MATH172 Galois Theory Notes

Xuehuai He

October 26, 2023

Contents

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. $r \times 1 = 1 \times r = r$ ← this is optional
- $r(s+t) = rs + rt$ and $(s+t)r = sr + tr \qquad \forall s, r, t \in R$

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

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: $\mathbb{Q}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Q}\}$ is a commutative ring ← square brackets just mean "polynomials in..."
- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a commutative ring

---

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 $\boxed{r \in R}$.

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

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. □

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

Definition 10. Suppose R is an integral domain. A *proper* ideal $P \subsetneq R$ is called **prime** of 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 $2, 3 \notin (6)$.

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. Axiom of choice. □

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 $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending sequence of (proper) ideals of R, there exists an $n > 0$ such that $I_n = I_{n+1} = \ldots$ 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

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

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

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

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, $(r_1 s_1) + I = (r_2 s_2) + I$. □

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 $\varphi : R \to S$ 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

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

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

Example 13. If R is a ring and I is an ideal, then $\pi : R \to R/I$ 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.

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

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. □

Example 14. The map $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ where $p(x) \mapsto p(0)$ is a surjective ring homomorphism with $\ker(\varphi) = (x)$. By the 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.

← 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.

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.

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

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

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

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

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

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. □

← 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. □

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. □

Definition 16. An integral domain R is an **Euclidean domain** if there exists a norm $N : R \to \mathbb{Z}_{\geq 0}$ 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 $N(a) = 0 \ \forall \ a \in F$.

← Because in a field everything divides!

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

← 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.

← Using recursive application of Euclidean algorithm.

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 $c'|c$.

← All other common divisors divide the gcd.

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

$$\begin{aligned} 47 &= 4 \times 10 + 7 \\ 10 &= 1 \times 7 + 3 \\ 7 &= 2 \times 3 + 1 && \leftarrow \text{circled is } \gcd(47, 10) \\ 3 &= 3 \times 1 && \leftarrow \text{final line with no remainders} \end{aligned}$$

← This is a much faster algorithm than factoring!

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 idea;. Consider $\{N(a) \mid a \in I\backslash\{0\}\}$. 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 assumes 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, $I \in (d)$, and therefore $I = (d)$. □

Definition 18. Suppose R is an integral domain and $p \in R\backslash\{0\}$. 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 $p|b$. □

Proposition 16. In an integral domain, all prime elenments 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. □

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 $p|rm$, 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. □

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. □

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 $(\sqrt{2})$.

← 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. □

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[1] $\bigcup_{i=1}^{\infty}(q_i)$. 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 $p_i = u_iq_i$ with units u_i up to reordering for all i. We do so by induction on n.

[1] 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. □

(*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:

	ID	$\supsetneq$	*UFD*	$\supsetneq$	*PID*	$\supsetneq$	*ED*	$\supsetneq$	*Fields*
Non-eg:	$\mathbb{Z}/6\mathbb{Z}$		$\mathbb{Z}[\sqrt{-5}]$		$\mathbb{Z}[x]$		$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$		$\mathbb{Z}$

Maximal $\Longrightarrow$ *Prime* $\Longrightarrow$ *Irreducible* (ID through Fields)

Prime $\Longleftrightarrow$ *Irreducible* (UFD through Fields)

Prime $\Longleftrightarrow$ *Maximal* (PID through Fields)

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 <u>every element of $F[x]/(p(x))$ can be represented by a polynomial of a degree less than $\deg(p(x))$</u>. In other words, if $\deg(p(x)) = n$, then $F[x]/(p(x))$ is of the form

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

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

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* $a = b$. <u>In other words, $F[x]/(p(x))$ contains an isomorphic copy of F, its field of scalars!</u> Namely, $\boxed{F \cong \varphi(F) = \{\bar{a} \in F[x]/(p(x)) \mid a \in F\}}$.

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

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

← 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 $\begin{array}{c} K \\ | \\ F \end{array}$ (*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 $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, then $\bar{x}$ is a **root** of

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

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

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

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

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 α. Consider the map $\varphi : F[x] \to F(\alpha) \subseteq K$ where $q(x) \mapsto q(\alpha)$ is simply the evaluation at α 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 α, so $\varphi(F[x])$ cannot be smaller than that. Hence, it must be true that $\varphi(F[x]) = F(\alpha)$.

