutative ring with  $1 \neq 0$  and  $I \subseteq R$  is an ideal. Then the quotient ring of  $R$  by  $I$  is the set

$$R/I = \{r + I \mid r \in R\}$$

with addition and multiplication defined representative-wise.

**Remark.** The **coset criterion** of ideals: let  $I$  be an ideal; the cosets  $r + I, s + I$  are the same *if and only if*  $r - s \in I$ .

**Example 12.**

- In  $\mathbb{Z}/(6)$  aka.  $\mathbb{Z}/6\mathbb{Z}$ , we have  $2 + (6) = \{\dots, -10, -4, 2, 8, 14, \dots\} = 26 + (6)$  due to  $2 - 26 \in (6)$ ;
- In  $\mathbb{Q}[x]/(x^2 - 2)$ , we have

$$\{3x^2 - 47x + 1 + q(x)(x^2 - 2) \mid q(x) \in \mathbb{Q}[x]\} = \{-47x + 7 + q(x)(x^2 - 2) \mid q(x) \in \mathbb{Q}[x]\}$$

$$\text{due to } 3x^2 - 47x + 1 - (-47x + 7) \in (x^2 - 2).$$

**Remark.** Let  $I$  be an ideal of  $R$ . Then  $(I, +) \trianglelefteq (R, +)$ .

**Definition 14.**  $R/I$  is a group under  $(r + I) + (s + I) = (r + s) + I$  and the operation  $+$  is well-defined. We also define that  $(r + I)(s + I) = (rs) + I$ . We claim that multiplication in  $R/I$  is also well-defined.

*Proof.* Let  $r_1 + I = r_2 + I$  and  $s_1 + I = s_2 + I$ . By coset criterion,  $r_1 - r_2 = i$ ,  $s_1 - s_2 = j$  for some  $i, j \in I$ . Hence  $r_1 s_1 = (r_2 + i)(s_2 + j) = r_2 s_2 + i s_2 + j r_2 + ij$  where the latter three terms are all in the ideal  $I$ . Thus,  $(r_1 s_1) + I = (r_2 s_2) + I$ .  $\square$

From  $R$ ,  $R/I$  inherits nice properties:

- $0 + I = 0_{R/I}$
- $1 + I = 1_{R/I}$
- Multiplication is commutative and distributive over addition in  $R/I$ , so it is also a comm. ring with identity.

**Definition 15.** A function  $\varphi : R \rightarrow S$  between rings is called a **ring homomorphism** if the following are satisfied:

- $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$
- $\varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2)$

**Theorem 9.** First ring isomorphism theorem

If  $\varphi : R \rightarrow S$  is a ring homomorphism, then  $R / \ker(\varphi) \cong \varphi(R)$ .

**Example 13.** If  $R$  is a ring and  $I$  is an ideal, then  $\pi : R \rightarrow R/I$  where  $r \mapsto r + I$  is a surjective homomorphism where  $\ker(\pi) = I$ . This is the *canonical projection* onto  $R/I$ .

**Corollary 10.** If  $I$  is a maximal ideal, then  $R/I$  is a field.

Recall Proposition 6. We now have a stronger statement:

**Proposition 11.** Suppose  $R$  is a commutative ring &  $P \subseteq R$  is an ideal. Then  $R/P$  is an integral domain *if and only if*  $P$  is prime.

*Proof.*  $R/P$  is an integral domain *if and only if* whenever  $(a+P)(b+P) = 0_{R/P}$  then one of  $a+P$  or  $b+P$  must already be  $0_{R/P}$ . This happens *if and only if* whenever  $ab+P = P$  then  $a+P$  or  $b+P$  in  $P$ , which happens *if and only if* whenever  $ab \in P$  then one of  $a, b \in P$ , which is the definition of a prime ideal.  $\square$

**Example 14.** The map  $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}$  where  $p(x) \mapsto p(0)$  is a surjective ring homomorphism with  $\ker(\varphi) = (x)$ . By the First Isomorphism Theorem 9,  $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ . As such, we conclude that  $(x)$  is a prime ideal since  $\mathbb{Z}$  is an integral domain.

**Lemma 12.** Suppose  $R$  is a comm. ring with  $M \subseteq R$  being an ideal.

There is a bijective correspondence between the ideals of  $R/M$  and the ideals of  $R$  containing  $M$ .

← Observe that kernels are ideals! And ideals are kernels of some homomorphism too.

← The *if and only if* version comes in Proposition 14.

← btw,  $(x) \subsetneq (x, 2)$ . the latter is the set of polynomials whose constant term is even, so it is also a proper ideal of  $\mathbb{Z}[x]$ . This is an excellent example where Prime  $\not\Rightarrow$  Maximal.

