Contents

1 Intro & Rings

1.1 Motivation

Definition (Radical): An expression involving only $+, -, *, /, \sqrt[n]{\cdot}$.

After a linear transformation, all cubics can be reduced to $x^3 + px = q$, and there is a formula for solutions to the above. Quartics can also be reduced to a cubic and solved.

The quintic was attempted by Euler, Bezout, Lagrange, etc without success. In 1799, Ruffini gave a 516-page proof on the insolubility of the quintic that was almost right. In 1824, Abel filled in the gap in Ruffini's proof.

The main steps of Galois theory are to:

1. Link a root α of a quintic to $\mathbb{Q}(\alpha)$, the smallest field containing α. It has more structure to be played with. Currently, our knowledge of $\mathbb{Q}(\alpha)$ is lacking. For instance, we don't know how many intermediate fields there are between $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ and $\mathbb{Q}$.

$$\begin{tikzcd}
 & \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbb{Q}\left(\sqrt{2}\right) \arrow[dr, no head] & \mathbb{Q}\left(\sqrt{3}\right) \arrow[d, no head] & \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) \cdots \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

   We can list infinitely many of these intermediate fields, but how many are actually distinct?

2. To ameliorate the situation, we link the field $\mathbb{Q}(\alpha)$ to a group. Precisely, we associate the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ to the group

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \left\{\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) : \varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}\right\}$$

   i.e. the set of automorphisms that fix the smaller field. It can be shown that if α is "good" then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. Moreover, there is a bijection between the intermediate fields of $\mathbb{Q}(\alpha)/\mathbb{Q}$ and the subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$. Galois theory is the interplay between fields and groups.

1.2 Review of ring theory

Rings in this course are by and large commutative and unital.

Definition (Integral Domain, Field): A ring R where for all $a, b \in R$ m $ab = 0 \implies a = 0$ or $b = 0$ is an **integral domain**. A **field** is a ring R such that $R^* = R \setminus \{0\}$.

Proposition 1.1 (Subrings of fields): Every subring of a field F, including F itself, is an integral domain.

Definition (Ideal): A subset I of a commutative ring such that $0 \in I$, and for $a, b \in I$ and any $r \in R$, $a - b \in I$ and $ra \in I$.

Remark: If $1 \in I$ is an ideal, then $I = R$, since any $r \in R$ satisfies $r1 = r \in I$, so $R \subseteq I$.

The only ideals of a field F are $\{0\}$ and F, since if $a \in I$ with $a \neq 0$, then $aa^{-1} = 1 \in I$, so $I = F$.

Recall that using the division algorithm in $\mathbb{Z}$, we can prove all ideals of $\mathbb{Z}$ are principal ideals.

Remark: The smallest field containing $\mathbb{Z}$ is $\mathbb{Q}$.

Definition ($F[x]$): Define $F[x] = \{a_0 + \ldots + a_m x^m : a_i \in F\}$.
- If $a_m = 1$, we say f is **monic**.
- If $a_m \neq 0$, the **degree** of f is $\deg(f) = m$. By convention, $\deg(0) = -\infty$.

- For $f, g \in F[x]$, $\deg(fg) = \deg(f) + \deg(g)$.

Notes about $F[x]$:
- $F[x]$ is an integral domain.
- The units of $F[x]$ are $F^* = F \setminus \{0\}$, i.e. the unital constant polynomials.
- The division algorithm works. For f, g with $f \neq 0$, we can write $g(x) = q(x)f(x) + r(x)$ with $\deg(r) < \deg(f)$ (here the $-\infty$ convention is handy).
- Using the DA, we can prove all ideals of $F[x]$ are principal. Moreover, if we impose that generators $f(x)$ are monic, then generators are unique.

Remark: The smallest field containing $F[x]$ is the set of rational functions

$$F(x) := \left\{ \frac{f(x)}{g(x)} : f, g \in F[x] \text{ and } g \neq 0 \right\}$$

Recall when I is an ideal of R, that the additive quotient group R/I is a ring with multiplication $(r + I)(s + I) = rs + I$, and the unit of R/I is $1 + I$.

Theorem 1.2 (First Isomorphism Theorem): Let $\varphi : R \to S$ be a ring homomorphism. Then $\operatorname{Ker}(\varphi)$ is an ideal of R and $R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.

Example: Let F be a field, S a ring, and $\varphi : F \to S$ be a ring homomorphism. Then either φ is injective or the zero map, since $\operatorname{Ker}(\varphi)$ is an ideal of F, hence either $\{0\}$ or F.

Definition (Prime, maximal): Let R be a commutative ring. An ideal $P \neq R$ is a **prime** ideal if whenever $rs \in P$, then $r \in P$ or $s \in P$.

An ideal $M \neq R$ of R is **maximal** if whenever A is an ideal such that $M \subseteq A \subseteq R$, then $A = M$ or $A = R$.

Theorem 1.3: Let $I \neq R$ be an ideal of a commutative ring R. Then

(1) I is maximal iff R/I is a field.

(2) I is prime iff R/I is an integral domain.

Proof:

(1) Suppose I is maximal. Note $I \neq R \iff R/I$ is a commutative ring with 1. We show the non-zero elements in R/I have inverses. Let $a \in R$ with $a \notin I$, so $a + I \neq 0 + I$. Since $a \notin I$, we have $I \subsetneq \langle a \rangle + I = \langle I \cup \{a\} \rangle = R$ by maximality, so $\langle a \rangle + I$ contains 1. Notice

$$\langle a \rangle + I = \{ar + m : m \in I, r \in R\}$$

so say $1 = ar + m$ where $r \in R, m \in I$. Then we have our inverse:

$$(a + I)(r + I) = ar + I = (ar + m) + I = 1 + I$$

Conversely if R/I is a field, since $1 + I \neq 0 + I$ we have $1 \notin I$ so $I \neq R$. Let A be an ideal with $I \subseteq A \subseteq R$ and suppose $A \neq I$. Choose $a \in A - I$ so $a + I \neq 0 + I$. Then since R/I is a field, $a + I$ has an inverse, say $b + M$. Then $(a + I)(b + I) = ab + I = 1 + I$. Then $1 - ab \in I \subseteq A$. Since $a \in A$ we have $ab \in A$, so $1 \in A \implies A = R$. Thus I is maximal.

(2) Since $I \neq R$, R/I is a commutative ring with 1. For $a, b \in R$,

$$(a + P)(b + P) = ab + P.$$

and $a + P = 0 + P \iff a \in P$. So $(a + P)(b + P) = 0 + P \iff ab \in P$. The result is immediate.

⬠

Corollary 1.4: Every maximal ideal is prime.

2 Domains

2.1 Irreducibles and primes

Definition (Divides): Let R be an integral domain and $a, b \in R$. We say a divides b, denoted $a \mid b$, if $ca = b$ for some $c \in R$.

Notice in $\mathbb{Z}$ that if $n \mid m$ and $m \mid n$, then $n = \pm m$ so $\langle n \rangle = \langle m \rangle$.

Proposition 2.1 (Divisibility characterization): Let R be an integral domain. For $a, b \in R$, TFAE:

(1) $a \mid b$ and $b \mid a$

(2) $a = ub$ for some unit $u \in R$

(3) $\langle a \rangle = \langle b \rangle$

Proof:

($1 \implies 2$) Suppose there are $u, v \in R$ so $b = ua$ and $a = vb$. If $a = 0$, then $b = 0$ so $a = 1b$. Otherwise,

$$a = vb = v(ua) = (vu)a \implies a(1 - vu) = 0.$$

Since R is an integral domain and $a \neq 0$, $1 - vu = 0 \iff vu = 1$. Thus v is a unit.

($2 \implies 3$) Say $a = ub$. Then $a \in \langle b \rangle$, so $\langle a \rangle \subseteq \langle b \rangle$. Since u is a unit and $b = u^{-1}a$, $\langle b \rangle \subseteq \langle a \rangle$.

($3 \implies 1$) If $\langle a \rangle = \langle b \rangle$, then $a \in \langle a \rangle = \langle b \rangle$, so $a = tb$ for some $t \in R$, giving $b \mid a$. Similarly, $a \mid b$.

⬠

Definition (Associated): Let R be an integral domain. For $a, b \in R$, we say a is associated to b, denoted $a \sim b$, if $a \mid b$ and $b \mid a$.

Often this is most useful with $a = ub$ for a unit u. From the previous proposition, we can show $\sim$ is an equivalence relation on R.

- $a = 1a \implies a \sim a$
- $a \sim b \implies a = ub \implies b = u^{-1}a = b \sim a$
- $a \sim b$ and $b \sim c$ gives $a = ub$ and $b = vc$ so $a = uvc$ where uv is a unit with inverse $v^{-1}u^{-1}$, so $a \sim c$.

Example: We claim $a \sim a', b \sim b' \implies ab \sim a'b'$ and $a \mid b \iff a' \mid b'$.

Say $a = ua'$ and $b = vb'$, u, v units. Then $ab = uva'b'$ by commutativity of the ring, so $ab \sim a'b'$.

Now suppose $a \mid b$. Then $b = ca$ for some $c \in R$, so $vb' = b = ca = cua'$, giving $v^{-1}cua' = b'$, so $a' \mid b'$. The converse is identical.