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

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 $\overline{x} = x + (p(x))$ 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 $y^2 - \overline{2} \in (\mathbb{Q}[x]/(x^2-2))[y]$ because

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

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

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

is a vector space over F of dimension n.

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

- 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** α.

← Read 'F adjoint α'

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

Figure 1: Field diagram

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

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

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

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 $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ with root $\frac{c}{d}$ written in reduced from (i.e. $\gcd(c,d) = 1$). Then $\boxed{c|a_0 \text{ and } d|a_n}$.

Proof.

$$\begin{aligned} d^n \cdot p\left(\frac{c}{d}\right) &= 0 \\ 0 &= (a_0 d^n + a_1 d^{n-1} c + \cdots + a_{n-1} d c^{n-1}) + a_n c^n \end{aligned}$$

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

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. □

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

Proof. Consider the surjective homomorphism $\pi : R[x] \to (R/I)[x]$. □

Proposition 25 (Eisenstein's Criterion)**.** Suppose $f(x) = \mathbb{1}x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a monic polynomial and $p \in \mathbb{Z}$ is a **prime** such that $p \mid a_0, \ldots, a_{n-1}$ but $p^2 \nmid a_0$. Then $\underline{f(x) \text{ is irreducible}}$.

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 $p^2 \nmid a_0$. □

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 $m = q_1 q_2 \ldots q_n$ 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 $m \cdot p(x) = c(x)d(x) = q_1(q_2 \ldots q_n)p(x)$, meaning that

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

Since $(\mathbb{Z}/q_1\mathbb{Z})[x] \cong \mathbb{Z}[x]/(q_1\mathbb{Z})[x]$ is an <u>integral domain</u>, WLOG, $\overline{c(x)} = \overline{0}$ *if and only if* $c(x) \in q_1\mathbb{Z}[x]$, meaning that all coefficients of $c(x)$ are multiples or 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 $q_1, q_2, \ldots, q_n$ and we are done. □

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

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

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 α with coefficients in F (as in $F[\alpha]$)!

← since it is a field containing the mult. inverse of α

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

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

Example 25. π 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 $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ must be linearly dependent. Hence, by linear algebra, there exist $a_0, a_1, \ldots, a_n \in F$ not all zero such that the linear combination $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$. Hence, α is a root of $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$. □

← since $n+1 > \dim(K/F) = n$

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

Proof.

($\Longleftarrow$) Follows from prop.

($\Longrightarrow$) If α is algebraic, then there exists an irreducible polynomial $p(x)$ with α 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: $F(\alpha) = \mathrm{Span}_F\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

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

□

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 α 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* α *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 α 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 $p(\alpha) = 0 = m_{\alpha,F}(\alpha)q(m_{\alpha,F}) + r(\alpha) = 0 + r(\alpha)$. 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 α is a root. □

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

(The following is kind of on a tangent)

Some exam prep!

- In general, for subrings $R \subseteq S$, we have if $r \in R^\times$, then $r \in S^\times$.
- If we adjoint one root of an irreducible polynomial to a field, the fields are isomorphic no matter which root of that polynomial we adjoint.

(Tangent ends here)

To summarize, if K/F is a field extension and $\alpha \in K$, then α is **algebraic** over F if it is the root of some polynomials in $F[x]$. For each algebraic α, there exists a unique, monic, irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ such that $m(\alpha) = 0$. In that case, the degree of extension $[F(\alpha) : F] = \deg(m_{\alpha,F}(x))$; and, if $p(\alpha) = 0$ for some $p(x) \in F[x]$, then $m_{\alpha,F}|p(x)$. In general, if $[K : F] < \infty$, then K/F is algebraic. Thus, $[F(\alpha) : F] < \infty$ *if and only if* α is algebraic over F.

Proposition 30. If $F \subseteq K \subseteq L$ are fields, then

$$[L : F] = [L : K] \cdot [K : F]$$

← $mn\left(\begin{array}{c} L \\ \big|\, n \\ K \\ \big|\, m \\ F \end{array}\right.$

Proof. We first see that if $[K : F] = \infty$, then for any $N \in \mathbb{N}$, there exists $\alpha_1, \ldots, \alpha_N \in K$ that are linearly independent over F. In that case, it is certainly true that $\alpha_1, \ldots, \alpha_N \in L$ are linearly independent over F. Thus, $[L : F] = \infty$.