*Proof.* Consider the projection  $\pi : R \rightarrow R/M$  where  $r \mapsto r + M$ . It is enough to show:

$$\begin{aligned}\pi(\pi^{-1}(J)) &= J && \text{for all ideals } J \subseteq R/M, \text{ and} \\ \pi^{-1}(\pi(I)) &= I && \text{for all ideals } M \subseteq I \subseteq R\end{aligned}$$

← To see why this is okay, see Homework 2 Sec. 7.3 P. 24

To prove the first statement, observe that, if  $J$  is an ideal of  $R/M$ , then  $\pi^{-1}(J) = \{r \in R \mid r + M \in J\}$  and so

$$\pi(\pi^{-1}(J)) = \{\pi(r) \in R/M \mid r + M \in J\} = \{r + M \mid r + M \in J\} = J$$

Next, to prove the second statement, first suppose  $M \subseteq I \subseteq R$  is an ideal. Let  $a \in I$ . Then  $a + M \in \{\alpha + M \mid \alpha \in I\} = \pi(I)$ . This implies that  $a \in \pi^{-1}(\pi(I))$ , and so  $I \subseteq \pi^{-1}(\pi(I))$ .

Conversely, suppose  $r \in \pi^{-1}(\pi(I))$ . This is the same as saying  $\pi(r) = r + M \in \pi(I) = \{\alpha + M \mid \alpha \in I\}$ . Hence, for any  $r \in \pi^{-1}(\pi(I))$ , there exists some  $a \in I$  such that  $r + M = a + M$ . Thus,  $r - a \in M \subseteq I$  by coset conditions. Since  $a \in I$ , we have  $a + (r - a) \in I$ , meaning that  $r \in I$  for any  $r \in \pi^{-1}(\pi(I))$ . This means that  $\pi^{-1}(\pi(I)) \subseteq I$ .

Hence,  $I = \pi^{-1}(\pi(I))$ .

Consequently, for any ideals  $J \subseteq R/M$ , we know that  $\pi^{-1}(J) \subseteq R$  is an ideal containing  $M$ . And if  $M \subseteq I \subseteq R$  is an ideal, we know  $\pi(I) \subseteq R/M$  is an ideal. Since  $\pi(\pi^{-1}(J)) = J$  and  $I = \pi^{-1}(\pi(I))$  for any  $I, J$ , the correspondence is a bijection.  $\square$

← Think about why this contains  $M$ !

**Proposition 13.** Suppose  $R$  is a comm. ring with an identity and  $I \subseteq R$  is an ideal. Then  $R/I$  is a field *if and only if*  $I$  is maximal.

*Proof.* If  $I$  is maximal, then there are no other proper ideals strictly containing  $I$ . Hence, by Lemma 14, we have that  $R/I$  only have ideals  $(0)$  and  $R/I$  itself. This happens *if and only if*  $R/I$  is a field.  $\square$

**Corollary 14.** If  $R$  is a commutative ring with identity and  $M \subseteq R$  is maximal, then  $M$  is prime.

← Hence maximal implies prime, but prime does not necessarily implies maximal.

*Proof.* Maximal  $\implies$  quotient is a field  $\implies$  quotient is an ID  $\implies$  prime.  $\square$

**Definition 16.** An integral domain  $R$  is an **Euclidean domain** if there exists a norm  $N : R \rightarrow \mathbb{Z}_{\geq 0}$  with  $N(0) = 0$  such that for all  $a, b \in R$  with  $b \neq 0$ , there exists  $q, r \in R$  for which

$$a = bq + r$$

with  $N(r) < N(b)$  or  $r = 0$ .

**Example 15.**  $\mathbb{Z}$  is a ED with  $N(a) = |a|$ .

**Example 16.**  $\mathbb{Q}[x]$  is a ED with  $N(p(x)) = \deg(p(x))$ .

**Example 17.** Every field  $F$  is a ED with  $N(a) = 0 \forall a \in F$ .

**Non-example 18.**  $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$  is a PID that is not an ED.

- ← Because in a field everything divides!
- ← This is one of the only good examples!

### Why do we care about Euclidean domains?

**Remark.** Greatest common divisors exist and are relatively quick to compute.

**Definition 17.** If  $a, b \in R$ , then  $\gcd(a, b) = c$  means

1.  $c$  divides  $a$  and  $b$ ; that is,  $a = cr, b = cs$  for some  $r, s \in R$
2. If  $c' \in R$  with  $c' | a$  and  $c' | b$ , then it must be true that  $c' | c$ .

- ← Using recursive application of Euclidean algorithm.
- ← All other common divisors divide the gcd.
- ← This is a much faster algorithm than factoring!

**Example 19.** Say we want to compute the gcd of 47 and 10.

$$47 = 4 \times 10 + 7$$

$$10 = 1 \times 7 + 3$$

$$7 = 2 \times 3 + \textcircled{1}$$

$$3 = 3 \times 1$$

← circled is  $\gcd(47, 10)$

← final line with no remainders

This also works for finding gcds in  $\mathbb{Q}[x]$  with polynomials long division and norm  $\deg(p(x))$ .

**Remark.** If  $F$  is a field, then  $F[x]$  is a Euclidean domain.

- ← Just use long division!

**Remark.** Euclidean domains are PIDs.

*Proof.* Suppose  $R$  is a ED and  $I \subseteq R$  is an ideal. Consider  $\{N(a) \mid a \in I \setminus \{0\}\}$ . This set has a minimal element by properties of natural numbers (or is an empty set if and only if  $I = (0)$ ).

