PMath 348

Jane Shi

Winter 2021

Schedule

- Field Theory
- Group Theory
- Galois Theory
- Applications

1 Ring theory

Definition (Radical): A radical is an expression involving only $+, -, \times, /, ^n\sqrt{}$

Note that linear quadratic, cubic (Cardano's formula) equations can be solvable by radicals. Same with quartic. How about quintic? Euler, Bezout, Langrage cant solve. Abel finally proved insolvability with Ruffini. We ask, given quintic, is it solvable radical? Reverse: Suppose radical solution exist, what does the quintic look like?
There are two main parts of galois theory. The first part is to link a root α, to the smallest field containing $\mathbb{Q}, \alpha$. The second is linking the field $\mathbb{Q}(a)$ to a group. We specifically associate the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ to the group. Galois theory turns infintie field questions into finite group problem.

1.1 Review for ring theory

Definition 1.1 (Commutative ring with 1): A commutative with 1 is a set R equipped with $+, \times$ such that

- R is an abelian group under $+$ with identity 0
- multiplication is commutative and associative. Also there exists $1 \in R$ such that $1r = r1 = r$ for all $r \in R$.
- For all r, s, t in R, $r(s + t) = rs + rt$. (distributive law)

In the following, we use the word **ring** to mean a commutative ring with 1.

Definition 1.2 (Field): A field F is a commutative ring with 1 such that every elements $a \in F \setminus \{0\}$ is a unit. (That is, $ab = 1$ for some $b \in F$.)

Definition 1.3 (Integral domain): A ring R is an integral domain if for $a, b \in R$, $ab = 0$ implies either $a = 0$ or $b = 0$.

For example, $\mathbb{Z}$ is an integral domain. The sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ are all fields.

Proposition 1.1:
Every subring of a field is an integral domain.

Definition 1.4 (Ideal): An ideal in a ring R is a subset I containing 0 such that for $a, b \in I$ and $r \in R$, $a - b \in I$ and $ra \in I$. (I.e. it "absorbs" all elements and differences are contained.) Note that an ideal is a subring.

Example: the only ideals of a field F are $\{0\}$ and F.

Definition 1.5 (PID- Principle Ideal Domain): An integral domain R is a PID if every ideal is generated by one element. **Note that it has to be an integral domain to begin with.**

In the following examples, we will list out common properties of $\mathbb{Z}$ and $\mathbb{F}[x]$ (set of polynomials in x over a field F.)
Example: $\mathbb{Z}$

- It is an integral domain and the units of $\mathbb{Z}$ are ± 1.
- Why is $\mathbb{Z}$ a PID? Using division algorithm in $\mathbb{Z}$, for $a, b \in \mathbb{Z}$ with $a \neq 0$, we can write $b = aq + r$ with $q, r \in \mathbb{Z}$, $0 \leq r < |a|$. So using the division algorithm in $\mathbb{Z}$, we are able to prove that an ideal I of $\mathbb{Z}$ is of the form $I = \langle n \rangle = n\mathbb{Z}$. If $n > 0$ then the generator n is unique. what if $n = 0, n < 0$?
- Consider all fields containing $\mathbb{Z}$. Their intersection (the smallest field containing $\mathbb{Z}$) is the set of rational numbers
$$\mathbb{Q} = \left\{ \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Example: Polynomials of x over a field F Let F be a field. We define

$$F[x] = \{ f(x) : a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m, a_1 \in F, (0 \leq i \leq m) \}$$

- If $a_m = 1$, we call $f(x)$ monic. If $a_m \neq 0$, the $deg(f)$ is equal to m. $deg(0) = -\infty$.
- for $f(x), g(x) \in F[x], deg(fg) = deg(f)deg(g)$. To preserve this degree formula, we define $deg(0) = \pm\infty$. why did we define it as $-\infty$ earlier? Why not $\pm\infty$ earlier?
- The set $F[x]$ is an integral domain and the units of $F[x]$ are $F^* = F \setminus \{0\}$.
- $F[x]$ is a PID: this can be shown using division algorithm. For $f(x), g(x) \in F[x]$, $f(x) \neq 0$, we can write $g(x) = q(x)f(x) + r(x)$, with $q, r \in F[x]$, $deg(r) < deg(f)$, we define $def(0) = -\infty$. Yes, in here you can only define it $-\infty$. Using this, we can prove that an ideal I of $F[x]$ is of the form $I = \langle f(x) \rangle = f(x)F[x]$. This shows that $F[x]$ is a pid. If $f(x)$ is monic, then the generator $f(x)$ is unique. why? why must generator be unique?

- Now, consider all the fields containing $F[x]$. Their intersection, which is the smallest field that contains $F[x]$, is the set of rational functions

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

Definition 1.6 (Quotient ring): The quotient ring of R modulo I, denoted by R/I, contains elements of the form $r + I, (r \in R)$. The addition and multiplication on R/I are defined by:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \text{ and } (r_1 + I) \times (r_2 + I) = r_1 r_2 + I$$

For example, for $n \in \mathbb{Z}$, we have

$$\mathbb{Z}/\langle n \rangle = \{r = r + \langle n \rangle, 0 \leq r < |n|\}$$

For $f(x) \in F[x]$, we have

$$F[x]/\langle f(x) \rangle = \{r(x) = r(x) + \langle f(x) \rangle, \deg(r) < \deg(f)\}$$

Theorem 1.2 (First isomorphism theorem):
Let $\phi : R \to S$ be a ring homomorphism. Then the kernel of ϕ is an ideal I. Furthermore, there is an isomorphism

$$R/I = R/ker(\phi) \to im\phi, r + I \mapsto \phi(r)$$

or equivalently,

- the kernel ϕ is an ideal of R.
- the image of ϕ is a subring of S.
- the image of ϕ is isomorphic to the quotient ring $R/\ker(\phi)$.