← Linear independence implies that whenever $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_N\alpha_N = 0$ for some coefficients $a_1, \ldots, a_N \in F$, then necessarily $a_1 = a_2 = \cdots = a_N = 0$.

If $[L : K] = \infty$, then for any $N \in \mathbb{N}$, there exists $\beta_1, \ldots, \beta_N \in L$ that are linearly independent over K. As a result, it also is linearly independent over F. Hence, $[L : F] = \infty$.

If $[K : F] = m$ and $[L : K] = n$, let $\alpha_1, \ldots, \alpha_m \in K$ be a basis for K over F and $\beta_1, \ldots, \beta_n \in L$ be a basis for L over K.

Claim: $\{\alpha_i\beta_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ forms a basis for L over F. □

← Use linear combinations to prove this claim.

Some nice consequences:

Corollary 31. Suppose K/F is an extension and $\alpha, \beta \in K$ are algebraic over F. Then:

- $F(\alpha, \beta) = (F(\alpha)(\beta))$
- $[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = \deg\left(m_{\alpha,F(\beta)}(x)\right) \cdot \deg\left(m_{\beta,F(x)}\right)$. However, note that the minimal polynomial

$$m_{\alpha,F(\beta)}(x) \mid m_{\alpha,F}(x) \in F(\beta)[x]$$

  so $\deg(m_{\alpha,F(\beta)}(x)) \leq \deg(m_{\alpha,F}(x))$. Hence,

$$[F(\alpha, \beta) : F] \leq \deg(m_{\alpha,F}(x)) \deg(m_{\beta,F}) < \infty$$

  This means that whenever α, β are algebraic over F, we get that $F(\alpha, \beta)/F$ is an algebraic extension.
- As a result, $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ are all algebraic over F. The algebraic elements hence form a **field**.

← the smallest subfield of K containing F, α, β

← since $p(\alpha) = 0 \iff m_{\alpha,F}(x) | p(x)$

Proposition 32. Suppose K/F is an extension. Then $[K : F] < \infty$ *if and only if* $K = F(\alpha_1, \ldots, \alpha_n)$ could be written where $\alpha_1, \ldots, \alpha_n \in K$ are algebraic over F.

In other words, an extension is finite *if and only if* it is generated by adjoining a finite amount of algebraic elements.

Proof.

($\Longrightarrow$) If $[K : F] < \infty$, then suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K over F. Then $\alpha_1, \ldots, \alpha_n$ are algebraic and every element of K is an F-linear combination of α_is. Hence K must be the smallest field containing F and α_is, which means $K = F(\alpha_1, \ldots, \alpha_n)$.

($\Longleftarrow$) We observe that

$$\begin{aligned}[K : F] &= [(F(\alpha_1, \dots, \alpha_{n-1}))(\alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdot \ldots \cdot [F(\alpha_1) : F] \\ &\leq \prod_{i=1}^{n} \deg(m_{\alpha_i, F}(x)) < \infty\end{aligned}$$

$\square$

Corollary 33. If L/K and K/F are algebraic extensions, then so is L/F.

← L/K and K/F need not be finite!

Proof. Suppose $\alpha \in L$. Since L/K is algebraic, there exists $p(x) \in K[x]$ such that $p(\alpha) = 0$. Let $\alpha_0, \dots, \alpha_n \in K$ be the coefficients of $p(x)$, necessarily algebraic over F since K/F algebraic. Therefore,

$$[F(a_0, \dots, a_n, \alpha) : F] = [(F(a_0, \dots, a_n))(\alpha) : F(a_0, \dots, a_n)][F(a_0, \dots, a_n) : F]$$

Since $p(\alpha) = 0$ has coefficients in $K \supseteq F(\alpha_0, \dots, \alpha_n)$, we have $[(F(a_0, \dots, a_n))(\alpha) : F(a_0, \dots, a_n)] < \infty$. The second term is also clearly $< \infty$. Therefore, $[F(a_0, \dots, a_n, \alpha) : F] < \infty$, meaning that α is algebraic over F. $\square$

←

$$\begin{tikzcd}
L \arrow[dr, dash] \arrow[dd, dash] & \\
& (F(a_0, \dots, a_n))(\alpha) \arrow[dd, dash] \\
K \arrow[dr, dash] \arrow[dd, dash] & \\
& F(a_0, \dots, a_n) \\
F \arrow[ur, dash] &
\end{tikzcd}$$