Let  $d \in I$  be an element of minimum norm (hence  $N(d) \leq N(a)$  for all  $a \in I$ ). We claim that  $(d) = I$ . Proof:

Since  $d \in I$ , we have  $rd \in I$  for any  $r \in R$ . This implies that  $(d) \subseteq I$ .

Then let  $a \in I$ . Since  $R$  is a ED, we first assume that there exists  $q, r \in R, r \neq 0$  such that  $a = qd + r$  and  $N(r) < N(d)$ . But we notice that  $r = a - qd$  must be in  $I$  as both  $a, qd \in I$ , contradicting the minimality of  $N(d)$ . Thus, it must be that  $r = 0$ . This implies  $a = qd$  and thus  $a \in (d)$  for all  $a \in I$ . Consequently,  $I \subseteq (d)$ , and therefore  $I = (d)$ .  $\square$



**Definition 18.** Suppose  $R$  is an integral domain and  $p \in R \setminus \{0\}$ . Then  $p$  is a **prime element** if  $(p)$  is a prime ideal.

**Proposition 15.** An element  $p \in R$  is prime *if and only if* whenever  $p|ab$  then  $p|a$  or  $p|b$ .

*Proof.*  $p$  is prime means that  $(p)$  is a prime ideal. This is true *if and only if* whenever  $ab \in (p)$  then  $a \in (p)$  or  $b \in (p)$ . This is the same as saying if  $ab = kp$  for some  $k \in R$  then  $a = lp$  or  $b = lp$  for some  $l \in R$ . This is to say that whenever  $p|ab$  then  $p|a$  or  $p|b$ .  $\square$

**Proposition 16.** In an integral domain, all prime elements are irreducibles.

*Proof.* Suppose  $R$  is an ID and  $p \in R$  is prime. If  $p = ab$  for some  $a, b$  in  $R$ , then, WLOG,  $p|a$ . That is,  $a = pk$  for some  $k \in R$ . Hence,  $p = pkb$ . Since in an ID cancellation rule holds,  $kb = 1$ , meaning that  $b$  is a unit. Thus,  $p$  is irreducible by definition Definition 5.  $\square$

**Proposition 17.** In PIDs, all *nonzero* prime ideals are maximal.

*Proof.* Suppose  $R$  is a PID and  $(p) \subseteq R$  is a prime ideal. If  $(p) \subseteq (m) \subseteq R$  is an ideal, then  $p \in (p) \subseteq (m)$  hence  $p = rm$  for some  $r \in R$ . Since  $p \nmid rm$ , we have  $p|r$  or  $p|m$ .

If  $p|r$ , this implies that  $r = pk$  for some  $k \in R$ . Substituting into  $p = rm$ , we get  $p = pkm$ . By cancellation, we get  $km = 1$ , meaning that  $m$  is a unit. Hence,  $(m) = R$ .

If  $p|m$ , we have  $m = pl$  for some  $l \in R$ , meaning that  $m \in (p)$ . Hence,  $(m) \subseteq (p)$ , but we also defined that  $(p) \subseteq (m)$ , so  $(m) = (p)$ .

Therefore,  $(p)$  has to be the maximal ideal.  $\square$

**Proposition 18.** In an UFD, irreducible implies prime.

*Proof.* Let  $R$  be a UFD and  $p \in R$  be irreducible. Let  $a, b \in R$  such that  $p|ab$ . Hence,  $pr = ab$  for some  $r \in R$ . Since  $R$  is a UFD, let  $a = q_1 \dots q_n, b = s_1 \dots s_m$  be the factorization. Since the factorizations are unique and each of the  $q_i, s_j$  are irreducible, if  $p|ab$ , then  $p$  must be an associate with one of the  $q_i, s_j$ . Therefore, either  $p|a$  or  $p|b$ , implying prime.  $\square$

**Example 20.**  $\mathbb{Q}$  is a field, so  $\mathbb{Q}[x]$  is a ED. Since EDs are UFDs, irreducible  $\implies$  prime. We see that  $x^2 - 2 \in \mathbb{Q}[x]$  is an irreducible element, which means that  $(x^2 - 2)$  is a prime ideal, meaning that it is a maximum ideal, meaning that  $\mathbb{Q}[x]/(x^2 - 2)$  is a field. We observe that it is a field containing  $\mathbb{Q}$  and  $(\sqrt{2})$ .

$\leftarrow$  In fact, this is the smallest field containing  $\mathbb{Q}$  and  $(\sqrt{2})$ .

**Lemma 19.** In a PID, irreducible elements are prime.

*Proof.* Suppose  $p \in R$  is irreducible in the principal ideal domain  $R$ . If  $p|ab$  for some  $a, b \in R$ , we want to show that either  $p|a$  or  $p|b$ , hereby showing that  $p$  is prime. Hence, we consider the ideal  $(a, p) = d$ , which is necessarily principal for some  $d \in R$ . Since  $a, p \in (d)$ , we have  $a = dr$  and  $p = ds$  for some  $r, s \in R$ . As  $p$  is irreducible, we get that one of  $d$  and  $s$  is a unit.