Example: Let $R = \mathbb{Z}\left[\sqrt{3}\right] = \left\{m + n\sqrt{3} : m, n \in \mathbb{Z}\right\}$. This is an integral domain, where $\left(2 + \sqrt{3}\right)\left(2 - \sqrt{3}\right) = 1$, so $2 + \sqrt{3}$ is a unit in R. Since $3 + 2\sqrt{3} = \left(2 + \sqrt{3}\right)\sqrt{3}$, we have $3 + 2\sqrt{3} \sim \sqrt{3}$.

Definition (Irreducible): Let R be an integral domain. We say $p \in R$ is **irreducible** if $p \neq 0$ and for all $b, c \in R$, if $p = bc$ then one of b, c is a unit.

Proposition 2.2 (Characterizations of irreducibility): Let R be an integral domain and $p \in R, p \neq 0$ with p not a unit. TFAE:

(1) p is irreducible.

(2) if $d \mid p$, then $d \sim 1$ or $d \sim p$.

(3) if $p \sim ab$, then $p \sim a$ or $p \sim b$.

(4) If $p = ab$, then $p \sim a$ or $p \sim b$.

Proof:

($1 \implies 2$) If $p = ad$ then one of a, d is a unit. If a is a unit then $p \sim d$. If d is a unit, $d \sim 1$.

($2 \implies 3$) If $p \sim ab$, then $b \mid p$. Then $b \sim 1$ or $b \sim p$. If the latter, we're done, if $b \sim 1$, then $a \sim p$.

($3 \implies 4$) If $p = ab$, then $p = 1ab$ so $p \sim ab$.

($4 \implies 1$) Say $p = ab$. If $p \sim a$ then $a = up$ for a unit u, Since R is commutative, $p = ab = upb = pub$ so $1 = ub$ since R is an integral domain. Thus b is a unit. Similarly, $p \sim b$ gives a is a unit.

⬠

Definition (Prime): Let R be an integral domain and $p \in R$. We say p is **prime** if $p \neq 0$ is not a unit, and if $p \mid ab \in R$ then $p \mid a$ or $p \mid b$.

Remark: If $p \sim q$, then p is prime iff q is prime. Indeed, say p is prime and suppose $q \mid ab \in R$. Then $dq = ab$ for some $d \in R$. Say $p = uq$ for a unit $u \in R$, so $ab = du^{-1}p$ so $p \mid ab$, so $p \mid a$ or $p \mid b$. If $p \mid a$ then $cp = a = cuq$ so $q \mid a$. Similarly $p \mid b \implies q \mid b$. The converse is identical.

By induction we can also show if p is prime and $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some i.

Proposition 2.3 (Primes are irreducible): Let R be an integral domain, $p \in R$. If p is prime, then p is irreducible.

Proof: Say $p = ab \in R$, and wlog $p \mid a$. Write $a = dp, d \in R$, so by commutativity $p = dpb = pdb$ so as $p \neq 0$, we have $db = 1$. Thus b is a unit, so p is irreducible. ⬠

Example: The converse is false. Consider $R = \mathbb{Z}\left[\sqrt{-5}\right]$, where we know $p = 1 + \sqrt{-5}$ is irreducible. Note

$$\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 6 = 2 \cdot 3$$

so $p \mid 2 \cdot 3$ but neither of 2 or 3. Indeed, if $p \mid 2$ then $qp = 2$ for some q, then $N(2) = N(q)N(p) \iff 4 = N(q)6$ but there are no integer solutions to this. The same argument works for 3.

Recall that for a prime $p \in \mathbb{Z}$, $\pm 1 \cdot \pm p$ are the only factorizations of p, so p is irreducible. Also, we can prove Euclid's lemma, showing p is prime. The same things hold for $F[x]$ when F is a field. We want to know the additional property of $\mathbb{Z}$ or $F[x]$ that gives us irreducible implying prime.

2.2 Ascending chains

Definition (ACCP): An integral domain R is said to satisfy the **ascending chain conditions on principal ideals** (ACCP) if for any chain

$$0 \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \dots.$$

of principal ideals in R, there is $n \in \mathbb{N}$ so

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \dots.$$

That is, the chain stabilizes eventually.

Example: $\mathbb{Z}$ satisfies ACCP.

Given a chain, we see $a_2 \mid a_1$ and $a_3 \mid a_2$, and so on. Thus taking absolute values gives

$$|a_1| \geq |a_2| \geq \dots.$$

Since each $|a_n| \geq 0 \in \mathbb{Z}$, we get $|a_n| = |a_{n+1}| = \dots$ for some n, so $a_{n+1} = \pm a_i$ for all $i \geq n$. Thus the chain stabilizes, so $\mathbb{Z}$ satisfies ACCP.

Notice this proof using the well-ordering principle on $\mathbb{N}$, and so does the proof of unique factorization over $\mathbb{Z}$ (MATH135).

Theorem 2.4 (Product of irreducibles): Let R be an integral domain satisfying ACCP. If $a \in R$ is not zero and not a unit, then a is a product of irreducibles.

Proof: Suppose bwoc a is not a product of irreducibles. Say $a = x_1 a_1$ where wlog a_1 is not a product of irreducibles, and a is not irreducible so $a \nsim x_1, a_1$. Inductively, construct $a_n = x_{n+1} a_{n+1}$ so $a_n \nsim a_{n+1}$ and a_{n+1} is not a product of irreducibles. Then

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \ldots$$

which violates ACCP, where the ideal containments are proper since $a_n \nsim a_{n+1}$. ⬠

Theorem 2.5 ($R[x]$ ACCP): If R is an integral domain satisfying ACCP, so is $R[x]$.

Proof: Suppose bwoc there is a chain

$$\{0\} \subsetneq \langle f_1 \rangle \subseteq \langle f_2 \rangle \subsetneq \ldots \in R[x].$$

Since $f_{i+1} \mid f_i$, let a_i be the leading coefficient of each f_i to get $a_{i+1} \mid a_i$ for all i. Thus

$$\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots.$$

Since R has ACCP, there is $n \in N$ so $\langle a_n \rangle = \langle a_{n+1} \rangle = \ldots$. For $m \geq n$, we have $f_m = g f_{m+1}$ for some $g(x) \in R[x]$, say g has leading coefficient b. Then $a_m = b a_{m+1}$, so b must be a unit and $\langle a_m \rangle = \langle a_{m+1} \rangle$. Now, if $g = b$ is a constant polynomial, then

$$\langle f_m \rangle = \langle f_{m+1} \rangle,$$

a contradiction, so $\deg(g) \geq 1$. Thus $\deg(f_m) > \deg(f_{m+1})$ for all $m \geq n$, but this is also a contradiction as $\deg(f_i) \geq 0$. ⬠

Example: Since $\mathbb{Z}$ satisfies ACCP, so does $\mathbb{Z}[x]$.

Example: Consider $R = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$, i.e. the set of polynomials in $\mathbb{Q}[x]$ with integer constant term. R is an integral domain, but consider

$$\langle x \rangle = \{x(n + xf)\}, \quad \langle \frac{1}{2}x \rangle = \left\{\frac{1}{2}x(n + xf)\right\}$$

and so on. This gives

$$\langle x \rangle \subsetneq \langle \frac{1}{2}x \rangle \subsetneq \langle \frac{1}{2^2}x \rangle \subsetneq \ldots.$$

Thus R is an integral domain that does not satisfy ACCP.

2.3 Unique factorization domains

Definition (UFD): An integral domain R is called a UFD if it satisfies:

- If $a \neq 0 \in R$ is not a unit, then a is a product of irreducibles
- If $p_1 p_2 \ldots p_n \sim q_1 q_2 \ldots q_s$ where p_i, q_j are irreducible, then $r = s$ and after possible relabelling, $p_i \sim q_i$ for all $i = 1, \ldots, r$.

Example: $\mathbb{Z}$ and $F[x]$ are UFDs, and a field F is also a UFD.

Proposition 2.6 (Irreducible implies prime): Let R be a UFD and $p \in R$. If p is irreducible, then p is prime.

Proof: Let $p \in R$ be irreducible. If $p \mid ab \in R$, write $ab = pd$ for $d \in R$. Since R is a UFD, we can factor a, b, d into irreducible elements:

$$a = q_1 \dots q_k$$
$$b = s_1 \dots s_\ell$$
$$d = r_1 \dots r_m.$$

We allow k, ℓ, m to be 0 in case a, b, d are units. Now since $pd = ab$,

$$pr_1 \dots r_m = q_1 \dots q_k s_1 \dots s_\ell.$$

Since p is irreducible and R is a UFD, $m + 1 = k + \ell$ and $p \sim q_i$ or $p \sim s_j$ for some i or j. Thus $p \mid a$ or $p \mid b$. ⬠

Example: $\mathbb{Z}$ is a UFD, where we know a prime satisfies Euclid's lemma. A similar statement holds for $F[x]$.

Example: Consider $R = \mathbb{Z}\left[\sqrt{-5}\right]$ and $p = 1 + \sqrt{-5}$. We have seen that p is irreducible but not prime, so R is not a UFD. Claim: R satisfies ACCP. Say

$$\{0\} \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots.$$

Then $a_{i+1} \mid a_i$ for all i, and as the norm is non-negative, and multiplicative,

$$N(a_{i+1}) \leq N(a_i).$$

Therefore,

$$N(a_1) \geq N(a_2) \geq \dots,$$

but each $N(a_n) \geq 0$, so we must have $N(a_n) = N(a_{n+1}) = \dots$ for some $n \in \mathbb{N}$.