For example, let F be a field and S be a ring. Let $\phi : F \to S$ be a ring homomorphism. Since the only ideals of F are $\{0\}$ and F, either ϕ is injective or $\phi = 0$.

Definition 1.7 (Maximal ideal and prime ideal): An ideal I in R is maximal if there does not exist a ring J such that $I \subsetneq J \subsetneq R$. An ideal I in R is prime if $I \neq R$ and $ab \in I$ implies $a \in I$ or $b \in I$.

Proposition 1.3:
Every maximal ideal is prime. Moreover, in PID, every prime ideal is maximal. ooops, I forgot the proof.

Example: In $\mathbb{Z}$, $\langle n \rangle$ is maximal if and only if n is a prime. In $F[x]$, $\langle f(x) \rangle$ is maximal if and only if $f(x)$ is irreducible.
PLEASE fill in proof for all of those theorems or props.

Theorem 1.4:
Let I be an ideal of a ring R, and $R \neq I$. Then

- I is a maximal ideal if and only if R/I is a field.
- I is a prime ideal if and only if R/I is an integral domain.

1.2 Eisenstein's criterion

In this section, we apply Gauss's lemma to prove Eisenstein's criterion, which is needed in a later chapter.

Proposition 1.5 (Gauss' lemma for $\mathbb{Z}[x]$):
Let $f(x) \in \mathbb{Z}[x]$, with $\deg(f) \geq 1$. If $f(x)$ is irreducible in $\mathbb{Z}[x]$ then it is irreducible in $\mathbb{Q}[x]$.

Please fill in the proof for Gausses lemma.

Definition 1.8 (Irreducibility): Note that in integral domain D, a polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $g(x)h(x)$, with $g(x), h(x) \in D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$.

Remark: The converse of the above is not true. That is, if a function is irreducible in $\mathbb{Q}$, it is possibly reducible in $\mathbb{Z}$. (Whenever writing it as $a((2x/a)+(4/a))$ for some $a \in \mathbb{Q}$, a will be a unit in $\mathbb{Q}$, so irreducible). For example, the polynomial $2x+8$ is irreducible in $\mathbb{Q}$, but it is not irreducible in $\mathbb{Z}[x]$ because $2x+8 = 2(x+4)$ and both 2 and $x+4$ are non-units.

Theorem 1.6 (Eisenstein's criterion $\mathbb{Z}[x]$):
Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. Let $p \in \mathbb{Z}$ be prime. If $p \nmid a_n$, and $p \mid a_i$ for all $0 \leq i \leq n-1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof: Consider the map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ defined by:

$$f(x) \mapsto \overline{f}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \ldots + \overline{a_0} \pmod{p}$$

where $\overline{a_i} \in \mathbb{Z}_p$ with $\overline{a_i} = a_i \pmod{p}$ for $0 \leq i \leq n$. Since $p \nmid a_n$ and $p \mid a_i$ for all $0 \leq i \leq n-1$, we have $\overline{f}(x) = \overline{a_n}x^n$ with $\overline{a_n} \neq 0$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, by Gauss's lemma, it is reducible in $\mathbb{Z}[x]$. Let $f(x) = g(x)h(x)$ for $g(x).h(x) \in \mathbb{Z}[x]$ with $\deg g \geq 1, \deg h \geq 1$. It follows that $\overline{a_n}x^n = \overline{g}(x)\overline{h}(x)$. Since $\mathbb{Z}_p[x]$ is a UFD, WHY is it a UFD and why does it imply that?, we can see that $\overline{g}(x) = bx^m$ and $\overline{h}(x) = cx^k$ for some $b, c \in \mathbb{Z}_p$. This means that $\overline{g}(x), \overline{h}(x)$ both have the 0 constant in $\mathbb{Z}_p$. (that is, the constant term of those polynomial is 0.) This means the constant terms of both $\overline{g}(x), \overline{h}(x)$ are divisible by p, so $p^2 \mid a_0$. This is a contradiction. Therefore $f(x)$ is irreducible in $\mathbb{Q}[x]$.

□

Example 1.7:
For example, $2x^7 + 3x^4 + 6x^2 + 12$ is irreducible over $\mathbb{Q}[x]$ by applying eisentein's criterion for $p = 3$.

Example 1.8:
Let p be a prime. Let

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

be the pth root of 1. It is a root of the pth cyclotomic polynomial:

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

Eisenstein's criterion does not imply irreducibility of $\Phi_p(x)$ immediately. However, we can consider $\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x)}$

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

Since p is a prime, we know $p \nmid 1$ and $p \mid \binom{p}{i}$ for $1 \leq i \leq p-1$, and $p^2 \nmid \binom{p}{p-2}$. By Eisenstein's criterion for $\mathbb{Z}[x]$, we know that $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}[x]$. This implies that $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$. Since $\Phi_p(x)$ is primitive, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$. why does primitive & irreducible in $\mathbb{Q}[x]$ imply irreducible in $\mathbb{Z}[x]$?

why does primitive & irreducible in $\mathbb{Q}[x]$ imply irreducible in $\mathbb{Z}[x]$?
The above results can be generalized to unique factorization domains.

Proposition 1.9 (Gauss' Lemma for PID):
Let R be a principle ideal domain with the field of fractions (definition) F. Let $g(x) \in R[x]$ with $\deg(g) \geq 1$. If $g(x)$ is irreducible in $R[x]$, then it is irreducible in $F[x]$.

Let R be a principal ideal domain and $l \in R$ be irreducible. Then $R\langle l\rangle$ is a field and $R/\langle l\rangle[x]$ is a unique factorization domain.Not sure about this
Applying the same proof for the Eisenstein's criterion of $\mathbb{Z}[x]$, we obtain the following result:

Theorem 1.10 (Eisenstein's criterion for PID):
Let R be a principal ideal domain with the field of fractions F. Let $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in R[x]$ with $n \geq 1$. Let $\ell \in R$ be an irreducible element. If $\ell \nmid b_n$, $\ell \mid b_i$ for $0 \leq i \leq n-1$, and $\ell^2 \nmid b_0$, then the polynomial g is irreducible in $F[x]$.