We first assume that  $s$  is a unit, in which case  $d = ps^{-1}$ , and so  $a = ps^{-1}r$  implying that  $p|a$ .

In another case,  $d$  is a unit, in which case  $(a, p) = (d) = R$  and so  $1 = ak + pl$  for some  $k, l \in R$ . Multiplying by  $b$ , we get  $b = abk + pbl$ . Since  $p|ab$ , we have  $b = abk + pbl = pmk + pbl$  for some  $m \in R$ . Hence,  $b = p(mk + bl)$ , meaning that  $p|b$ .

Therefore, whenever  $p|ab$ , either  $p|a$  or  $p|b$ . Hence, in a PID,  $p$  is prime whenever it is irreducible.  $\square$

**Proposition 20.** PIDs are UFDs.

*Proof.* Suppose  $R$  is a PID and  $a \in R$  is nonzero, nonunit. If  $a$  is irreducible, we are done. If not, we write  $a = p_1q_1$  for some  $p_1, q_1 \in R$  nonunit. If  $p_1, q_1$  are irreducibles, we are done. If not, then WLOG say  $q_1 = p_2q_2$  for some nonunits  $p_2, q_2$ . We would like to show that this splitting process terminates.

Observe that  $(q_1) \subseteq (q_2)$  since  $q_2|q_1$ . Hence, the chain of splitting results in the chain of ideals  $(q_1) \subseteq (q_2) \subseteq (q_3) \subseteq \dots$ .

Now consider the ideal  $\bigcup_{i=1}^{\infty} (q_i)$ . Since this is a PID, we have  $\bigcup_{i=1}^{\infty} (q_i) = (q)$  for some  $q \in R$ . Since  $q \in \bigcup_{i=1}^{\infty} (q_i)$ , it is contained in some  $(q_n)$  for some  $n \geq 1$ . This implies that  $(q) \subseteq (q_n)$ , but we also know that  $(q_n) \subseteq (q)$ , hence  $(q) = (q_n)$ . Hence, this process terminates, and there exists an  $n$  in this chain such that  $q_n$  is irreducible. Therefore,  $R$  is a factorization domain.

Now we want to prove the uniqueness. That is, if  $p_1 \dots p_n = q_1 \dots q_m$  for irreducibles  $p_i, q_j$  and  $n \leq m$  WLOG, then we want to show that  $m = n$  and that  $p_i = u_i q_i$  with units  $u_i$  up to reordering for all  $i$ . We do so by induction on  $n$ .

<sup>1</sup>The proof that this is an ideal is as follows:

We first prove that  $\bigcup_{n=1}^{\infty} I_n$  is a subgroup of  $R$  under addition. Let  $r, s \in \bigcup_{n=1}^{\infty} I_n$ , where  $r \in I_k$  and  $s \in I_{k+i}$  for some  $k, i \in \mathbb{N}$ . Since  $I_1 \subseteq I_2 \subseteq \dots$  are ideals of  $R$ , we know that  $r \in I_k$  implies that  $r \in I_{k+i}$ . Thus,  $r - s \in I_{k+i}$  due to  $I_{k+i}$  being an ideal. As  $I_{k+i} \subseteq \bigcup_{n=1}^{\infty} I_n$ , we have  $r - s \in \bigcup_{n=1}^{\infty} I_n$ , which means that  $\bigcup_{n=1}^{\infty} I_n$  is closed under additive inverse. Hence,  $\bigcup_{n=1}^{\infty} I_n$  is a subgroup of  $R$  under addition.

Then, we prove that for any  $t \in R, r \in \bigcup_{n=1}^{\infty} I_n$ , we would have  $tr, rt \in \bigcup_{n=1}^{\infty} I_n$ . Since  $r \in \bigcup_{n=1}^{\infty} I_n$ , it must be true that  $r \in I_k$  for some  $k \in \mathbb{N}$ . Hence,  $tr, rt \in I_k$  due to  $I_k$  being an ideal. Therefore,  $tr, rt \in \bigcup_{n=1}^{\infty} I_n$  for any  $t \in R, r \in \bigcup_{n=1}^{\infty} I_n$ .

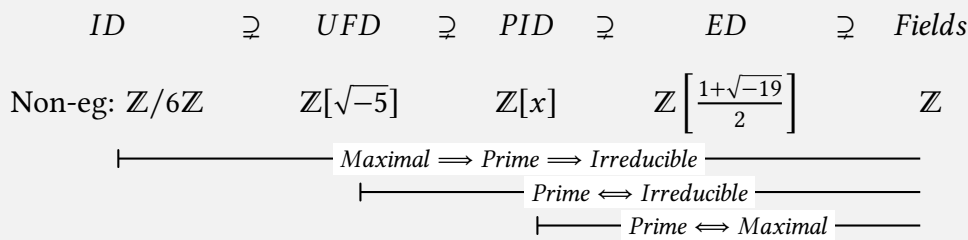
In conclusion, since  $\bigcup_{n=1}^{\infty} I_n$  is a subgroup of  $R$  under addition with the property that  $tr, rt \in \bigcup_{n=1}^{\infty} I_n$  for any  $t \in R, r \in \bigcup_{n=1}^{\infty} I_n$ , it is an ideal of  $R$ .  $\square$

(Base case) If  $p_1 = q_1 \dots q_m$  and  $p_1$  irreducible, then  $q_2 \dots q_m$  are all units. Hence,  $m = 1$  and  $p_1 = q_1$ .