The takeaway here is UFD implies ACCP, but ACCP does not imply UFD. We would like to know exactly how much stronger a UFD is than an integral domain with ACCP.

Definition (GCD): Let R be an integral domain and $a, b \in R$. We say $d \in R$ is a **greatest common divisor** of a and b, denoted $\gcd(a, b)$ if:
- $d \mid a, b$.
- If $e \in R$ with $e \mid a, b$ then $e \mid d$.

Remark: One can show if R is a UFD and a, b are non-zero and $p_1, \dots, p_k$ are non-associated primes dividing a, b, say

$$a \sim p_1^{\alpha_1} \dots p_k^{\alpha_k}$$
$$b \sim p_1^{\beta_1} \dots p_k^{\beta_k}$$

Then $\gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_k^{\min\{\alpha_k, \beta_k\}}$.

Furthermore, if R is a UFD and $d, a_1, \dots, a_m \in R$, we have

$$\gcd(da_1, \dots, da_m) = d \gcd(a_1, \dots, a_m).$$

Theorem 2.7 (UFD characterization): Let R be an integral domain. TFAE:

(1) R is a UFD

(2) R satisfies ACCP and $\gcd(a, b)$ exists for all $a, b \neq 0 \in R$

(3) R satisfies ACCP and every irreducible element is prime.

Proof:

$(1 \implies 2)$ By the previous remark, $\gcd(a, b)$ exists for all $a, b \neq 0$. Also, suppose

$$\{0\} \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots.$$

Since $\langle a_1 \rangle \neq \{0\}$ and a_1 is not a unit, we can write $a \sim p_1^{k_1} \cdots p_r^{k_r}$ where p_i are non-associated primes and $k_i \in \mathbb{N}$. Since $a_i \mid a_1$ for all i we have

$$a_i \sim p_1^{d_{i,1}} \cdots p_r^{d_{i,r}}$$

for $0 \leq d_{i,j} \leq k_j$ $(1 \leq j \leq r)$. Thus there are only finitely many non-associated choices for a_i, and so there exist $m \neq n$ with $a_m \sim a_n \Longrightarrow \langle a_m \rangle = \langle a_n \rangle$, a contradiction. Hence R satisfies ACCP.

$(2 \Longrightarrow 3)$ Let r be irreducible and suppose $p \mid ab \in R$. Then let $d = \gcd(a, p)$. Since $d \mid p$ which is irreducible, $d \sim 1$ or $d \sim p$. If $d \sim p$ then $d \mid a \Longrightarrow p \mid a$. Otherwise, $d \sim 1$ so $1 \sim \gcd(a, p) \Longrightarrow b \sim \gcd(ab, pb)$, where $p \mid ab$ and $p \mid pb$, so $p \mid b$.

$(3 \Longrightarrow 1)$ R satisfies ACCP, so for $a \neq 0 \in R$ not a unit, a is a product of irreducibles, so it suffices to prove such factorizations are unique. Suppose we have

$$p_1 \cdots p_r \sim q_1 \ldots q_s$$

where each p_i, q_j is irreducible. Since p_1 is prime by assumption, we have $p_1 \mid q_j$ for some j, say wlog $p_1 \mid q_1$. Thus $p_1 \sim q_1$. Since $p_1 \sim q_1$ we can divide out and repeat inductively to get $p_1 \cdots p_r \sim q_1 \ldots q_s$ has $r = s$ and $p_i \sim q_i$ $(1 \leq i \leq r)$. Thus the factorization is unique.

⬠

2.4 Principal ideal domains

Definition (PID): An integral domain R is a **principal ideal domain** (PID) if every ideal in R is principal (singly-generated).

Example: $\mathbb{Z}$ and $F[x]$ are PIDs, as are fields. Note that although all ideals in $\mathbb{Z}_n$ are principal, $\mathbb{Z}_n$ is not an integral domain, so is not a PID.

Proposition 2.8: Let R be a PID and $a_1, \ldots, a_n \neq 0$. Then $d \sim \gcd(a_1, \ldots, a_n)$ exists, and there exist $r_1, \ldots, r_n \in R$ so that

$$\gcd(a_1, \ldots, a_n) \sim r_1 a_1 + \ldots + r_n a_n.$$

Proof: Let $A = \langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \ldots + r_n a_n : r_i \in R\}$ so A is an ideal, hence principal i.e. there is $d \in R$ so $A = \langle d \rangle$. In particular,

$$d = r_1 a_1 + \ldots + r_n a_n$$

for some $r_i \in R$ as $d \in A$. We claim $d \sim \gcd(a_1, \ldots, a_n)$. For each $i \in [n]$, $a_i \in \langle d \rangle$ so $a_i = qd$ for some q, hence $d \mid a_i$. Also, if $r \mid a_i$ for all i, then $r \mid (r_1 a_1 + \ldots + r_n a_n) \Longleftrightarrow r \mid d$, so $d \sim \gcd(a_1, \ldots, a_n) \sim r_1 a_1 + \ldots + r_n a_n$ by definition. ⬠

Theorem 2.9 (PIDs are UFDs): Every PID is a UFD.

Proof: If R is a PID, by Theorem 2.7 and Proposition 2.8 it suffices to show R satisfies ACCP. Suppose

$$\{0\} \subsetneq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots.$$

Let $A = \bigcup_{i \in \mathbb{N}} \langle a_i \rangle$, which is an ideal, so $\langle a \rangle = A$ for some $a \in R$. Then as $a \in A$, there is $n \in \mathbb{N}$ so $a \in \langle a_n \rangle$. Thus $a \in \langle a_m \rangle$ for all $m \geq n$, so $\langle a \rangle \subseteq \langle a_m \rangle \subseteq \langle a \rangle \Longrightarrow \langle a \rangle = \langle a_m \rangle$, so the chain stabilizes. Thus R satisfies ACCP, so is a UFD. ⬠

Example: We claim $\mathbb{Z}[x]$ is not a PID. Consider

$$A := \{2n + x f(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$$

i.e. those polynomials with even constant term. Suppose $A = \langle g(x) \rangle$ for some $g(x) \in \mathbb{Z}[x]$. Since $2 \in A$, $g(x) \mid 2$, so $g(x) \sim 1$ or $g(x) \sim 2$. In the former case, $1 \in A \implies A = \mathbb{Z}[x]$ is a contradiction, and in the latter case, $A = \{2f(x) : f(x) \in \mathbb{Z}[x]\}$ which is also a contradiction, since e.g. $x \in A$. Therefore there exist ideals that are not principal.

Theorem 2.10: Let R be a PID. If $0 \neq p \in R$ is not a unit, TFAE:

(1) p is prime

(2) $R/\langle p \rangle$ is a field (iff $\langle p \rangle$ is a maximal ideal)

(3) $R/\langle p \rangle$ is an integral domain (iff $\langle p \rangle$ is a prime ideal)

Proof:

($1 \implies 2$) Let p be prime and let $0 + \langle p \rangle \neq a + \langle p \rangle \in R/\langle p \rangle$ for some $a \in R$ such that $p \nmid a$. We wish to show $(a + \langle p \rangle)^{-1}$ exists. Consider the ideal

$$A = \langle a, p \rangle = \{ra + sp : r, s \in R\}.$$

Since R is a PID, $A = \langle d \rangle$ for some $d \in R$. Since $p \in A$ we have $d \mid p$, but as p is prime hence irreducible, $d \sim 1$ or $d \sim p$. Notice if $d \sim p$ then $\langle p \rangle = \langle d \rangle = A$ where $a \in A$, so then $p \mid a$, a contradiction.

Thus we have $d \sim 1$, so $A = \langle d \rangle = \langle 1 \rangle = R$. Hence $1 = ba + cp$ for some $b, c \in R$, giving

$$\begin{aligned}(a + \langle p \rangle)(b + \langle p \rangle) &= ab + \langle p \rangle \\ &= (1 - cp) + \langle p \rangle \\ &= 1 + \langle p \rangle.\end{aligned}$$

Therefore $(a + \langle p \rangle)^{-1}$ exists, so $R/\langle p \rangle$ is a field.

($2 \implies 3$) Every field is an integral domain.

($3 \implies 1$) Suppose $p \mid ab \in R$. Then

$$(a + \langle p \rangle)(b + \langle p \rangle) = ab + \langle p \rangle = 0 + \langle p \rangle$$

because $p \mid ab \implies ab \in \langle p \rangle$. Since $R/\langle p \rangle$ is an integral domain, one of $a + \langle p \rangle, b + \langle p \rangle$ is $0 + \langle p \rangle$, so one of $a, b \in \langle p \rangle$ i.e. $p \mid a$ or $p \mid b$, so p is prime.

⬠

Remark: The proofs for $(2) \implies (3)$ and $(3) \implies (1)$ work for integral domains, only $(1) \implies (2)$ leverages that R is a PID.

Note: We have the following relations between algebraic structures:

$$\begin{array}{ccccccccccccc} \text{Field} & \subsetneq & \text{PID} & \subseteq & \text{UFD} & \subsetneq & \text{ACCP} & \subsetneq & \text{ID} & \subsetneq & \text{Comm Ring} & \subsetneq & \text{Ring} \\ \mathbb{Q} & & \mathbb{Z} & & \mathbb{Z}[x] & & \mathbb{Z}\left[\sqrt{-5}\right] & & A & & \mathbb{Z}_n & & M_n(\mathbb{R}). \end{array}$$

where $A = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$.