Proposition 1.11 (Gauss' Lemma for UFD):
Let S be a UFD with the field of fractions E. Let $h(x) \in S[x]$ with $\deg(h) \geq 1$. If $h(x)$ is irreducible in $S[x]$ then it is irreducible in $E[x]$.

Theorem 1.12 (Eisenstein's Criterion for UFD):
Let S be a unique factorization domain with field of fractions E. Let $h(x) = c_n x^n + \ldots + c_1 x + c_0 \in S[x]$ with $n \geq 1$. Let $l \in S$ be an irerducible element. If $l \nmid c_n, l \mid c_i$ for all $0 \leq i \leq n-1$ and $l^2 \nmid c_0$, then $h(x)$ is irreducible in $E[x]$.

Proof: Prove by contradiction. If $h(x)$ is reducible in $E[x]$ then by Gauss' lemma for UFD, there exists $s(x), t(x) \in S[x]$ of degree ≥ 1 such that $h(x) = s(x)t(x)$. We write

$$s(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$$

$$t(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_k x^k$$

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

$$c_0 = a_0 b_0, c_1 = a_0 b_1 + a_1 b_0, c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots$$

Consider the constant term. Since $l \mid c_0$, we have $l \mid a_0 b_0$. Since l is irreducible, $l \mid a_0$ or $l \mid b_0$. WLOG say $l \mid a_0$. Since $l^2 \nmid c_0$, we have $l \nmid b_0$.
If we consider the coefficient of x, since $l \mid c_1$, we have $l \mid (a_0 b_1 + a_1 b_0)$. Since $l \mid a_0$, we have $l \mid a_1 b_0$. Since $l \nmid b_0$, we have $l \mid a_1$.
By repeating the above argument, the condition on coefficients of $h(x)$ imply that $l \mid a_i$ for all $0 \leq i \leq (m-1)$ and $l \nmid a_m$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{t}(x) \in S/\langle l \rangle[x]$. By the assumption on the coefficient of h, $\overline{h}(x) = \overline{c_n} x^n$. However, since $\overline{f}(x) = \overline{s}(x)\overline{t}(x) = \overline{a_m} x^m$ and $l \nmid b_0$, $\overline{s}(x)\overline{t}(x)$ contain the term $\overline{a_m b_0} x^m$, which leads to a contradiction (because the m term is supposedly having f as a factor). So $h(x)$ is not reducible in $E[x]$.

□

2 Field Extensions

2.1 Degree of Extensions

Definition 2.1 (Field extensions): If E is a field containing another field F, then E is a **field extension** of F, denoted by E/F.
We note that the notation E/F is **NOT** a quotient ring, because the field E does not have ideals other than $\{0\}$ and E. (Recall that all ideals of a field are either $\{0\}$ or itself.)

If E/F is a field extension we can view E as a vector space of F.

- addition: if $e_1, e_2 \in E$ then we set $e_1 + e_2 := e_1 + e_2$ (Addition of E)
- scalar multiplication: for $c \in F$, $e \in E$, $ce := ce$ (Multiplication of E)

Definition 2.2: The dimension of E over F (viewed as a vector space) is called the **degree** of E over F, denoted by $[E : F]$. If $[E : F] < \infty$, then we say that E/F is a **finite extension**. If $[E : F] = \infty$, we say E/F is an **infinite extension.** It is important to notice that, the finite/infinite just refers to the degree of the extension.

Example 2.1:
Examples: $[\mathbb{C}:\mathbb{R}] = 2$ is a finite field extension, since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$.

Example 2.2:
Let F be a field. Let

$$F[x] = \{f(x) : a_0 + a_1x + \ldots + a_nx^n \text{ where } a_0, a_1, \ldots, a_n \in F, n \in \mathbb{N} \cup \{0\}\}$$

Let

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

Note that $F[x]$, square bracket is polynomials, yet $F(x)$ is the rational functions (i.e. fractions whose denominator and numerators are $F(x)$, polynomials, with the denominator nonzero.)

Then $[F(x) : F]$ is ∞, an infinite field extension, since $\{1, x, x^2, \ldots\}$ are linearly independent over F. Is this a basis? What is a basis of $[F(x) : F]$?
Note that $F(x)$ is indeed a field! But $F[x]$ is **not a field**.

Theorem:
If E/K and K/F are finite field extensions, then E/F is a finite field extension and that

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

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

Proof:
Suppose that $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, a_2, \ldots a_m\}$ be a basis of E/K and $\{b_1, b_2, \ldots b_n\}$ be a basis of K/F.
Claim 1: every element of E is a linear combination of $\{a_ib_j\}$ over F. For $e \in E$, we have

$$e = \sum_{i=1}^{m} k_ia_i, \text{ where } k_i \in K$$

for $k_i \in K$ we have

$$k_i = \sum_{j=2}^{n} c_{i,j}b_k, \text{ where } c_{i,j} \in F$$

Thus

$$e = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{i,j}b_ja_i.$$

□

Claim 2: the set $\{a_ib_j, 1 \leq i \leq m, 1 \leq j \leq n\}$ is linearly independent over F.
This is because

suppose that

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{i,j} b_j a_i = 0 \text{ where } c_{i,j} \in F$$

Since $\sum_{j=1}^{n} c_{i,j} b_j \in K$ and $\{a_1, a_2, \ldots, a_m\}$ is independent over K, we have

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

Since $\{b_1, b_2, \ldots b_n\}$ is independent over F, we have $c_{i,j} = 0$. This implies that $\{a_i b_j, 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for E/F and we have

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

For example, $[\mathbb{C} : \mathbb{R}] = 2$. $\{1, i\}$ is a basis of $\mathbb{C}/\mathbb{R}$.