(Inductive step) Say we have already proven the statement for  $n = k$ . Then consider  $p_1 p_2 \dots p_{k+1} = q_1 q_2 \dots q_m$ . Since  $R$  is a PID where irreducible implies prime,  $p_1$  is a prime element dividing the product of primes  $q_1 q_2 \dots q_m$ , so we say WLOG  $p_1 | q_1$ . This means that  $q_1 = u_1 p_1$  for some  $u \in R$ , but since  $q_1$  is not reducible, it forces  $u_1$  to be a unit. Hence, we apply cancellation on both sides and get  $p_2 \dots p_{k+1} = (u_1 q_2) \dots q_m$ .

By inductive hypothesis,  $m - 1 = k$  and  $p_i, q_i$  are associates up to reordering for any  $i$ . Hence, the factorization must be unique.  $\square$

We have shown:



## Field extensions

We observe that the polynomial  $x^2 - 2 \in \mathbb{Q}[x]$  is irreducible. If we have  $x^2 - 2 = p(x)q(x)$  where  $p, q$  nonunits, then  $\deg(p) + \deg(q) = 2$  and we cannot have any  $0+2$  combinations due to constants being units, we only have  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ , but  $x \pm \sqrt{2} \notin \mathbb{Q}[x]$ !

Since  $\mathbb{Q}[x]$  is a UFD, the irreducible element  $(x^2 - 2)$  is prime, and since  $\mathbb{Q}[x]$  is a PID,  $(x^2 - 2)$  is maximal which means that  $\mathbb{Q}[x]/(x^2 - 2)$  is a field.

Phase II plan: Field extensions!

Suppose  $F$  is a field and  $p(x) \in F[x]$  nonzero. Recall that  $F[x]$  is a ED with the norm function  $\deg(a(x))$  and long division of polynomials. Let  $a(x) + (p(x)) \in F[x]/(p(x))$ . By the division algorithm, we have  $a(x) = p(x)q(x) + r(x)$  for  $q(x), r(x) \in F[x]$  and  $\deg(r(x)) < \deg(p(x))$  or  $r(x)$  is the zero polynomial.

←  $a(x)$  is a coset rep  
← We can do division algorithm since this is an ED

Now we see that since  $a(x) - r(x) \in (p(x))$ , they are in the same coset! Hence  $a(x) + (p(x)) = r(x) + (p(x))$ . We observe that every element of  $F[x]/(p(x))$  can be represented by a polynomial of a degree less than  $\deg(p(x))$ . In other words, if  $\deg(p(x)) = n$ , then  $F[x]/(p(x))$  is of the form

← The expression under the bar functions like  $r(x)$ ! Also note that span is just the set of linear combinations.

$$\begin{aligned} F[x]/(p(x)) &= \left\{ \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \mid a_0, a_1, \dots, a_{n-1} \in F \right\} \\ &= \text{Span}_F\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\} \end{aligned}$$

In fact,  $F[x]/(p(x))$  is (partly) just a **vector space** over  $F$ ...

← Why is this not the vector space over  $F/(p(x))$  but just  $F$ ? See the next paragraph.

We shall observe that it does not matter if we are using  $F$  or  $\bar{F}$ .

Consider  $\varphi : F \hookrightarrow F[x]/(p(x))$  where  $a \mapsto \bar{a}$ . We observe this is an **injective** map: whenever  $\deg(p(x)) = n > 0$ , we have  $\varphi(a) = \varphi(b)$  if and only if  $\bar{a} = \bar{b}$ , which happens if and only if  $a - b \in (p(x))$ ; but the difference of two constants always have  $\deg 0$  and cannot be in  $(p(x))$  unless it is a straight zero, which tells us that  $\bar{a} = \bar{b}$  if and only if  $a = b$ . In other words,  $F[x]/(p(x))$  contains an isomorphic copy of  $F$ , its field of scalars! Namely,  $\overline{F \cong \varphi(F) = \{\bar{a} \in F[x]/(p(x)) \mid a \in F\}}$ .

...Hence,  $F[x]/(p(x))$  is a vector space **of dimension  $n$**  over the scalar field  $F$  that also contains an isomorphic copy of  $F$ .

Moreover, if  $p(x)$  is irreducible, then  $(p(x))$  is prime since this is an ED, and hence, it is also a maximal ideal, meaning that  $F[x]/(p(x))$  is a field containing an isomorphic copy of  $F$ .

← all thanks to Euclidean domains!

**Definition 19.** Suppose  $F \subseteq K$  are fields. Then  $K$  is called a **field extension** of  $F$ .

- Notation:  $K/F$  or  $\begin{smallmatrix} K \\ | \\ F \end{smallmatrix}$  (the lattice notation)

← Please, this is NOT a quotient. DO NOT CONFUSE THOSE!!