We don't yet know if the PID $\subseteq$ UFD containment is proper, but we will show $\mathbb{Z}[x]$ is a UFD eventually.

Remark: Theorem 2.10 fails for UFDs. Consider $\langle x \rangle \in \mathbb{Z}[x]$, then $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ which is an integral domain but not a field, i.e. $\langle x \rangle$ is a prime ideal but not a maximal ideal.

In a PID, non-zero proper ideals are prime iff they are maximal. In general, only maximal implies prime.

In a UFD, non-zero non-units are prime iff they are irreducible. In general, only prime implies irreducible.

2.5 Polynomials

Consider $2x + 4$, which is irreducible in $\mathbb{Q}[x]$, but factors as $2(x + 4)$ in $\mathbb{Z}[x]$ where 2 is not a unit, so it is reducible in $\mathbb{Z}[x]$. This motivates the following definition:

Definition (Content, primitive): If R is a UFD and $0 \neq f(x) \in R[x]$, a greatest common divisor of all coefficients of f is called a **content** of f, denoted $c(f)$. If $c(f) \sim 1$, we say f is a **primitive** polynomial.

Example: In $\mathbb{Z}[x]$, $c(6 + 10x^2 + 15x^3) \sim \gcd(6, 10, 15) \sim 1$ so this is primitive. However, $c(6 + 9x^2 + 15x^3) \sim \gcd(6, 9, 15) \sim 3$, so this is not primitive.

Lemma 2.11: Let R be a UFD and $0 \neq f(x) \in \mathbb{R}[x]$.
- $f(x)$ can be written as $f(x) = c(f)f_1(x)$ for some primitive $f_1(x) \in \mathbb{R}[x]$
- if $0 \neq b \in R$, then $c(bf) \sim bc(f)$.

Proof: Let $f(x) = a_m x^m + \dots + a_0$. Let $c(f) \sim \gcd(a_m, \dots, a_0)$ and write $a_i = c(f)b_i$ for all i, so

$$f(x) = c(f)f_1(x), \text{where } f_1(x) = b_m x^m + \dots + b_0.$$

We show f_1 is primitive. Indeed,

$$c(f) \sim \gcd(a_m, \dots, a_0) \sim \gcd(c(f)b_m, \dots, c(f)b_0) \sim c(f) \gcd(b_m, \dots, b_0).$$

Hence $1 \sim \gcd(b_m, \dots, b_0) \iff c(f_1) \sim 1$, so f_1 is primitive. Furthermore, the coefficients of bf for $b \neq 0$ are $ba_m, \dots, ba_0$, so

$$c(bf) \sim \gcd(ba_m, \dots, ba_0) \sim b \gcd(a_m, \dots, a_0) \sim bc(f).$$

Thus $c(bf) \sim bc(f)$. ⬠

Lemma 2.12: Let R be a UFD and $\ell(x) \in R[x]$ be irreducible with $\deg(\ell) \geq 1$. Then $c(\ell) \sim 1$.

Proof: Write $\ell(x) = c(\ell)\ell_1(x)$ with ℓ_1 primitive and $\deg(\ell_1) = \deg(\ell) = 1$. Since ℓ is irreducible one of $c(\ell), \ell_1$ must be a unit but clearly ℓ_1 cannot be, so $c(\ell) \sim 1$. ⬠

Theorem 2.13 (Gauss' Lemma): Let R be a UFD. If $f, g \neq 0 \in R[x]$ then $c(fg) \sim c(f)c(g)$. In particular, the product of primitive polynomials is again primitive.

Proof: Let $f = c(f)f_1$ and $g = c(g)g_1$ with f_1, g_1 primitive. Then

$$c(fg) \sim c(c(f)f_1 c(g)g_1) \sim c(f)c(g)c(f_1 g_1).$$

It suffices then to prove a product of primitives is primitive. Suppose bwoc f, g are primitive but fg is not. Write

$$\begin{aligned} f(x) &= a_0 + \dots + a_m x^m \\ g(x) &= b_0 + \dots + b_n x^n. \end{aligned}$$

Since R is a UFD, there is a prime p dividing each coefficient of fg. Since f, g are primitive, there is some k, s so $p \nmid a_k, b_s$. Let k and s be the minimum such values. Then
- $p \nmid a_k$ but $p \mid a_i$ for $i = 0, \dots, k - 1$
- $p \nmid b_s$ but $p \mid b_j$ for $j = 0, \dots, s - 1$

Now the coefficient c_{k+s} of x^{k+s} in fg is

$$\begin{aligned} c_{k+s} &= \sum_{i+j=k+s} a_i b_j \\ &= a_0 b_{k+s} + \dots + a_{k-1}b_{s+1} + a_k b_s + a_{k+1}b_{s-1} + \dots + a_{k+s}b_0. \end{aligned}$$

By the above, p divides every term on the left of $a_k b_s$ and every term on the right of it. However, it does not divide $a_k b_s$, hence cannot divide the sum, i.e. $p \nmid c_{k+s}$, a contradiction. Thus fg is primitive. ⬠

Theorem 2.14: Let R be a UFD whose field of fractions F is

$$F = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}.$$

Regard R as a subring of F. If $\ell(x) \in R[x]$ is irreducible in $R[x]$, then $\ell(x)$ is irreducible in $F[x]$.

Proof: Let $\ell(x) \in R[x]$ be irreducible. Suppose $\ell(x) = g(x)h(x) \in F[x]$. If a, b are the products of the denominators of the coefficients of $g(x)$ and $h(x)$, then $g_1(x) = ag(x) \in R[x]$ and $h_1(x) = bh(x) \in R[x]$. Notice that $ab\ell(x) = g_1(x)h_1(x)$ is a factorization in $R[x]$. Since $\ell(x)$ is irreducible, $c(\ell) \sim 1$. Also, by Gauss' lemma, we have

$$ab \sim abc(\ell) \sim c(ab\ell) \sim c(g_1 h_1) \sim c(g_1)c(h_1). \quad (\star)$$

Now, write $g_1(x) = c(g_1)g_2(x)$ and $h_1(x) = c(h_1)h_2(x)$ where $g_2(x), h_2(x)$ are primitive in $R[x]$. Then

$$ab\ell(x) = g_1(x)h_1(x) = c(g_1)c(h_1)g_2(x)h_2(x).$$

By $(\star)$ we have $\ell(x) \sim g_2(x)h_2(x)$ in $R[x]$. Since $\ell(x)$ is irreducible, it follows that $h_2(x) \sim 1$ or $g_2(x) \sim 1$.

If $g_2(x) \sim 1$, then $ag(x) = g_1(x) = c(g_1)g_2(x)$. Thus $g(x) = a^{-1}c(g_1)g_2(x)$ with $g_2(x) \sim 1$ is a unit in $F[x]$. Similarly if $h_2(x) \sim 1$, we can show $h(x)$ is a unit in $F[x]$. Thus $\ell(x) = g(x)h(x)$ in $F[x]$ implies that either $g(x)$ or $h(x)$ is a unit in $F[x]$, so $\ell(x)$ is irreducible in $F[x]$. ⬠

Recall the converse is false: $2x + 4$ is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{Z}[x]$. What's notable about this example is the content of $2x + 4$ is not a unit. One might wonder if this is the only such restriction preventing an iff statement. Indeed it is.

Proposition 2.15: Let F be a UFD whose field of fractions is F. Let $f(x) \in R[x]$ with $\deg(x) \geq 1$. TFAE:

(1) $f(x)$ is irreducible in $R[x]$.

(2) $f(x)$ is primitive and irreducible in $F[x]$.

Proof:

($1 \Longrightarrow 2$) Follows from Lemma 2.12 and Theorem 2.14.

($2 \Longrightarrow 1$) Suppose $f(x)$ is primitive and irreducible in $F[x]$ but reducible in $R[x]$. Then a nontrivial factorization of $f(x)$ in $R[x]$ must be of the form $f(x) = dg(x)$ with $d \in R$ and $d \nsim 1$ (if both factors have degree ≥ 1, then it would be a nontrivial factorization in $F[x]$). Since $d \mid f(x)$, $d \nsim 1$ divides each coefficient of $f(x)$, contradicting the fact that $f(x)$ is primitive. Thus $f(x)$ is irreducible in $R[x]$.

⬠

Notice that primitive guarantees irreducibility in $R[x]$ iff $F[x]$. Only the $R[x] \Longrightarrow F[x]$ direction holds for general polynomials.

Theorem 2.16: If R is a UFD, then so is $R[x]$.

Let R be a UFD and $x_1, ..., x_n$ be n commutative variables and define the ring $R[x_1, ..., x_n]$ of polynomials in n variables inductively by

$$R[x_1, ..., x_n] = (R[x_1, ..., x_{n-1}])[x_n].$$

Corollary 2.17: If R is a UFD, then for all $n \in \mathbb{Z}^+$, $R[x_1, ..., x_n]$ is a UFD.

Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[x]$ and $\mathbb{Z}[x_1, ..., x_n]$ are UFDs. With this, we can say that PID $\subsetneq$ UFD because $\mathbb{Z}[x]$ is a UFD but not a PID.

Theorem 2.18 (Eisenstein's criterion): Let R be a UFD with field of fractions F. Let $h(x) = c_n x^n + ... + c_1 x + c_0 \in R[x]$ with $n \geq 1$. Let $\ell \in R$ be irreducible. If:

- $\ell \nmid c_n$
- $\ell \mid c_i$ for all $i = 0, ..., n-1$
- $\ell^2 \nmid c_0$

Then h is irreducible in $F[x]$.