Algebraic and Transcendental extensions

Definition 2.3 (Algebraic vs Transcendental): Let E/F be a field extension and $\alpha \in E$ is **algebraic over** F is there exists $f(x) \in F[x] \setminus \{0\}$ such that $f(\alpha) = 0$. Otherwise we say that α **is transcendental over** F.

For example, $\frac{c}{d} \in \mathbb{Q}, \sqrt{2}, \sqrt{2} + \sqrt{-2}$ are algebraic over $\mathbb{Q}$, but e and π are transcendental over $\mathbb{Q}$.

Definition 2.4 ($F[\alpha]$, $F(\alpha)$): Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subring of E containing F and α. Let $F(\alpha)$ be the smallest subfield of E containing F and α. For $\alpha, \beta \in E$, we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.
This notion is similar to $F[x], F(x)$, where the earlier defines the polynomials where as the latter is $F(x)$, which is the radicals, it is a field.) So the latter $F(x)$ is very large compared to $F[x]$, and we can say that similarly $F(\alpha)$ is the smallest field that contains $F[\alpha]$.

Definition 2.5 (Simple extensions): If $E = F(\alpha)$ for some $\alpha \in E$, then we say that E is a *simple extension of* F.

The degree of the simple extension $F(\alpha)/F$ is either infinite or finite. In this section, we will show this depends on whether α is transcendental or algebraic.

Definition 2.6 (F homorphism): Let R and R_1 be two ring which both contains F. Then a ring homomorphism $\phi : R \to R_1$ is said to be a F homomorphism if $\phi\mid_F = 1_F$. That is, the homomorphism fixes every element in F.

Theorem 2.3 (Relationships between $F[\alpha], F[x], F(\alpha), F(x)$ for transcendental α):
Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F, then

$$F[\alpha] \simeq F[x], \text{ and } F(\alpha) \simeq F(x)$$

In particular, $F[\alpha] \neq F(\alpha)$.

Proof: Let $\phi : F(x) \to F(a)$ be the unique $F-$homomorphism defined by $\phi(x) = a$. Thusm for $f(x), g(x) \in F[x], g(x) \neq 0$, we have

$$\phi(f/g) = f(\alpha)/g(\alpha) \in F(\alpha)$$

Note that since α is transcendental, we have $g(\alpha) \neq 0$. So the map is well defined. Since $F(x)$ is a field and $\ker(\phi)$ is an ideal of $F(x)$, we know that $\ker(\phi) = F(x)$ or 0. Thus $\phi = 0$ or ϕ is injective.
Since $\phi(x) = \alpha \neq 0$, we know that ϕ is injective. Also, since $F(x)$ is a field, $im(\phi)$ contains a field generated by F and α. That is, $F(\alpha) \subseteq Im(\phi)$. Thus $Im(\phi) = F(\alpha)$ and ϕ is surjective. It follows that ϕ is an isomorphism and we have

$$F(\alpha) \simeq F(x), \text{ and } F[\alpha] \simeq F[x]$$

□

Theorem 2.4:
Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F, then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists a $F-$ isomorphism

$$\psi : F[x]/\langle p(x)\rangle \to F[\alpha], \ \psi(x) = \alpha$$

From which we conclude $F[\alpha] = F(\alpha)$.

Proof: We first notice that α is algebraic, then the map from the last theorem, $f/g \mapsto f(\alpha)/g(\alpha)$ is no longer well defined because denominator may be 0. Consider the unique F-homomorphism

$$\psi : F[x] \to F(\alpha)$$

defined by $\psi(x) = \alpha$. Thus, for $f(x) \in F[x]$, we have $\psi(f) = f(\alpha) \in F[\alpha]$. Since $F[x]$ is a ring, $im(\psi)$ contains a ring generated by F and α, that is $F[\alpha] \subseteq im(\psi)$. Therefore, $im(\psi) = F[\alpha]$.

Let

$$I = \ker\psi = \{f(x) \in F[x], \psi(f(x)) = f(\alpha) = 0\}$$

Since α is algebraic, $I \neq \{0\}$. We have $F[x]/I \simeq Im(\psi)$, a subring of a field $F(\alpha)$. Thus, $F[x]/I$ is an integral domain and I is a prime ideal. (since a subring of a field is always an integral domain, and the quotient ring of a ring by an ideal is ID iff the ideal is prime.) So it follows that $I = \langle p(x)\rangle$ where $p(x)$ is irreducible. (Since $F[x]$ is a PID, prime ideals are maximal. So $p(x)$ is a maximal ideal. This implies that $p(x)$ is irreducible.) If we assume that $p(x)$ is monic, then it is unique. It follows that

$$F[x]/\langle p(x)\rangle \simeq F[\alpha]$$

Since $p(x)$ is irreducible, $F[x]/\langle p(x)\rangle$ is a field (the ideal is maximal, and quotienting by maximal ideal yields a field). Thus $F[\alpha]$ is a field. Also, since $F(a)$ is the smallest field containing $F[\alpha]$ we have

$$F[\alpha] = F(\alpha)$$

This completes the proof.

□

Definition 2.7 (Minimal polynomial over F): If α is algebraic over a field F, the unique monic irreducible polynomial $p(x)$ in the previous theorem is called the minimal polynomial of α over F. From the proof of the above theorem, we see that if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$. (That is, $f(x) \in \langle p(x)\rangle$ hence must be some multiple of $p(x)$.)

As a direct result from the two above theorems, we obtain that

Theorem 2.5:
Let E/F be a field extension and $\alpha \in E$. Then

1. α is transcendental over F if and only if $[F(\alpha) : F]$ is ∞.
2. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.
3. Moreover, if $p(x)$ is the minimial polynomial of α over F, we have $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)/F$. (That is why we call $[F(\alpha) : F]$ the degree of a field extension.)