The dimension of  $K$  as a vector space over  $F$  is called the **degree** of the extension.

- Notation:  $[K : F]$

But does my field  $F$  always have an extension? Here is a systematic way to get extensions:

**Example 21.** If  $p(x) \in F[x]$  is an irreducible polynomial of degree  $n \geq 1$  over the field  $F$ , then  $F[x]/(p(x))$  is a **field extension** of  $F$  of degree  $n$ .

← Since  $\varphi(F) \cong F$ , and  $\varphi(F) \subseteq F[x]/(p(x))$

Furthermore, if  $p(x) = a_0 + a_1x + \cdots + a_nx^n$ , then  $\bar{x}$  is a **root** of

$$\varphi(p(x)) = \bar{a}_0 + \bar{a}_1y + \cdots + \bar{a}_ny^n \in (F[x]/(p(x)))[y]$$

because, plugging in  $y = \bar{x}$ , we get

$$\bar{a}_0 + \bar{a}_1\bar{x} + \cdots + \bar{a}_n\bar{x}^n = \overline{p(x)} = \bar{0} \in F[x]/(p(x))$$

Hence, the isomorphic copy of the polynomial  $p(x)$  has **roots** in the field extension  $F[x]/(p(x))$ .

So, what the hell is  $F[x]/(p(x))$ ? We have already shown that the field extension  $F[x]/(p(x))$  does indeed contain a root of  $p(x)$ . Now we think about it **the other way around**: if we want to find an extension of  $F$  that contains a root of  $p(x)$ , we would eventually get this one!

Suppose  $p(x) \in F[x]$  is irreducible. Let  $K/F$  be an extension, and  $\alpha \in K$  a root of  $p(x)$ . Denote by  $F(\alpha) \subseteq K$  the **smallest** subfield of  $K$  that contains both  $F$  and  $\alpha$ . Consider the map  $\varphi : F[x] \rightarrow F(\alpha) \subseteq K$  where  $q(x) \mapsto q(\alpha)$  is simply the evaluation at  $\alpha$  map. We note that  $p(x) \in \ker(\varphi) = (d(x))$  since an ED is a PID; this implies that  $p(x) = u(x)d(x)$ . As  $p(x)$  is irreducible,  $u(x)$  must be a unit, which means  $p(x)$  and  $d(x)$  are associates and  $\ker(\varphi) = (p(x))$ . Therefore,

$$F[x]/(p(x)) = F[x]/\ker(\varphi) \cong \varphi(F[x]) \subseteq F(\alpha)$$

by first isomorphism theorem. However,  $F(\alpha) \subseteq K$  the **smallest** subfield of  $K$  that contains both  $F$  and  $\alpha$ , so  $\varphi(F[x])$  cannot be smaller than that. Hence, it must be true that  $\varphi(F[x]) = F(\alpha)$ .

Therefore,  $F(\alpha)$  is simply  $F[x]/(p(x))$ . □

### To summarize so far!

Suppose  $p(x) \in F[x]$  is an irreducible polynomial with coefficients in the field  $F$ .

- $F[x]/p(x)$  is a **field** containing an isomorphic copy of  $F$  in which  $\bar{x} = x + (p(x))$  is a **root** of (the image of)  $p(y) \in (F[x]/(p(x)))[y]$ .

**Example 22.** In  $\mathbb{Q}[x]/(x^2 - 2)$ , we have  $x + (x^2 - 2)$  is a root of  $y^2 - \bar{2} \in (\mathbb{Q}[x]/(x^2 - 2))[y]$  because

$$\begin{aligned} & (x + (x^2 - 2))^2 - (2 + (x^2 - 2)) \\ &= x^2 - 2 + (x^2 - 2) && \text{by coset addition \& multiplication} \\ &= 0 + (x^2 - 2) && \text{since } x^2 - 2 \in (x^2 - 2) \\ &= \bar{0} \end{aligned}$$

← We think about modding out by  $(p(x))$  as making it equal to zero, which is how we find roots.

← Observe that  $\varphi(F[x])$  is a field:  $\ker(\varphi)$  is a maximal ideal

Furthermore, if  $\deg(p(x)) = n$ , then

$$F[x]/(p(x)) = \left\{ \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \mid a_0, a_1, \dots, a_{n-1} \in F \right\}$$

is a vector space over  $F$  of dimension  $n$ .

**Example 23.**  $\mathbb{Q}[x]/(x^2 - 2) = \{\bar{a}_0 + \bar{a}_1\bar{x} \mid a_0, a_1 \in \mathbb{Q}\} = \text{Span}_{\mathbb{Q}}\{\bar{1}, \bar{x}\}$

- If  $K/F$  is an extension and  $\alpha \in K$  is a root of  $p(x)$ , denote by  $F(\alpha)$  **the smallest field containing  $F$  and  $\alpha$**  ← Read ' $F$  adjoint  $\alpha$ '

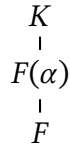


Figure 1: Field diagram

Then  $F(\alpha) \cong F[x]/(p(x))$ , and

$$\begin{aligned} F(\alpha) &= \left\{ \overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} \mid a_0, a_1, \dots, a_{n-1} \in F \right\} \\ &= F[\alpha] \quad \leftarrow \text{the polynomial of } \alpha \text{ over } F \end{aligned}$$

← The eval map  
 $\varphi : F[x] \rightarrow F(\alpha)$   
 where  $f(x) \mapsto f(\alpha)$   
 has in fact  
 $\ker(\varphi) = (p(x))$   
 when  $\alpha$  is a root of  
 $p(x)$ .