Proof: By contradiction. If $h(x)$ is reducible in $F[x]$, by Gauss' lemma there are $r(x), s(x) \in R[x]$ of degree at least 1 so $h(x) = s(x)r(x)$. Write

$$s(x) = a_0 + ... + a_m x^m$$
$$r(x) = b_0 + ... + b_k x^k.$$

where $1 \leq m, k < n$. Since $h(x) = s(x)r(x)$ we have

$$c_0 = a_0 b_0, ..., c_{k+s} = \sum_{i+j=k+s} a_i b_j.$$

Consider the constant term. Since $\ell \mid c_0$, we have $\ell \mid a_0 b_0$. Since ℓ is irreducible and R is a UFD, ℓ is prime, hence $\ell \mid a_0$ or $\ell \mid b_0$. Wlog, suppose $\ell \mid a_0$. Since $l^2 \nmid c_0$, we have $\ell \nmid b_0$.

If we consider the coefficient of x, since $\ell \mid c_1$ we have $\ell \mid (a_0 b_1 + a_1 b_0)$ where $\ell \mid a_0$ but $\ell \nmid b_0$, hence $\ell \mid a_1 b_0 \Longrightarrow \ell \mid a_1$.

By repeating the above argument, conditions on coefficients of $h(x)$ imply that $\ell \mid a_i$ for all $1 \leq \ell \leq m-1$. However, $\ell \nmid a_m$ since $\ell \nmid c_m$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{r}(x)) \in (R/\langle \ell \rangle)[x]$. By the assumption on the coefficients of h, we have $\overline{h}(x) = \overline{c_n} x^n$. However, since $\overline{s}(x) = \overline{a_m} x^m$ and $\ell \nmid b_0$, $\overline{s}(x)\overline{r}(x)$ contains the term $\overline{a_m b_0} x^m$, which is a contradiction. Thus $h(x)$ is irreducible in $F[x]$. ⬠

Example: Consider $2x^7 + 3x^4 + 6x^2 + 12$, where for $p = 3$ by Eisenstein's criterion this is irreducible in $\mathbb{Q}[x]$.

Example: Let p be prime and $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$ be a p^{th} root of unity. Now ζ_p is a root of the p^{th} cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$
$$= x^{p-1} + x^{p-2} + ... + x + 1.$$

Eisenstein's does not work directly here, but $\Phi_p(x+1)$ is irreducible iff $\Phi_p(x)$ is, so

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$$
$$= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + ... + \binom{p}{p-2} x + \binom{p}{p-1} \in \mathbb{Z}[x].$$

Then $p \mid \binom{p}{i}$ for $i = 1, ..., p-1$, but $p \nmid 1$ and $p^2 \nmid \binom{p}{p-1} = p$. Thus by Eisenstein's criterion $\Phi_p(x+1)$ is irreducible iff $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. Furthermore, observe $\Phi_p(x)$ is primitive, so by Proposition 2.15 it is irreducible in $\mathbb{Z}[x]$ as well.

3 Field Extensions

Definition (Field extension): If E is a field containing another field F, we say E is a **field extension** of F, denoted E/F.

Remark: E/F does *not* mean a quotient ring, as the only ideals are $\{0\}$ and E.

If E/F is a field extension, we can view E as a vector space over F with the obvious addition and scaling.

Definition (Degree): The dimension of E over F is called the **degree** of E over F, denoted $[E : F]$. If $[E : F] < \infty$ we say E/F is a finite extension, and otherwise it is an infinite extension.

Example: $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension.

Example: Let F be a field and let $F(x) = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in F[x], g(x) \neq 0\right\}$. Then $[F(x) : F]$ is an infinite extension since $\{1, x, x^2, ...\}$ is linearly independent over F.

Theorem 3.1 (Intermediate field extensions): If E/K and K/F are finite field extensions then E/F is a finite field extension with

$$[E : F] = [E : K][K : F].$$

In particular, if K is an intermediate field of a finite extension F, then $[K : F] \mid [E : F]$.

Proof: Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, ..., a_m\}$ and $\{b_1, ..., b_n\}$ be bases for E/K and K/F respectively. It suffices to show $\{a_i b_j\}$ is a basis for E/F.

For $e \in E$ we have

$$e = \sum_{i=1}^{m} k_i a_i$$

for some $k_i \in K$, and for each k_i we have

$$k_i = \sum_{j=1}^{n} c_{i,j} b_j$$

with each $c_{i,j} \in F$. Hence

$$e = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} b_j a_i \in \operatorname{Span}_F\{a_i b_j\}.$$

Next, we have

$$\sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j} a_i b_j = 0$$
$$\implies \sum_{i=1}^{m} a_i \sum_{j=1}^{n} c_{i,j} b_j = 0.$$

Since the a_i are LI in E/K with each sum term in K, by linearly independence of the a_i over K we have

$$\sum_{j=1}^{n} c_{i,j} b_j = 0$$

for each i. Then by the linear independence of the b_j over K/F, we have each $c_{i,j} = 0$, so the $\{a_i b_j\}$ are LI. ⬠

Definition (Algebraic, transcendental): Let E/F be a field extension and $\alpha \in E$. We say α is **algebraic over F** if there is $f(x) \in F[x] \setminus \{0\}$ such that $f(\alpha) = 0$. Otherwise, α is **transcendental over F**.

Example: $q \in \mathbb{Q}$ and $\sqrt{2}$ are algebraic over $\mathbb{Q}$, but e and π are transcendental over $\mathbb{Q}$.

Example: Claim: $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

$$\begin{aligned}\left(\alpha - \sqrt{2}\right)^2 &= 3 \\ \alpha^2 - 1 &= 2\sqrt{2}\alpha \\ \alpha^4 - 10\alpha^2 + 1 &= 0\end{aligned}$$

So α is a root of $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, so is algebraic over $\mathbb{Q}$.

Notation: Let E/F be a field extension and $\alpha \in E$. Then $F[\alpha]$ denotes the smallest subring of E containing F and α, and $F(\alpha)$ denotes the smallest subfield of E containing F and α. For $\alpha, \beta \in E$ we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.

Definition (Simple extension): If $E = F(\alpha)$ for some $\alpha \in E$, we say E is a **simple** extension of F.

We would like to know what $[F(\alpha) : F]$ is.

Definition (F-homomorphism): Let R, R_1 be two rings containing a field F. A ring hom $\varphi : R \to R_1$ is called an F-homomorphism if $\varphi|_F = \mathrm{id}$.

Theorem 3.2: Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F, then $F[\alpha] \cong F[x]$ and $F(\alpha) \cong F(x)$. In particular, $F[\alpha] \neq F(\alpha)$.

Proof: Define $\psi : F(x) \to F(\alpha)$ as the unique F-hom mapping $x \mapsto \alpha$. Then for $f(x), g(x) \in F[x]$ with $g(x) \neq 0$,

$$\psi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)}.$$

Notice this is well-defined as α is transcendental, so $g(\alpha) \neq 0$. Now $\operatorname{Ker} \psi$ is an ideal of $F(x)$, so ψ is injective as $x \notin \operatorname{Ker}(\psi)$. Also, since $F(x)$ is a field, $\operatorname{Im}(\psi)$ contains a field generated by F and α, so $F(\alpha) \subseteq \operatorname{Im}(\psi)$. Thus $F(\alpha) = \operatorname{Im}(\psi)$ and by the first isomorphism theorem, $F(x)/\operatorname{Ker}(\psi) \cong F(x) \cong \operatorname{Im}(\psi) = F(\alpha)$. As $F[x]$ and $F[\alpha]$ are subrings of these fields, they too are isomorphic. ⬠

Theorem 3.3: Let E/F be a field extension with $\alpha \in E$. If α is algebraic over F, there is a unique monic irreducible $p(x) \in F[x]$, called the **minimal polynomial of α over F**, such that there is an F-isomorphism $\varphi : F[x]/\langle p(x) \rangle \to F[\alpha]$ with $\varphi(x) = \alpha$ from which we conclude $F[\alpha] = F(\alpha)$.

Remark: Since α is algebraic, the map in the proof of Theorem 3.2 is not well-defined.

Proof: Consider the unique F-homomorphism $\varphi : F[x] \to F[\alpha]$ sending $x \mapsto \alpha$. Since $F[x]$ is a ring, $\operatorname{Im}(\varphi)$ is a ring containing F and α, so $F[\alpha] \subseteq \operatorname{Im}(\varphi)$ gives $\operatorname{Im}(\varphi) = F[\alpha]$.

Let $I = \operatorname{Ker}(\varphi) = \{f(x) \in F[x] : f(\alpha) = 0\}$. Since α is algebraic, $I \neq \{0\}$, where I is an ideal of $F[x]$. Since $F[x]/I \cong \operatorname{Im} \varphi = F[\alpha]$ is an integral domain, I is a prime ideal. As $F[x]$ is a PID, there is a unique monic irreducible $p(x)$ so that $I = \langle p(x) \rangle$. Since I is a prime ideal and therefore a maximal ideal, $F[x]/\langle p(x) \rangle$ is a field by Theorem 2.10.