Proof: It suffices to prove the $\implies$ direction of 1 and 2, as the reverse direction is the contrapositive.

1. $\implies$. From the earlier theorem, if α is transcendental over F, then $F(\alpha) \simeq F(x)$. In $F(x)$, the elements $\{1, x, x^2, \dots\}$ are linearly independent over F. Thus $[F(\alpha) : F]$ is ∞.
2. From the other theorem, if α is algebraic over F, $F(\alpha) \simeq F[x]/\langle p(x)\rangle$, with $x \mapsto \alpha$. Note that

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

Is the above by division algo?

thus $\{1, x^2, \dots, x^{\deg(p)-1}\}$ forms a basis of $F[x]/\langle p(x)\rangle$. It follows that $[F(\alpha) : F] = \deg p$ and $\{1, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ forms a basis of $F(\alpha)$ over F.

□

Example: Let p be a prime. Let $\zeta_p = e^{2\pi i/p}$, a pth root of 1. We have seen in chapter 1 that ζ_p is a root of the pth cyclotomic polynomial $\Phi_p(x)$, which is irreducible. Thus, by the big theorem, $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$ and

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

The field $\mathbb{Q}(\zeta_p)$ is called the pth cyclotomic extension of $\mathbb{Q}$.

Theorem 2.6 (Changing a finite extension to chains of simple extensions): Let E/F be a field extension. If $[E:F]<\infty$, there exists $\alpha_1,\alpha_2,\dots\alpha_n \in E$ such that

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

Therefore, if we want to understand a finite extension, it suffices to understand a finite simple extension.

Proof:
We prove this theorem by induction on $[E:F]$. If $[E:F]=1$ then $E=F$, we are done. Suppose that $[F:F]>1$, and the statement holds for all field extensions $\tilde{E}/\tilde{F}$ with $[\tilde{E}:\tilde{F}]<[E:F]$.
Let $\alpha_1 \in E\setminus F$. By the theorem on degrees

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

Since $[E:F(\alpha_1)]>1$, we have $[E:F]>[F(\alpha_1):F]$. By induction hypothesis, there exists $\alpha_1,\alpha_2,\dots,\alpha_n$ such that

$$F(\alpha_1) \subsetneq F(\alpha_1)(\alpha_2) \subsetneq F(\alpha_1)(\alpha_2,\alpha_3) \subsetneq \dots \subsetneq F(\alpha_1)(\alpha_2,\dots\alpha_n)=E=F(\alpha_1,\alpha_2,\dots\alpha_n)$$

Hence we have

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

□

Definition 2.8 (Algebraic vs transcendental field extensions): A field extension E/F is algebraic if every $\alpha\in E$ is algebraic over F. Otherwise it is transcendental.

Theorem 2.7:
Let E/F be a field extension. If $[E:F]<\infty$, then E/F is algebraic over F.

Proof: The proof basically uses the maximality definition of linearly independence of a basis.
Suppose that $[E:F]=n$. For $\alpha\in E$, the elements $\{1,\alpha,\alpha^2,\dots\alpha^n\}$ are not linearly independent over F. So there exists $c_i\in F, 0\le i\le n$ not all 0 such that

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

Then α is a root of the polynomial $\sum_{i=0}^{n} c_i x^i \in F[x]$. So it is algebraic over F. □

Theorem 2.8 (Algebraic closure is a field):
Let E/F be a field extension. Define

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

Then L is an intermediate field of E/F.

Proof: If $\alpha, \beta \in L$, we need to show $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0) \in L$.
By definition of L, we have $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Now we consider the field $F(\alpha, \beta)$. Since the minimal polynomial of α over $F(\beta)$ divides the minimal polynomial of α over F. (the minimal polynomial of α over F, say $p(x) \in F[x]$, is also a polynomial over $F(\beta)$, i.e. $p(x) \in F(\beta)[x]$ such that $p(\alpha) = 0$. The min poly on F might be bigger because it is not equipped with β.), we have $[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F]$. (this is explained by the min poly over $F(\beta)$ is a factor of the min poly over F.) Combining this with the degree of extensions theorem,

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

Since $\alpha + \beta \in F(\alpha, \beta)$, $F(\alpha + \beta)$ is a subfield of $F(\alpha, \beta)$. it follows that

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

This says $\alpha + \beta \in L$. Similarly, $\alpha - \beta, \alpha\beta, \alpha/\beta(\beta \neq 0) \in L$. This shows that L is a field. □

Definition 2.9 (Algebraic closure): Let E/F be a field extension. The set

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

is called the algebraic closure of F in E. Recall the lattice? Is it the smallest field that contains all the algebraic numbers over F?

Definition 2.10 (Algebraically closed): A field F is algebraically closed if for any algebraic extension E/F, $E = F$. For example, $\mathbb{C}$ is algebraically closed but $\mathbb{R}$ is not.

Example: By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed, and $\mathbb{C}$ is the algebra closure of $\mathbb{R}$ in $\mathbb{C}$ and we have $[\mathbb{C} : \mathbb{R}] = 2$.
Example: Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. That is,

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

since $\zeta_p \in \overline{\mathbb{Q}}$, we have

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

since $p \to \infty$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. We have seen that that in a previous theorem, if E/F is finite, then E/F is algebraic, this example show that algebraic extensions does not need to be finite. It is an algebraic extension because everything in $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$. So the theorem: finite extension implies algebraic extension, its converse is not true.

Splitting Field

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 $f(x)$, that is, $f(x)$ is 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
- there is no proper subfield of E such that $f(x)$ splits over

Then we say that E is a **splitting field** of $f(x) \in F[x]$ in $\tilde{E}$. An intuition of this is that a splitting field is the smallest field extension such that the polynomial splits.

Existence of splitting fields

To show the existence of a splitting filed of $f(x)$, we first find a field extension of F which contains at least one root of $f(x)$.