**Example 24.**  $\mathbb{Q}(\sqrt{2}) = \{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{2}]$

## Irreducibility – a survey

**Proposition 21.** If  $p(x) \in F[x]$ , then  $\alpha \in F$  is a root *if and only if*  $x - \alpha$  divides  $p(x)$ .

*Proof.* Write  $p(x) = (x - \alpha)q(x) + r(x)$  with  $q(x), r(x) \in F[x]$  and  $\deg(r(x)) = 0$  or  $r(x) = 0$ . Then  $0 = p(\alpha) = 0 + r(\alpha)$  which forces  $r(x) = 0$ . □

**Corollary 22.** A degree-2 or -3 polynomial over a field  $F$  is irreducible *if and only if* it has no roots in  $F$ .

**Proposition 23.** Suppose  $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$  with root  $\frac{c}{d}$  written in reduced form (i.e.  $\gcd(c, d) = 1$ ). Then  $\boxed{c|a_0 \text{ and } d|a_n}$ .

*Proof.*

$$\begin{aligned} d^n \cdot p\left(\frac{c}{d}\right) &= 0 \\ 0 &= (a_0d^n + a_1d^{n-1}c + \cdots + a_{n-1}dc^{n-1}) + a_nc^n \end{aligned}$$

$$0 = a_0 d^n + (a_1 d^{n-1} c + \cdots + a_{n-1} d c^{n-1} + a_n c^n)$$

Looking at the 2nd line, since  $d$  divides all of the ones in the  $()$ , it must also divide the last term  $a_n c^n$ . However, since  $\gcd(c, d) = 1$ , it forces  $d$  to divide  $a_n$ .

Similarly, we make the same argument for  $c$  and  $a_0$  using the 3rd line.  $\square$

**Lemma 24.**  $(R/I)[x] \cong R[x]/(I)$  where  $(I) = I[x]$ .

*Proof.* Consider the surjective homomorphism  $\pi : R[x] \rightarrow (R/I)[x]$ .  $\square$

**Proposition 25** (Eisenstein's Criterion). Suppose  $f(x) = 1x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$  is a monic polynomial and  $p \in \mathbb{Z}$  is a **prime** such that  $p \mid a_0, \dots, a_{n-1}$  but  $p^2 \nmid a_0$ . Then  $f(x)$  is irreducible.

*Proof.* Assume BWOC that  $f(x) = a(x)b(x)$  for some nonunit  $a(x), b(x) \in \mathbb{Z}[x]$ , then

$$x^n = \bar{f}(x) = \bar{a}(x)\bar{b}(x)$$

in  $(\mathbb{Z}/p\mathbb{Z})[x] \cong \mathbb{Z}[x]/p\mathbb{Z}[x]$  since all other terms are divisible by  $p$ . Since  $\mathbb{Z}/p\mathbb{Z}$  does not contain any zero divisors,  $\bar{a}(x), \bar{b}(x)$  must have zero constant terms. Hence  $a(x), b(x)$  have constant terms that are multiples of  $p$ , so  $a(x)b(x)$  have constant term divisible by  $p^2$ . This is a contradiction with  $p^2 \nmid a_0$ .  $\square$

**Lemma 26** (Gauss' Lemma). If  $p(x) \in \mathbb{Z}[x]$  is reducible in  $\mathbb{Q}[x]$ , then it is reducible in  $\mathbb{Z}[x]$ .

*Proof.* Suppose  $p(x) = a(x)b(x)$  for  $a(x), b(x) \in \mathbb{Q}[x]$ . Then by multiplying by coefficient denominators, for some  $m \in \mathbb{Z}$ , we could write  $m \cdot p(x) = c(x)d(x)$  for some  $c(x), d(x) \in \mathbb{Z}[x]$ . Now since  $m \in \mathbb{Z}$ , we could write  $m = q_1 q_2 \dots q_n$  be a product of irreducibles in  $\mathbb{Z}$ .

Now in  $(\mathbb{Z}/q_1\mathbb{Z})[x] \cong \mathbb{Z}[x]/(q_1\mathbb{Z})[x]$ , we observe that  $m \cdot p(x) = c(x)d(x) = q_1(q_2 \dots q_n)p(x)$ , meaning that

$$\overline{c(x)} \overline{d(x)} = \overline{q_1(q_2 \dots q_n)p(x)} = \bar{0}$$

Since  $(\mathbb{Z}/q_1\mathbb{Z})[x] \cong \mathbb{Z}[x]/(q_1\mathbb{Z})[x]$  is an integral domain, WLOG,  $\overline{c(x)} = \bar{0}$  if and only if  $c(x) \in q_1\mathbb{Z}[x]$ , meaning that all coefficients of  $c(x)$  are multiples of  $q_1$ . Therefore,  $\frac{1}{q_1}c(x) \in \mathbb{Z}[x]$ .