Then, $F[x]/\langle p(x) \rangle \cong F[\alpha]$ is a field containing F and α, so $F(\alpha) \subseteq F[\alpha]$. The reverse containment is obvious, so $F[\alpha] = F(\alpha)$. ⬠

Remark: If $p(x)$ is the minimal polynomial of α over F, we have $\langle p(x) \rangle = \{f(x) \in F[x] : f(\alpha) = 0\}$. In particular, if $f(x) \in F[x]$ satisfies $f(\alpha) = 0$, then $p(x) \mid f(x)$.

As a direct consequence of these theorems, we have the following result:

Theorem 3.4 (Degree of a simple extension): Let E/F be a field extension, $\alpha \in E$.

(1) α is transcendental over F iff $[F(\alpha) : F]$ is infinite.

(2) α is algebraic over F iff $[F(\alpha) : F]$ is finite. Moreover, if $p(x)$ is the minimal polynomial of α over F, $[F(\alpha) : F] = \deg(p)$ and $\left\{1, \alpha, \alpha^2, ..., \alpha^{\deg(p)-1}\right\}$ is a basis for $F(\alpha)/F$.

Proof:

TODO: The backwards directions?

(1) $(\Longrightarrow)$ By Theorem 3.2 we have $F(x) \cong F(\alpha)$. In $F(x)$, the elements $\{1, x, x^2, ...\}$ are linearly independent over F, so $[F(\alpha) : F] = \infty$.

(2) $(\Longrightarrow)$ By Theorem 3.3, $F(\alpha) \cong F[x]/\langle p(x)\rangle$. Note that

$$F[x]/\langle p(x)\rangle = \{r(x) \in F[x] : \deg(r) < \deg(p)\}$$

so $\left\{1, x, x^2, ..., x^{\deg(p)-1}\right\}$ is a basis of $F[x]/\langle p(x)\rangle$.

⬠

Example: Let p be a prime and $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$ be a root of $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + ... + x + 1$. By Theorem 3.4, $\Phi_p(x)$ is the minimal polynomial of ζ_p. Thus $\left[\mathbb{Q}\left(\zeta_p\right) : \mathbb{Q}\right] = p - 1$.

Example: $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic, as a root of $x^4 - 10x^2 + 1$. We would like to show that this is the minimal polynomial of α over $\mathbb{Q}$ by showing $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Notice

$$\left(\alpha - \sqrt{2}\right)^2 = \sqrt{3}^2 \Longrightarrow \sqrt{2} = \frac{\alpha^2 - 1}{2\alpha},$$

so $\sqrt{2} \in \mathbb{Q}(\alpha)$. We have the following diagram:

$$\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}\left(\sqrt{2}\right) \\ | \\ \mathbb{Q} \end{array}$$

Since $\sqrt{2}$ is a root of $x^2 - 2$, which is irreducible, we have $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$. Also, $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$, giving $\left[\mathbb{Q}(\alpha) : \mathbb{Q}\left(\sqrt{2}\right)\right] \geq 2$. Since $\alpha \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}\left(\sqrt{2}\right)$, it follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 4$. However, α is a root of a degree 4 polynomial, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$, so we have equality, and thus $x^4 - 10x^2 + 1$ is the minimal polynomial of α over $\mathbb{Q}$.

It turns out that to understand finite field extensions, it suffices to understand simple ones.

Theorem 3.5: Let E/F be a field extension. If $[E : F] < \infty$, there exist $a_1, ..., a_n \in E$ such that

$$F \subsetneq F(\alpha_1) \subsetneq ... \subsetneq F(\alpha_1, ..., \alpha_n) = E.$$

Proof: By induction on $[E : F]$. If $[E : F] = 1$, then $E = F$ and we are done. Suppose $[E : F] > 1$ and the statement holds for all field extensions E_1/F_1 with $[E_1 : F_1] < [E : F]$. Let $\alpha_1 \in E \setminus F$ so by Theorem 3.1 we have

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F].$$

Since $[F(\alpha_1) : F] > 1$, we have $[E : F(\alpha_1)] < [E : F]$ so by the IH, there are $a_2, ..., a_n \in E$ such that

$$F(\alpha_1) \subsetneq F(a_1, \alpha_2) \subsetneq ... \subsetneq F(\alpha_1, \alpha_2, ..., \alpha_n) = E.$$

Therefore placing $F \subsetneq F(\alpha_1)$ at the start of this chain gives the desired result. ⬠

Definition (Algebraic field extension): A field extension E/F is **algebraic** if every $\alpha \in E$ is algebraic over F. Otherwise, it is **transcendental**.

Theorem 3.6: Let E/F be a field extension. If $[E : F] < \infty$, then E/F is algebraic.

Proof: Suppose $[E : F] = n$. For $\alpha \in E$, the elements $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ are not linearly independent over F, so there exist $c_i \in F$ not all zero such that

$$\sum_{i=0}^{n} c_i \alpha^i = 0$$

i.e. that α is a root of $c_0 + ... + c_n x^n \in F[x]$, so α is algebraic over F. ⬠

Theorem 3.7 (Algebraic closure): Let E/F be a field extension. Define

$$L := \{\alpha \in E : [F(\alpha) : F] < \infty\}.$$

Then L, called the **algebraic closure of F in E**, is an intermediate field of E/F.

Proof: Certainly $F \subseteq L$, so if $\alpha, \beta \in L$ we need to show $\alpha \pm \beta, \alpha\beta$, and $\frac{\alpha}{\beta}$ for $\beta \neq 0$ are all in L. By definition, $[F(\alpha) : F], [F(\beta) : F] < \infty$.

Consider the field $F(\alpha, \beta)$. Notice the minimal polynomial of α over F, say $p(x) \in F[x]$, is also an element of $F(\beta)[x]$ with $p(\alpha) = 0$. Therefore the minimal polynomial of α over $F(\beta)$ divides the minimal polynomial of α over F, so the former has at most the degree of the latter. It follows by Theorem 3.1 that

$$[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F]$$
$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] \leq [F(\alpha) : F][F(\beta)F] < \infty.$$

Now since $\alpha \pm \beta \in F(\alpha, \beta)$, we have $[F(\alpha + \beta) : F] \leq [F(\alpha, \beta) : F] < \infty$, so $\alpha \pm \beta \in L$. Similarly, we can show $\alpha\beta, \frac{\alpha}{\beta} \in L$, so L is a field. ⬠

Definition (Algebraically closed): A field F is **algebraically closed** if for any algebraic extension E/F, we have $E = F$.

Example: By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed. Moreover, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ in $\mathbb{C}$.

Example: Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, i.e.

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

For a prime p, since $\zeta_p \in \overline{\mathbb{Q}}$ as ζ_p is a root of its minimal polynomial $\Phi_p(x)$, we have

$$\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

As there are infinitely many primes, $\left[\overline{\mathbb{Q}} : \mathbb{Q}\right] = \infty$. In particular, this example shows that an algebraic extension need not be finite, i.e. the converse of Theorem 3.6 is false.

4 Splitting Fields

4.1 Existence

Definition (Splits over): Let E/F be a field extension. We say $f(x) \in F[x]$ **splits over E** if E contains all roots of $f(x)$, i.e. f can be written as a product of linear factors in $E[x]$.

Definition (Splitting field): Let $\tilde{E}/F$ be a field extension, $f(x) \in F[x]$, and $F \subseteq E \subseteq \tilde{E}$. If
- $f(x)$ splits over E and
- $f(x)$ does not split over any proper subfield of E

we say that E is a splitting field of $f(x)$ in $\tilde{E}$.

Theorem 4.1: Let $p(x) \in F[x]$ be irreducible. The quotient ring $F[x]/\langle p(x)\rangle$ is a field containing F and a root of $p(x)$.

Proof: Since $p(x)$ is irreducible, $I := \langle p(x)\rangle$ is a prime ideal. Since $F[x]$ is a PID, I is maximal iff $E := F[x]/I$ is a field. Consider the map

$$\begin{aligned} \varphi : F &\to E \\ a &\mapsto a + I. \end{aligned}$$

Since F is a field and $\varphi \neq 0$, φ is injective. Thus by identifying F with $\varphi(F)$, we view F as a subfield of E. We claim $\alpha := x + I$ is a root of $p(x)$. Write

$$\begin{aligned} p(x) &= a_0 + a_1 x + \ldots + a_n x^n \in F[x] \\ &= (a_0 + I) + (a_1 + I)x + \ldots + (a_n + I)x^n \in E[x]. \end{aligned}$$

We have

$$\begin{aligned} p(\alpha) &= a_0 + I + (a_1 + I)\alpha + \ldots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \ldots + (a_n + I)(x + I)^n \\ &= (a_0 + a_1 x + \ldots + a_n x^n) + I \\ &= p(x) + I = 0 + I = I. \end{aligned}$$

Thus $\alpha = x + I \in E$ is a root of $p(x)$. ⬠

Theorem 4.2 (Kronecker's theorem): Let $f(x) \in F[x]$. There exists a field E containing F such that $f(x)$ splits over E.

Proof: By induction on $\deg(f)$ with any field. If $\deg(f) = 1$, we let $E = F$ and are done. If $\deg(f) > 1$, write $f(x) = p(x)h(x)$ with $p(x)$ irreducible in $F[x]$. By Theorem 4.1, there is a field K with $F \subseteq K$ containing a root of $p(x)$, say α. Thus

$$\begin{aligned} p(x) &= (x - \alpha)q(x) \\ \implies f(x) &= (x - \alpha)q(x)h(x) \end{aligned}$$

where $q(x) \in K[x]$. Since $\deg(qh) < \deg(f)$, by induction there is a field E containing K over which $q(x)h(x)$ splits. It follows that $f(x)$ splits over E. ⬠

Theorem 4.3 (Splitting fields are finite extensions): Every $f(x) \in F[x]$ has a splitting field which is a finite extension of F.