Definition 23. Suppose L/F is an extension & K_1 and K_2 are intermediate fields. The **composite** field K_1K_2 is the smallest subfield of L containing K_1 and K_2.

$$\begin{tikzcd}
& L \arrow[d, dash] & \\
& K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
& K_1 \cap K_2 \arrow[d, dash] & \\
& F &
\end{tikzcd}$$

Definition 24. Suppose F is a field and $p(x) \in F[x]$. The **splitting field** of $p(x)$ over F is the smallest field extension of F over which $p(x)$ could be factored into **linear factors**.

← Assuming that splitting fields **exist** and are **unique** up to isomorphism.

Remark. If E is the splitting field of $p(x)$ over F then $[E : F] \leq n!$ where $n = \deg(p(x))$.

Remark. Such an extension is called **normal**.

Proposition 34. Splitting fields exist.

Proof outline. By induction on $\deg(p(x))$, whose base case, $\deg(p(x)) = 1$, yields F as a splitting field. More generally, any $p(x)$ has a root α in $F(\alpha) \cong F[x]/(q(x))$ for some irreducible $q(x)$ so $p(x) = (x - \alpha)f(x) \in F(\alpha)[x]$. We observe that $\deg(f(x)) = \deg(p(x)) - 1$. Induction takes care of the rest. $\square$

← The splitting field of $p(x)$ over F is the same as the splitting field of $f(x)$ over $F(\alpha)$

Remark. K is a splitting field over F *if and only if* every irreducible $p(x) \in F[x]$ that has one root in K has **all** its roots in K.

Non-example 26. $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is not such an extension.

Lemma 35. Suppose $\varphi : F_1 \to F_2$ is a field isomorphism, $p_1(x) \in F_1[x]$, and $p_2(x) =$" $\varphi((p_1(x)))$" (φ applied to coeffs of $p_1(x)$). Let α_1 be a root of the irreducible factor $q_1(x)$ of $p_1(x)$, and let $q_2(x) =$" $\varphi(q_1(x))$" and α_2 be a root of $q_2(x)$. Then there exists an isomorphism $\tau : F_1(\alpha_1) \to F_2(\alpha_2)$ such that $\tau(\alpha_1) = \alpha_2$ and $\tau_{|F_1} = \varphi$ (this means "τ restricted to F_1").

← In this way, φ induce a ring isomorphism $F_1[x] \to F_2[x]$.

Proof outline.

$$\begin{array}{lccccccc}
 & F_1(\alpha_1) & \xrightarrow{\sim} & F_1[x]/(q_1(x)) & \xrightarrow{\sim} & F_2[x]/(q_2(x)) & \xrightarrow{\sim} & F_2(\alpha_2) \\
 & \alpha_1 & \longrightarrow & \bar{x} & \longrightarrow & \bar{x} & \longrightarrow & \alpha_2 \\
\text{if } a \in F_1, & a & \longrightarrow & \bar{a} & \longrightarrow & \overline{\varphi(a)} & \longrightarrow & \varphi(a)
\end{array}$$

□

Proposition 36. Suppose $F_1, F_2, \varphi, p_1(x)$ and $p_2(x)$ are as in Lemma 35. Let $E_1 \& E_2$ be splitting fields of p_1 and p_2 respectively. Then there exists an isomorphism $\sigma : E_1 \to E_2$ such that $\sigma_{|F_1} = \varphi$.

← if we set $F_1 = F_2$ and $p_1 = p_2$, we get corollary: splitting fields are unique up to isomorphism.

Proof. Proceed by induction on $\deg(p_1(x))$. For the base case, if $\deg(p_1(x)) = 1$, then $E_1 = F_1$ and $\sigma = \varphi$.

Assume the result is true for all polynomials of fixed degree $k \geq 1$ and suppose $\deg(p_1(x)) = k+1$. Let α_1 be a root of $p_1(x)$ and α_2 be a root of the φ-corresponding irreducible factor of $p_2(x)$. By Lemma 35, φ can be extended to $\tau : F_1(\alpha_1) \to F_2(\alpha_2)$ such that $\tau_{|F_1} = \varphi$.