Theorem (3.1.1):
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, the ideal $I = \langle p(x)\rangle$ is maximal. Thus $E = F[x]/I$ is a field. Consider the map

$$\psi : F \to E, a \mapsto a + I$$

Since F is a field and $\psi \neq 0$, ψ is injective. Thus, by identifying F with $\psi(F)$, and F can be viewed as a subfield of E.
Claim: Let $\alpha = x + I \in E$, then α is a root of $p(x)$.
Write

$$p(x) = a_0 + a_1x + \ldots + a_nx^n = (a_0 + I) + (a_1 + I)x + \ldots + (a_n + I)x^n \in E[x]$$

We have

$$\begin{aligned} p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + (a_2 + I)\alpha^2 + \ldots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + (a_2 + I)(x + I)^2 + \ldots + (a_n + I)(x + I)^n \\ &= (a_0 + a_1x + \ldots + a_nx^n) + I \text{ (since } ((x + I)^i = x^i + I(0 \leq i \leq n))) \\ &= p(x) + I = 0 + I = I \end{aligned}$$

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

□

Theorem (3.1.2. (Kronecker)):
Let $f(x) \in F[x]$. There exists a field E containing F such that $f(x)$ splits over E.

Proof: We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, then $E = F$ and we are done. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$. ($g(x)$ is not necessarily in $F[x]$.) We write $f(x) = p(x)h(x)$ where $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. (It is possible $h(x)$ has degree 0.)
By the theorem 3.1.1., (Using irreducible polynomial $p(x)$) there exists a field K such that $F \subseteq K$ and K containing a root of $p(x)$, say α. Thus

$$p(x) = (x - \alpha)q(x) \text{ and } f(x) = (x - \alpha)q(x)h(x)$$

where $q(x) \in K[x]$. We also see that all of $(x - \alpha)$,$h(x)$,$q(x) \in K[x]$.
Since $\deg(hq) < \deg(f)$, by induction, there exist a field E containing K over which $h(x)q(x)$ splits. Since $\alpha \in K$, we also have $(x - \alpha) \in E[x]$. So all the factors split in E. It then follows that $f(x)$ splits over E. □

Theorem (3.1.3):
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 3.1.2, there exists a field extension E/F such that $f(x)$ splits, say $\alpha_1, \ldots, \alpha_n$ are roots of $f(x)$ in E. Now, consider $F(\alpha_1, \ldots, \alpha_n)$. This is the smallest subfield of E containing all roots of $f(x)$. This $f(x)$ does not split over any proper subfield of it. This means that $F(\alpha_1, \ldots, \alpha_n)$ is the splitting field of $f(x)$ in E. (that is, if you make a strictly smaller subfield, it wont contain all the roots anymore, so it is indeed the splitting field). Also, since α_i are all algebraic, it means $F(\alpha_1, \ldots, \alpha_n)/F$ is finite.

□

Uniqueness of Splitting fields

We have seen from theorem 3.1.3 that for a fixed field extension E/F, a splitting field of $f(x) \in F[x]$ in E is of the form $F(\alpha_1, \ldots, \alpha_n)$ such that α_i are the roots of $f(x)$ in E. This means that the splitting field of $f(x)$ is unique within E. The question is: if we change E/F to a different field extension, for example E_q/F, what is the relation between the splitting field of $f(x)$ in E and the one in E_1?
What are some examples of having two field extensions E_1, E_2 of F, each has a different splitting field?

Definition (Extending the homomorphism): Let $\phi : R \to R_1$ be a ring homomorphism, and $\Phi : R[x] \to R_1[x]$ be the unique ring homomorphism satisfying $\Phi\mid_R = \phi$ and $\Phi(x) = x$. In this case, we say that Φ **extends** ϕ.

Basically it is the unique homomorphism of the polynomial rings that comes from the homomorphism of the rings.

More generally, if $R \subseteq S$, and $R_1 \subseteq S_1$, and $\Phi : S \to S_1$ is a ring homomorphism with $\Phi\mid_R = \phi$, we say Φ extends ϕ.

Theorem (3.2.1):
Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring homomorphism which extends ϕ. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.

Proof: We prove this theorem by induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear factors in $F[x]$, so is $f_1(x)$ in $F_1[x]$. Thus $E = F$ and $E_1 = F_1$. Take $\psi = \phi$ and we are done.

Now, suppose $[E : F] > 1$ and the statements is true for all field extension $\tilde{E}/\tilde{F}$ with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) \geq 2$, and let $p_1(x) = \Phi(p(x))$ (such $p(x)$ exists. Because if all irreducible factors of $f(x)$ are of degree 1. Then $[E : F] = 1$). Let $\alpha \in E$ and $\alpha_1 \in E_1$ be roots of $p(x)$ and $p_1(x)$ respectively. From theorem 2.2.2, we have an F isomorphism

$$F(\alpha) \simeq F[x]/\langle p(x)\rangle, \alpha \mapsto x + \langle p(x)\rangle$$

Similarly, there is an F_1 isomorphism

$$F_1(\alpha_1) \simeq F_1[x]/\langle p_1(x)\rangle, \alpha_1 \mapsto x + \langle p_1(x)\rangle$$

Now, consider the isomorphism $\Phi : F[x] \to F_1[x]$ which extends ϕ. Since $p_1(x) = \Phi(p(x))$, there exists a field isomorphism

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

which extends ϕ.
It follows there exists a field isomorphism

$$\tilde{\phi} : F(\alpha) \to F_1(\alpha_1), \alpha \mapsto \alpha_1$$

which extends ϕ.
Since $\deg(p) \geq 2$, $[E : F(\alpha)] < [E : F]$, 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 exists $\psi : E \to E_1$ which extends ϕ. Thus ψ also extends ϕ.