Proof: For $f(x) \in F[x]$, by Theorem 4.2 there is a field extension E/F over which $f(x)$ splits. Say $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in E. Consider $L := F(\alpha_1, \ldots, \alpha_n)$, which is the smallest subfield of E containing all roots of $f(x)$, so $f(x)$ does not split over any proper subfield of L. Thus L/F is a splitting field of $f(x)$ in E. In addition, since the α_i are all algebraic in L, $[L : F]$ is finite. ⬠

Example: Consider $x^3 - 2 \in \mathbb{Q}[x]$. We know $x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}\zeta_3\right)\left(x - \sqrt[3]{2}\zeta_3^2\right)$ where $\zeta_3 = \exp\left(\frac{2\pi i}{3}\right)$. Hence the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\right) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3\right).$$

4.2 Uniqueness

Question: If we have two field extensions E/F and E_1/F, what is the relation between the splitting field of $f(x)$ in E and in E_1?

Definition (Homomorphism extension): Let $\varphi : R \to R_1$ be a ring homomorphism, and $\Phi : R[x] \to R_1[x]$ be the unique ring homomorphism satisfying $\Phi|_R = \varphi$ and $\Phi(x) = x$. We say Φ **extends** φ.

More generally, if $R \subseteq S$ and $R_1 \subseteq S_1$ are all rings and $\Phi : S \to S_1$ is a ring homomorphism with $\Phi|_R = \varphi$, we say Φ extends φ.

Theorem 4.4: Let $\varphi : F \to F_1$ be a field isomorphism and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ extend φ. Let $f_1(x) = \Phi(f(x))$ and $E/F, E_1/F_1$ be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there is an isomorphism $\psi : E \to E_1$ which extends φ.

Proof: By induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear factors in $F[x]$, and so is $f_1(x)$ in $F_1[x]$. Thus $E = F$, $E_1 = F_1$, so let $\psi = \varphi$ and we are done.

Suppose $[E : F] > 1$ and the statement holds for all $\tilde{E}/\tilde{F}$ with $\left[\tilde{E} : \tilde{F}\right] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) \geq 2$. Such a p exists, as otherwise all the irreducible factors of f are degree 1, giving $[E : F] = 1$. Define $p_1(x) := \Phi(p(x))$.

Let $\alpha \in E$ and $\alpha_1 \in E_1$ be roots of $p(x)$ and $p_1(x)$ respectively. From Theorem 3.3, we have the F and F_1-isomorphisms

$$\begin{aligned} F(\alpha) &\cong F[x]/\langle p(x)\rangle, \quad \alpha \mapsto x + \langle p(x)\rangle \\ F_1(\alpha_1) &\cong F_1[x]/\langle p_1(x)\rangle, \quad \alpha_1 \mapsto x + \langle p_1(x)\rangle. \end{aligned}$$

Consider the isomorphism $\Phi : F[x] \to F_1[x]$ extending φ. Since $p_1(x) = \Phi(p(x))$, there is a field isomorphism $\tilde{\Phi}$ given by

$$\begin{aligned} \tilde{\Phi} : F[x]/\langle p(x)\rangle &\to F_1[x]/\langle p_1(x)\rangle \\ x + \langle p(x)\rangle &\mapsto x + \langle p_1(x)\rangle \end{aligned}$$

which extends φ. It follows from the commutative diagram below that there exists a field isomorphism $\tilde{\varphi} : F(\alpha) \to F_1(\alpha_1), \alpha \mapsto \alpha_1$ extending φ.

$$\begin{tikzcd}
E \arrow[rrr, "\psi"] \arrow[dd, dash] & & & E_1 \arrow[dd, dash] \\
& F[x]/\langle p(x)\rangle \arrow[r, "\tilde{\Phi}"] & F_1[x]/\langle p_1(x)\rangle \arrow[dr, "\sim"] & \\
F(\alpha) \arrow[ur, "\sim"] \arrow[rrr, bend right=15, "\tilde{\varphi}"] \arrow[d, dash] & & & F_1(\alpha_1) \arrow[d, dash] \\
F \arrow[rrr, "\varphi"] & & & F_1
\end{tikzcd}$$

Notice since $\deg(p) \geq 2$, we have $[E : F(\alpha)] < [E : F]$. Since E (resp. E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ (resp. $f_1(x) \in F_1(\alpha_1)[x]$) over $F(\alpha)$ (resp. $F_1(\alpha_1)$), by induction there is an isomorphism $\psi : E \to E_1$ which extends $\tilde{\varphi}$. Therefore ψ extends φ. ⬠

Corollary 4.5 (Uniqueness of splitting fields): Any two splitting fields of $f(x) \in F[x]$ over F are isomorphic, and so we can say *the* splitting field of $f(x)$ over F.

Proof: Let $\varphi : F \to F$ be the identity map, and apply Theorem 4.4. ⬠

Theorem 4.6: Let F be a field, $f(x) \in F[x]$ with $\deg(f) = n \geq 1$. If E/F is the splitting field of $f(x)$, then $[E : F] \mid n!$.

Proof: By induction on $\deg(f)$. If $\deg(f) = 1$, choose $E = F$ and we have $[E : F] \mid 1!$. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$. Two cases:

Case 1. $f(x)$ is irreducible in $F[x]$. Let $\alpha \in E$ be a root of $f(x)$, and by Theorem 3.3

$$F(\alpha) \cong F[x]/\langle f(x)\rangle$$
$$\text{and } [F(\alpha) : F] = \deg(f) = n$$

since f is the minimal polynomial of α. Write $f(x) = (x - \alpha)g(x)$ with $g(x) \in F(\alpha)[x]$ and $\deg(g) \leq n - 1$. Since E is the splitting field of $g(x)$ over $F(\alpha)$, by induction $[E : F(\alpha)] \mid (n - 1)!$ which gives

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] = n \cdot [E : F(\alpha)] \Longrightarrow [E : F] \mid n!.$$

Case 2. $f(x)$ is reducible in $F[x]$. Write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ and $\deg(g) = m, \deg(h) = k$, $m + k = n$, and $1 \leq m, k < n$. Let K be the splitting field of $g(x)$ over F. Since $\deg(g) = m$, by induction $[K : F] \mid m!$. Since E is the splitting field of $h(x)$ over K, by induction $[E : K] \mid k!$. Therefore $[E : F] \mid m!k!$ which is a factor of $n!$ since $\binom{n}{m} = \frac{n!}{m!k!}$ is an integer.

Aside: E is the splitting field of $h(x)$ over K because E is the splitting field of $f(x)$ over F, so K contains the roots of f not present in h, so adjoining all the roots of h to K must produce E. This is true even if K already contains some (or all) of the roots of h. ⬠

5 More Field Theory

5.1 Prime fields

Definition (Prime field): The **prime field** of a field F is the intersection of all subfields of F.

Theorem 5.1: If F is a field, its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for a prime p.

Definition (Character): Given a field F, if its prime field is isomorphic to $\mathbb{Q}$ (resp. $\mathbb{Z}_p$), we say F has characteristic 0 (resp. p), denoted $\mathrm{ch}(F) = 0$ (resp. $\mathrm{ch}(F) = p$).

Remark: When $\mathrm{ch}(F) = p$, for $a, b \in F$,

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \dots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p \\ &= a^p + b^p\end{aligned}$$

since $p \mid \binom{p}{i}$ for each $i = 1, \dots, p-1$.

Proof of Theorem 5.1: Let F_1 be a subfield of F. Consider the map

$$\begin{aligned}\chi : \mathbb{Z} &\to F_1 \\ n &\mapsto n \cdot 1\end{aligned}$$

where $1 \in F_1 \subseteq F$. Let $I = \operatorname{Ker}\chi$. Since $\mathbb{Z}/I \cong \operatorname{Im}\chi$, a subring of F_1, $\mathbb{Z}/I$ is an integral domain. Thus I is a prime ideal.

- If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F_1$. Since F_1 is a field, $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) \subseteq F_1$.
- If $I = \langle p \rangle$ for a prime p, $\mathbb{Z}_p \cong \mathbb{Z}/\langle p \rangle \cong \operatorname{Im}\chi \subseteq F_1$. ⬠

Proposition 5.2: Let F be a field with $\mathrm{ch}(F) = p$ and $n \in \mathbb{N}$. Then $\varphi : F \to F, u \mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$ homorphism of fields. If F is finite, then φ is an isomorphism.

Proof:

TODO:

⬠

5.2 Formal derivatives and repeated roots

Definition (Formal derivative): If F is a field, the monomials $\{1, x, x^2, \dots\}$ form an F-basis for $F[x]$. Define the linear operator

$$\begin{aligned}D : F[x] \to F[x]1 &\mapsto 0 \\ x^i &\mapsto ix^{i-1}, \forall i \in \mathbb{N}.\end{aligned}$$

Notice that $D(f+g) = D(f) + D(g)$ and $D(fg) = D(f)g + fD(g)$. We call $D(f) =: f'$ the **formal derivative** of f.

Theorem 5.3: Let F be a field, $f(x) \in F[x]$.

(1) If $\mathrm{ch}(F) = 0$, then $f'(x) = 0 \Longleftrightarrow f(x) = c$ for some $c \in F$.