In $(F_1(\alpha_1))[x]$, we can factor out $p_1(x) = (x - \alpha_1)g_1(x)$, and in $(F_2(\alpha_2))[x]$ we factor $p_2(x) = (x - \alpha_2)g_2(x)$ with $g_2(x) = \tau(g_1(x))$. We observe that E_1 and E_2 are the splitting fields of g_1 and g_2 over $F_1(\alpha_1)$ and $F_2(\alpha_2)$!

←

$$\begin{array}{lccc}
\sigma : & E_1 & \xrightarrow{\sim} & E_2 \\
 & | & & | \\
\tau : & F_1(\alpha_1) & \to & F_2(\alpha_2) \\
 & | & & | \\
\varphi : & F_1 & \xrightarrow{\sim} & F_2
\end{array}$$

By inductive hypothesis, τ could be extended to σ and $\sigma_{|F_1(\alpha)} = \tau$ and $\sigma_{|F_1} = \varphi$. □

Corollary 37. Splitting fields are unique.

Proof. Set $F_1 = F_2$, $\varphi =$id, $p_1(x) = p_2(x)$. □

(The following is kind of on a tangent)

Homework hint: the proof of existence & uniqueness of splitting fields relied on inductive arguments where we adjoin one root at a time. This is the same as saying $E = F(\alpha_1, \dots, \alpha_n)$ but this tends to overlook isomorphic ways to adjoin roots. In this context, it is convenient to start by considering a specific K containing F and all roots of $p(x)$. In that case, $E = F(\alpha_1, \dots, \alpha_n)$ becomes more rigorous.

(Tangent ends here)

Definition 25. A polynomial is called **separable** if it doesn't have repeated roots.

← First note that a poly of degree n over a field has exactly n roots.

Definition 26. Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The **formal derivative** of $f(x)$ is the polynomial

$$D_x f(x) = f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$$

From this definition, we can check that the usual differential rules hold.

Lemma 38. Suppose F is a field, $f(x)$ is a polynomial in $F[x]$, and E/F a field extension containing a root α of $f(x)$. Then α is a repeated root of $f(x)$ *if and only if* α is a root of the formal derivatve $f'(x)$.

Proof. If α is a repeated root of $f(x)$ then $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$. In that case, $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$ and so $f'(\alpha) = 0$.

Conversely, if $f'(\alpha) = 0$, then differentiating $f(x) = (x-\alpha)h(x)$ (where $h(x) \in E[x]$) and plugging $x = \alpha$ yields $0 = f'(\alpha) = h(\alpha) + (\alpha - \alpha)h'(\alpha) = h(\alpha)$. This is saying that $h(x) = (x-\alpha)g(x)$ for some $g(x) \in E[x]$. □

Lemma 39. If $f(x) \in F[x]$ is **irreducible and not separable**, then $f'(x) = 0$.

finish proof.

□

If $f(x)$ is not constant and $f'(x) = 0$, then $\mathrm{char}(F) = p > 0$ and $f(x) = g(x^p)$.

← All powers in $f(x)$ are multiples of $p(x)$.

Proposition 40. If $\mathrm{char}(F) = 0$, or $|F| < \infty$ and $\mathrm{char}(F) = p$, then every irreducible polynomial in $F[x]$ is separable.

Proof. For the case of char=0, it follows from 39.

For the case of char>0, suppose F is a finite field of p^n elements[2]. Then the map $F \to F$ where $\alpha \mapsto \alpha^p$ is a field isomorphism. Hence, every element of F is a p^{th} power.

← Use binomial theorem.

← Such fields are called **perfect**.

Now suppose BWOC $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ is an irreducible but not separable polynomial. Therefore, $f'(x) = 0$ must be true. This happens *if and only if* $f(x) = \sum_{j=0}^{m} a_{jp} x^{jp}$, that is, the x in all terms are of p^{th} degree. However, we know that all elements $a_{jp} \in F$ are already the p^{th} powers of sth else $(b_{jp})^p = a_{jp}$, so

$$f(x) = \sum_{j=0}^{m} (b_{jp}^p) x^{jp}$$

and by reverse Binomial Theorem, we get

$$f(x) = \sum_{j=0}^{m} (b_{jp}^p) x^{jp} = \left(\sum_{j=0}^{m} b_{jp} x^j \right)^p$$

is not irreducible! □

Non-example 27. Let $F = \mathbb{F}_p(t) = \left\{ \frac{f(t)}{p(t)} \,\middle|\, f(t), g(t) \in \mathbb{F}_p[t], g(t) \neq 0 \right\}$.