Basic idea is:
(found a set where the statements work in a smaller degree. That is, the F, F_1 being the $F(\alpha)$,$F_1(\alpha)$ resp, and with E, E_1 still being their splitting fields of polynomials in the polynomial rings of those respective fields, $F(\alpha)[x]$,$F_1(\alpha)[x]$ resp. So we apply induction with the setting where the extension is of smaller number.) □

Corollary (3.2.2.):
Any two splitting fields of $f(x) \in F[x]$ over F are $F-$isomorphic. Thus, we can now refer to “the” splitting field of $f(x)$ over F.

Proof: Let $\phi : F \to F$ be the identity map. Apply Theorem 3.2.1. □

Degree of Splitting fields

Theorem (3.3.1):
Let F be a field and let $f(x) \in F[x]$ with $\deg(f) = n \geq 1$. If E/F is the splitting field of $f(x)$, then $[E : F] \mid n!$

Proof: We prove this theorem by induction on $\deg(f)$. If $\deg(f) = 1$, then choose $E = F$ we have $[E : F] \mid 1!$. Suppose $\deg(f) > 1$, then the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ (though $g(x)$ is not necessarily in $F[x]$.) We have two cases:

1. Case I. If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$, then by theorem 2.2.2 :

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

   we write $f(x) = (x - \alpha)g(x) \in F(\alpha)[x]$ with $g(x) \in F(\alpha)[x]$. Since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n - 1$, by induction, $[E : F(\alpha)] \mid (n - 1)!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F] \mid n!$.

2. If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$ with $\deg(g) = m, \deg(h) = k$, $m + k = n$ 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 and $\deg(h) = k$, by induction, $[E : K] \mid k!$. This, $[E : F] \mid m!k!$, which is a factor of $n!$ (since $n!/m!k! = \binom{n}{m} \in \mathbb{Z}$.)

□

More Field Theory

This chapter, we introduce more field theory, our focus is to understand difference between fields of characteristic 0 and of characteristic p.

Prime Fields

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

Theorem (4.4.1.):
If F is a field, then its prime fields is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

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

$$\chi : \mathbb{Z} \to F_1, n \to n \cdot 1 \text{ where } 1 \in F_1 \subseteq F$$

Let $I = \ker \chi$ be the kernel of χ. Since $\mathbb{Z}/I \simeq im\chi$(by the first isomorphism theorem), a subring of F_1, it is an integral domain. Thus I is a prime ideal. Two cases:

- If $I = \langle 0\rangle$, then $\mathbb{Z} \subseteq F_1$. Since F_1 is a field

$$\mathbb{Q} = Frac(\mathbb{Z}) \subseteq F_1$$

- If $I = \langle p \rangle$, then by first isomorphism theorem
$$\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \cong im\chi \subseteq F_1$$

□

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

Note that if $ch(F) = p$ then, for $a, b \in F$,
$$(a+b)^p = a^p + b^p$$

Proposition (4.1.2):
Let F be a field with $ch(F) = p$, and let $n \in \mathbb{N}$. Then the map $\psi : F \to F$ given by $u \mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$ homomorphism of fields. If F is finite, then ψ is a $\mathbb{Z}_p$ isomorphism of F.

Formal Derivatives and Repeated Roots

Definition 2.11: If F is a field, then the monomials $\{1, x, x^2, \ldots\}$ form an F basis of $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^i) = ix^{i-1}, i \in \mathbb{N}$. Thus, for
$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, a_i \in F$$
we have
$$D(f)(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$$
Note that

- $D(f+g) = D(f) + D(g)$
- Leibniz Rule: $D(fg) = D(f) \cdot g + f \cdot D(g)$.

We call $D(f) = f'$ the **formal derivative** of f.

Theorem (4.2.1):
Let F be a field and $f(x) \in F[x]$.

1. If $ch(F) = 0$, then $f'(x) = 0$ if and only if $f(x) = c$ for some $c \in F$.
2. If $ch(F) = p$, then $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Proof:

1. $\Longleftarrow$ Is clear.

   $\Longrightarrow$ For $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1} = 0$ implies that

$ia_i = 0$ for $1 \leq i \leq n$. Since $ch(F) = 0$, we know $i \neq 0$. So $a_i = 0$ for $i \geq 1$. Thus, $f(x) = a_0 \in F$.

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

$$f(x) = g(x^p) = b_0 + b_1 x^p + b_2 x^{2p} + \ldots + b_m x^{pm}$$

Thus,

$$f'(x) = pb_1 x^{p-1} + 2pb_2 x^{2p-1} + \ldots + pmb_m x^{pm-1}$$

Since $Ch(F) = p$ we have $f'(x) = 0$.

$\Longrightarrow$ For $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, $f'(x) = a_1 + 2a_2 x + \ldots + na_n x^{n-1} = 0$ implies that $ia_i = 0$ for $1 \leq i \leq n$. Since $ch(F) = p, ia_i = 0$ implies $a_i = 0$ unless $p \mid i$. Therefore

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

where $g(x) = a_0 a_p x + a_{2p} x^2 + \ldots + a_{mp} x^m \in F[x]$.

□

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

Theorem (4.2.2.):
Let E/F be a field extension, $f(x) \in F[x]$ and $\alpha \in E$. Then α is a repeated root of $f(x)$ if and only if $(x - \alpha)$ divides both f and f', that is, $(x - a) \mid gcd(f, f')$.

Proof:

- $\Longrightarrow$ Suppose that $f(x) = (x - \alpha)^2 g(x)$, then

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$$

- $\Longleftarrow$ Suppose that $(x - \alpha)$ divides both f and f'. Write $f(x) = (x - \alpha)h(x), h(x) \in E[x]$. Then

$$f'(x) = h(x) + (x - \alpha)h'(x)$$

$f'(\alpha) = 0$ imiplies $h(\alpha) = 0$. Therefore $(x - \alpha)$ is a factor of $h(x)$ and $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in E[x]$.

□

Corollary (4.2.3):
Let F be a field and $f(x) \in F[x]$. Then $f(x)$ has no repeated root in any extension of F if and only if $\gcd(f, f') = 1$.