← since  $q_1$  is irreducible and hence prime in UFD

Now we repeat the process for all  $q_1, q_2, \dots, q_n$  and we are done.  $\square$

Recall that if  $F \subseteq K$  are fields,  $\alpha \in K$  and  $p(x) \in F[x]$  is irreducible with root  $\alpha$ , then

$$F[\alpha] = F(\alpha) \cong F[x]/(p(x)) = \overline{\{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}}$$

We observe that this has a few implications. For instance,  $F(\alpha)$  contains  $\frac{1}{\alpha}$ , meaning that it could also be written as a polynomial of  $\alpha$  with coefficients in  $F$  (as in  $F[\alpha]$ )!

← since it is a field containing the mult. inverse of  $\alpha$

**Definition 20.** Suppose  $K/F$  is a field extension and  $\alpha \in K$ . We say that  $\alpha$  is **algebraic over  $F$**  if there exists  $p(x) \in F[x]$  such that  $p(\alpha) = 0$ . If not,  $\alpha$  is **transcendental**.

**Definition 21.** The extension  $K/F$  is an **algebraic extension** if **every** element  $\alpha \in K$  is algebraic over  $F$ .

**Example 25.**  $\pi$  is transcendental over  $\mathbb{Q}$  but algebraic over  $\mathbb{R}$  (since it is a root of  $x - \pi$ ).

**Proposition 27.** If  $K/F$  is a **finite extension**, then it is an algebraic extension.

← finite extension just means finite degree  
 $[K : F] < \infty$

*Proof.* Call  $[K : F] = n$  and let  $\alpha \in K$ . Then the  $n + 1$  elements  $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$  must be linearly dependent. Hence, by linear algebra, there exist  $a_0, a_1, \dots, a_n \in F$  not all zero such that the linear combination  $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$ . Hence,  $\alpha$  is a root of  $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$ .  $\square$

← since  $n + 1 > \dim(K/F) = n$

**Corollary 28.** If  $K/F$  is an extension and  $\alpha \in K$ , then  $\alpha$  is algebraic over  $F$  if and only if  $[F(\alpha) : F] < \infty$ .

*Proof.*

( $\Leftarrow$ ) Follows from prop.

( $\Rightarrow$ ) If  $\alpha$  is algebraic, then there exists an irreducible polynomial  $p(x)$  with  $\alpha$  as a root and of degree  $n < \infty$ . Then  $F(\alpha) \cong F[x]/(p(x))$  is a  $n$ -dimensional vector space over  $F$ .

Another perspective:  $F(\alpha) = \text{Span}_F\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ .

← Review proof of  $F(\alpha) \cong F[x]/(p(x))$ .

$\square$

**Proposition 29.** Suppose  $K/F$  is an extension &  $\alpha \in K$  is algebraic over  $F$ . Then there exists a unique, irreducible, and monic polynomial  $m_{\alpha, F}(x) \in F[x]$  that has  $\alpha$  as a root.

**Remark.** We observe that  $m$  does depend on the base field  $F$ ;  $m_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2$ , but  $m_{\sqrt{2}, \mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$ .



*Proof.* Since the subset of  $F[x]$  satisfying  $\alpha$  is a root is nonempty, we can pick one with a **minimal degree**. By multiplying by an element of  $F$  if necessary, we can assume WLOG this polynomial is **monic**. Call it  $m_{\alpha,F}(x)$ .

Assume BWOC that  $m$  is the product of two other polynomials of lesser degree such that  $m_{\alpha,F}(x) = a(x)b(x)$ , then we plug in  $0 = m_{\alpha,F}(\alpha) = a(\alpha)b(\alpha)$ . Since there are no zero divisors in  $F[x]$ , WLOG  $a(\alpha) = 0$ , contradicting the minimality of  $m_{\alpha,F}$ . Hence  $m_{\alpha,F}$  is **irreducible**.

← So  $F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$

Then, BWOC if  $p(x) \in F[x]$  with  $\alpha$  as a root and is monic and irreducible, there exist  $q(x), r(x) \in F[x]$  such that  $p(x) = m_{\alpha,F}(x)q(x) + r(x)$  where  $\deg(r) < \deg(m_{\alpha,F})$  or  $r(x) = 0$ . Then, we observe that  $p(\alpha) = 0 = m_{\alpha,F}(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha)$ . Thus,  $r(\alpha) = 0$ , so  $\deg(r) \geq \deg(m_{\alpha,F})$  unless  $r(x) = 0$  by minimality. Hence we must have  $r(x) = 0$ , so  $m_{\alpha,F} | p$ . This contradicts the assumption that  $p$  is monic and irreducible. Therefore,  $m_{\alpha,F}$  is the **only** minimal, monic and irreducible polynomial where  $\alpha$  is a root.  $\square$

**Definition 22.**  $m_{\alpha,F}(x)$  is the **minimal** polynomial of  $\alpha$  over  $F$ .