← This is a field of char>0 but is infinite.

Then $p(x) = x^p - t$ is not separable (but it is irreducible). This can be seen if we suppose α is a root of $p(x)$ (so $\alpha = t$). Then, in $F(\alpha)[x]$, we have $p(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p$, which tells us $p(x)$ is not separable.

← The coefficients of $p(x)$ are ratios of polys in $\mathbb{F}_p(t)$.

(The following is kind of on a tangent)

Prime fields

Suppose R is a commutative ring with identity. The map $\mathbb{Z} \to R$ where $n \mapsto \pm(\underbrace{1_R + 1_R + \cdots + 1_R}_{|n| \text{ times}})$ ($-$ if $n < 0$) is a ring homomorphism with kernel $n\mathbb{Z}$ where $n = \text{char}(R)$. So:

← check it!

- if char $(R) = 0$, then R contains $\mathbb{Z}$;
- if char $(R) = n > 0$, then R contains $\mathbb{Z}/n\mathbb{Z}$.

[2] See Section 27

If F is a field, then:

- if char $(F) = 0$, then F conatins $\mathbb{Q}$;
- if char $(F) = p > 0$, then p prime and F contains $\mathbb{Z}/p\mathbb{Z}$. ← That is, F is an extension of $\mathbb{Z}/p\mathbb{Z}$!

In other words, every field is an extension of $\mathbb{Q}$ or $\mathbb{F}_p$. Moreover, a finite field is a *finite* extension of $\mathbb{F}_p$: if $[F : \mathbb{F}_p] = n$, then $|F| = p^n$.

In addition, $|F - \{0\}| = p^n - 1 \implies$ if $\alpha \in F - \{0\}$ then $\alpha^{p^n-1} = 1$, implying that if $\alpha \in F$, then $\alpha^{p^n} = \alpha$, meaning that α is a root of $x^{p^n} - x \in F[x]$. Therefore, F is the splitting field of $x^{p^n} - x$. But splitting fields are unique, so we conclude that there is only one unique finite field for each order. ← By Lagrange's Theorem

(Tangent ends here)

Definition 27. An algebraic extension K/F is called (algebraically) **separable** if $m_{\alpha,F}(x)$ is separable for **all** $\alpha \in K$.

Definition 28. A finite extension K/F is called **Galois** if K/F is normal and separable. ← normal just means it is a splitting field of something

Galois Theory

Definition 29. If K/F is an extension, then the **automorphism group** of K/F is defined as

$$\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(a) = a \,\forall\, a \in F\}$$

That is, all the automorphisms of K that also fix the field F.

Theorem 41 (The Fundamental Theorem of Galois Theory)**.**

If K/F is Galois, then

$$\begin{tikzcd}
K \arrow[d, dash] & & 1 \arrow[d, dash] \\
E \arrow[d, dash] \arrow[rr, shift right, "\mathrm{Aut}(K/E)"'] & & H \arrow[ll, shift right, "\{\alpha\in K \mid \sigma(\alpha)=\alpha\ \forall\ \sigma\in H\}"'] \arrow[d, dash] \\
F & & \mathrm{Aut}(K/F)
\end{tikzcd}$$

where H is a subgroup of $\mathrm{Aut}(K/F)$ that fixes the field E, an extension of F contained in K.

> **Galois theory** is concerned with the study of roots of polynomials by way of automorphisms of splitting fields (of separable polynomials).
> In particular, we are interested in what
>
> $$\mathrm{Aut}(K) = \{\sigma : K \to K \text{ isomorphisms}\}$$
>
> (a group under composition) is. Naturally, such groups are *finite*.

← review MATH171 finite groups!

Last time, we showed that $K \supseteq \begin{Bmatrix} \mathbb{Q} & \text{if } \mathrm{char}(K) = 0 \\ \mathbb{F}_p & \text{if } \mathrm{char}(K) = p \end{Bmatrix}$, since $\sigma(1) = \sigma(1^2) = (\sigma(1))^2$ implies that $\sigma(1) = 1$ must always be true! Hence, $\sigma(n) = n$ must be true in char 0 fields, or $\sigma(\bar{n}) = \bar{n}$ if char>0 for all $n \in \mathbb{Z}$. Therefore, σ **fixes** the prime subfield $\mathbb{Q}$ or $\mathbb{F}_p$.