(2) If $\mathrm{ch}(F) = p$, then $f'(x) = 0 \Longleftrightarrow f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Proof:

(1) ($\Longleftarrow$) is clear. For ($\Longrightarrow$), say $f(x) = a_0 + \dots + a_n x^n$. Then

$$f'(x) = a_1 + 2a_2 x + \dots + na_n x^{n-1} = 0$$

implies that each $ia_i = 0$ for all $i = 1, ..., n$. Since $\mathrm{ch}(F) = 0$ we have $i \neq 0$, and so each $a_i = 0$. Therefore $f(x) = a_0$.

(2) ($\Longleftarrow$) Write $g(x) = b_0 + b_1 x + ... + b_m x^m \in F[x]$. Then

$$\begin{aligned} f(x) &= g(x^p) = b_0 + b_1 x^p + ... + b_m x^{pm} \\ \implies f'(x) &= b_1 p x^{p-1} + ... + b_m p m x^{pm-1}. \end{aligned}$$

Since $\mathrm{ch}(F) = p$, we have $p = 0$ so $f'(x) = 0$.

($\Longrightarrow$) For $f(x) = a_0 + ... + a_n x^n$,

$$f'(x) = a_1 + 2a_2 x + ... + n a_n x^{n-1} = 0$$

implies $ia_i = 0$. Since $\mathrm{ch}(F) = p$, $ia_i = 0$ gives $a_i = 0$ unless $p \mid i$. Thus

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + ... + a_{mp} x^{mp} = g(x^p)$$

where $g(x) = a_0 + a_p x + ... + a_{mp} x^m$. ⬠

Definition (Repeated root): Let E/F be a field extension, $f(x) \in F[x]$. We say $\alpha \in E$ is a **repeated root** of $f(x)$ if $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in E[x]$.

Theorem 5.4: Let E/F be a field extension, $f(x) \in F[x]$, $\alpha \in E$. Then α is a repeated root of $f(x)$ iff $x - \alpha$ divides both f and f', i.e. $(x - \alpha) \mid \gcd(f, f')$.

Proof: ($\Longrightarrow$) Suppose $f(x) = (x - \alpha)^2 g(x)$. Then

$$\begin{aligned} f'(x) &= 2(x - \alpha) g(x) + (x - \alpha)^2 g'(x) \\ &= (x - \alpha)[2g(x) + (x - \alpha) g'(x)], \end{aligned}$$

so $(x - \alpha) \mid f, f'$.

($\Longleftarrow$) Suppose $(x - \alpha) \mid f, f'$. Write $f(x) = (x - \alpha) h(x)$ with $h(x) \in E[x]$. Then

$$\begin{aligned} f'(x) &= h(x) + (x - \alpha) h'(x) \\ \implies h(\alpha) &= f'(\alpha) - (\alpha - \alpha) h'(\alpha) = 0, \end{aligned}$$

since $(x - \alpha) \mid f'$. So α is a root of h, giving $(x - \alpha) \mid h$, hence $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in E[x]$. ⬠

Definition (Separable): Let F be a field, $f(x) \in F[x] \setminus \{0\}$. We say $f(x)$ is **separable over F** if it has no repeated roots in any extension of F.

Example: $f(x) = (x - 4)(x - 9)$ is separable in $\mathbb{Q}[x]$.

Corollary 5.5: Let F be a field and $f(x) \in F[x]$. $f(x)$ is separable iff $\gcd(f, f') = 1$.

Remark: The condition of repeated roots depends on the extension of F while gcd involves only F.

Proof: Note $\gcd(f, f') \neq 1 \iff (x - \alpha) \mid \gcd(f, f')$ for some α in some extension of F. By Theorem 5.4, the result follows. ⬠

Corollary 5.6: If $\mathrm{ch}(F) = 0$, then every irreducible $r(x) \in F[x]$ is separable.

Proof: Let $r(x) \in F[x]$ be irreducible. Then

$$\gcd(r, r') = \begin{cases} 1 \text{ if } r' \neq 0 \\ r \text{ if } r' = 0 \end{cases}$$

If $r'(x) = 0$, then $r(x) = c$ for $c \in F$, but $\deg(r) \geq 1$ as r is irreducible, so we must have $\gcd(r, r') = 1$ and the result follows by Corollary 5.5. ⬠

Example: $\Phi_p(x) = 1 + x + \ldots + x^{p-1} = \frac{x^p - 1}{x-1}$ is irreducible, hence separable. Recall the roots of $\Phi_p(x)$ are $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ which are all distinct.

5.3 Finite fields

Given a field F, define $F^\times := F \setminus \{0\}$ (the group of units).

Proposition 5.7: If F is a finite field, then $\mathrm{ch}(F) = p$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof: Since F is finite, by Theorem 5.1 its prime field is $\mathbb{Z}_p$ for some prime p. Since F is a finite dimensional vector space over $\mathbb{Z}_p$, $F \cong \mathbb{Z}_p^n$ where $n = [F : \mathbb{Z}_p]$. Therefore $|F| = |\mathbb{Z}_p|^n = p^n$. ⬠

Theorem 5.8: Let F be a field and G finite subgroup of $F^\times$. Then G is cyclic. In particular, the group of units of a finite field is cyclic.

Proof: Wlog we assume $G \neq \{1\}$. Since G is a finite abelian group, by the classification of finite abelian groups

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_r}$$

where each $n_i \mid n_{i+1}$ and $n_i > 1$ since $G \neq \{1\}$. Notice every $g \in G$ must then satisfy $g^{n_r} = 1$, so is a root of $x^{n_r} - 1 \in F[x]$. Since $x^{n_r} - 1$ has at most n_r distinct roots in F, we have $|G| \leq n_r$, where the above isomorphism gives $|G| = n_1 \times n_2 \times \ldots \times n_r$, so it must be that $r = 1$ and $G \cong \mathbb{Z}_{n_1}$ is a cyclic group. ⬠

Corollary 5.9: If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$.

Proof: By taking $u \in F$ to be a generator of $F^\times$, we have $F = \mathbb{Z}_p(u)$. ⬠

Theorem 5.10: Let p be a prime and $n \in \mathbb{N}$.

(1) F is a finite field with $|F| = p^n$ iff F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

(2) Let F be a finite field with $|F| = p^n$, let $m \in \mathbb{N}$ with $m \mid n$. Then F contains a unique subfield K with $|K| = p^m$.

Proof:

(1) ($\Longrightarrow$) Suppose $|F| = p^n$. Then $|F^\times| = p^n - 1$, so every $u \in F^\times$ satisfies $u^{p^n - 1} = 1$, thus is a root of $f(x) := x(x^{p^n - 1} - 1) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Also, $0 \in F$ is a root of $f(x)$, so every element of F is a root of $f(x)$ which therefore has p^n distinct roots in F. Clearly $f(x)$ cannot split over any smaller field, so F must be the splitting field of $f(x)$ over $\mathbb{Z}_p$.

($\Longleftarrow$) Suppose F is the splitting field of $f(x) := x^{p^n} - x$ over $\mathbb{Z}_p$. Since $\mathrm{ch}(F) = p$, we have

$$f'(x) = p^n x^{p^n - 1} - 1 = -1.$$

Thus $\gcd(f, f') = 1$, so by Corollary 5.5 $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F and define

$$\begin{aligned} \varphi : F &\to F \\ u &\mapsto u^{p^n}. \end{aligned}$$

Notice $u \in F$ satisfies $u \in E$ iff $\varphi(u) = u$. This equality condition is closed under $+, -, \times, /$, and so E is a subfield of F of order p^n. Since F is a splitting field, it is generated over $\mathbb{Z}_p$ by the roots of $f(x)$ i.e. the elements of E, so $F = \mathbb{Z}_p(E) = E$, giving $|F| = p^n$.

(2) Let $\alpha \neq 0$ be a root of $x^{p^m} - x$, so α must be a root of $x^{p^m - 1} - 1$, giving $\alpha^{p^m - 1} = 1$ We recall

$$x^{ab} - 1 = (x^a - 1)\left(x^{ab-a} + x^{ab-2a} + \ldots + 1\right)$$

so as $m \mid n \Longleftrightarrow n = mk$ for $k \in \mathbb{Z}$, we have

$$p^n - 1 = p^{mk} - 1 = (p^m - 1)M$$

for some $M \in \mathbb{Z}$, and so

$$\alpha^{p^n - 1} = \alpha^{(p^m-1)M} = \left(\alpha^{p^m - 1}\right)^M = 1^M = 1.$$

Therefore α is a root of $x^{p^n-1} - 1$, and so every root of $x^{p^m} - x$ is a root of $x^{p^n} - x$. Since $x^{p^n} - x$ splits over F, so does $x^{p^m} - x$. Let

$$K := \left\{u \in F : u^{p^m} - u = 0\right\}.$$

Then $|K| = p^m$ since the roots of $x^{p^m} - x$ are distinct and by (1), K is a field. Now if $\tilde{K} \subseteq F$ is a subfield with $\left|\tilde{K}\right| = p^m$, then $\tilde{K} \subseteq K$, since all elements $v \in \tilde{K}$ satisfy $v^{p^m} - v = 0$. Therefore $\tilde{K} = K$, so K is unique.

⬠

Corollary 5.11 (E.H. Moore): Let p be a prime and $n \in \mathbb{N}$. Then any two finite fields of order p^n are isomorphic. We denote such a field by $\mathbb{F}_{p^n}$.