Remark. Why does Definition 29 have to fix the field F? Because we've shown that $\mathrm{Aut}(K) = \begin{Bmatrix} \mathrm{Aut}(K/\mathbb{Q}) & \text{if } \mathrm{char}(K) = 0 \\ \mathrm{Aut}(K/\mathbb{F}_p) & \text{if } \mathrm{char}(K) = p \end{Bmatrix}$.

Lemma 42. If K/F is an extension, $\alpha \in K$ is algebraic over F and $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$.

Proof. Observe that $m_{\alpha,F}(\alpha) = 0 = \sigma(0) = \sigma(m_{\alpha,F}(\alpha))$. Hence, since $\sigma(\alpha) = \alpha$ for all $\alpha \in F$,

$$\sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n = m_{\alpha,F}(\sigma(\alpha))$$

□

So if $f(x) \in F[x]$, then every $\sigma \in \mathrm{Aut}(K/F)$ **permutes** the roots of $f(x)$ that lie in K. It would be nice if the roots of $f(x)$ all lived in K. This is why we consider K the splitting field of some polynomial over F.

← Recall: if irreducible $f(x)$ has one root in such K, then all roots lie in K.

Proposition 43. If K is the splitting field of some polynomial $f(x)$ over F (so $[K : F] < \infty$), then $|\mathrm{Aut}(K/F)| \leq [K : F]$, with equality if $f(x)$ is separable.

Proof. We will prove a more general statement by induction. If $\sigma : F_1 \to F_2$ is an isomorphism, $f_1(x) \in F_1[x]$ and $f_2(x) = \sigma(f_1(x)) \in F_2[x]$ and E_1 and E_2 are the splitting fields of f_1 and f_2 over F_1 and F_2 respectively. Then we would like to show that there are at most $[E_1 : F_1]$ isomorphisms $\tau : E_1 \to E_2$ such that $\tau_{|F_1} = \sigma$ with equality if f_1 separable.

← The prop above fixes $F_1 = F_2$ and σ being identity.

Base case. If $[E_1 : F_1] = [E_2 : F_2] = 1$, then $E_1 = F_1$, $E_2 = F_2$ and $\tau = \sigma$ is our only choice.

Inductive step. Suppose we've proven the result for all extensions of degree $< n$ for some $n \geq 2$. Now consider $[E_1 : F_1] = [E_2 : F_2] = n$. Pick $\alpha \in E_1 \backslash F_1$ and let $\beta \in E_2$ be any root of $\sigma(m_{\alpha,F_1}(x))$. Then σ could be extended to $\rho : F_1(\alpha) \to F_2(\beta)$ such that $\rho(\alpha) = \beta$ and $\rho_{|F_1} = \sigma$. Observe that $[F_1(\alpha) : F_1] = \deg(m_{\alpha,F_1}(x))$. Moreover, the number of extensions of σ to ρ equals the number of *distinct* roots of $\sigma(m_{\alpha,F_1}(x))$. Thus, the number of extensions of σ to $F_1(\alpha)$ is *at most* the degree of $m_{\alpha,F_1}(x)$ which is $[F_1(\alpha) : F_1]$ with equality if $m_{\alpha,F_1}(x)$ is separable. Since $[E_1 : F_1] = [E_2 : F_2] = n$, we have $[E_1 : F_1(\alpha)] < n$, by inductive hypothesis, there are at most $[E_1 : F_1(\alpha)]$ ways of extending ρ to $\tau : E_1 \to E_2$. Hence,

$$\begin{aligned}
|\{\text{extensions of } \sigma \text{ to } \tau\}| &= |\{\text{extensions of } \sigma \text{ to } \rho\}||\{\text{extensions of } \rho \text{ to } \tau\}| \\
&\leq [F_1(\alpha) : F_1][E_1 : F_1(\alpha)] \\
&= [E_1 : F_1]
\end{aligned}$$

Looking at the case $F_1 = F_2$, $E_1 = E_2$, $\sigma = \text{id}$, we get our result. □

Definition 30. If K/F is a normal extension, then the extension is **Galois** if $[K : F] = |\text{Aut}(K/F)|$.