Remark: we notice that the condition of repeated roots depend on the extensions of F while the gcd condition involves only F. That is , $gcd(f, f') \neq 1$ if and only if $(x-\alpha) \mid gcd(f, f')$ for α in some extension of F. By theorem 4.2.2., this result follows.

Finite Fields.

Notation: Given a field F, let $F^* = F \setminus \{0\}$ be the multiplicative group of nonzero elements of F.

Proposition (4.3.1.):
If F is a finite field, then $ch(F) = p$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof: Since F is a finite filed, by theorem 4.1.1. its prime field is $\mathbb{Z}_p$. Since F is a finite dimensional vector space over $\mathbb{Z}_p$, we have $F \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$. hence $|F| = p^n$. □

Theorem (4.3.2.):
Let F be a field and G a finite subgroup of F^*. Then G is a cyclic group. In particular, if F is a finite field, then F^* is a cyclic group.

Proof: WLOG, we can assume that $G \neq \{1\}$. Since G is a finite abelian group,

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

where $n_1 > 1$ and $n_1 \leq n_2 \leq \ldots n_r$. Since $n_r(\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}) = 0$, it follows that every $u \in G$ is a root of $x^{n_r - x} \in F[x]$. Since the polynomial has at most n_r distinct roots in F, we have $r = 1$ and $G \cong \mathbb{Z}/n_r\mathbb{Z}$. □

Here: a little bit confused.
By taking u to be a generator of the multiplicative group of F^*, we have

Corollary (4.3.3.):
If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$, that is, $F = \mathbb{Z}_p(u)$ for some $u \in F$.

Theorem (4.3.4.):

1. If F is a finite field with $|F| = p^n$ if and only if F is a 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. $\Longrightarrow$: If $|F| = p^n$, then $|F^*| = p^n - 1$. Thus every $u \in F^*$ satisfies $u^{p^n-1} = 1$, and thus is a root of $x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Since $0 \in F$ is also a root of $x^{p^n} - x$, the polynomial x^{p^n-x} has p^n distinct roots in F. That is it splits over F. Thus F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.

   $\Longleftarrow$ Suppose that F is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. Since $ch(F) = p$, we have $f'(x) = -1$. Since $gcd(f, f') = 1$, by corollary 4.2.3., $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F. Let $\varphi : F \to F$ be given by $u \mapsto u^{p^n}$. For $u \in F$, u is a root of $f(x)$ if and only if $\varphi(u) = u$. Since the condition is closed under addition, subtraction, multiplication and division, the set E is a subfield of F of order p^n, which contains $\mathbb{Z}_p$. (Since all $u \in \mathbb{Z}_p$ satisfy $u^p = p$ and thus $u^{p^n} = u$). Since F is a splitting field, it is generated over $\mathbb{Z}_p$ by the roots of $f(x)$, that is, the elements of E. Thus $F = \mathbb{Z}_p(E) = E$.

2. We recall
   $$x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + \ldots + x^a + 1)$$
   If $n = mk$, then we would have
   $$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x^{p^m-1} - 1)g(x) = (x^{p^m-x})g(x)$$
   for some $g(x) \in \mathbb{Z}_p[x]$.

   Since $(x^{p^n} - x)$ splits over F, so does (x^{p^m-x}). Let
   $$K = \{u \in F : u^{p^m} - u = 0\}$$
   Then $|K| = p^m$ since roots of $x^{p^m} - x$ are distinct. Also, by (1), K is a field. Note that if $\tilde{K} \subseteq F$ be any field with $|\tilde{K}| = p^m$, then $\tilde{K} \subseteq K$ Why must this be a subfield. So $\tilde{K} = K$. Thus we see that a subfield K of F with $|K| = p^m$ is unique.

□

As a direct consequence of theorem 4.3.4. and corollary 3.2.2. we have

Corollary (4.3.5.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 it by $\mathbb{F}_{p^n}$.

Separable Polynomials

Definition (Separable over): Let F be a field and $f(x) \in F[x] \setminus \{0\}$. If $f(x)$ is irreducible, we say $f(x)$ is separable over F if it has no repeated root in any extension of F. In general, we say $f(x)$ is separable over F is each irreducible factor of $f(x)$ is separable over F.

Examples

- $f(x) = (x - 4)^9$ is separable in $\mathbb{Q}[x]$.
- Consider the polynomial $f(x) = x^n - a \in F[x]$ with $n \geq 2$.

  We recall corollary 4.2.3 which states that if $gcd(f, f') = 1$, then $f(x)$ has no repeated root in any extension of F, so $f(x)$ is separable.

If $a = 0$ the only irreducible factor of f is x. Since $gcd(x, x') = 1$, $f(x)$ is separable. Now we assume $a \neq 0$. Now $f'(x) = nx^{n-1}$. Thus the only irreducible factor of $f'(x)$ is x, provided that $n \neq 0$.

1. If $ch(F) = 0$, since $x \nmid f(x)$, we have $gcd(f, f') = 1$. Then $f(x)$ is separable.
2. If $ch(F) = p$, and $gcd(n, p) = 1$, since $x \nmid f(x)$, $gcd(f, f') = 1$. hence $f(x)$ is separable.
3. If $ch(F) = p$, consider $f(x) = x^p - a$. Since $f'(x) = px^{p-1} = 0$, we have $gcd(f, f') \neq 1$. However, it is still possible that all irreducible factors $l(x)$ of $f(x)$ has the property that $gcd(l, l') = 1$. To decide if $f(x)$ is separable, we need to find its irreducible factors first. Define

$$F^p = \{b^p, b \in F\} \text{ which is a subfield of } F$$

   (a) Case I: if $a \in F^p$, say $a = b^p$, for some $b \in F$, then

$$f(x) = x^p - b^p = (x - b)^p \in F[x]$$

   which is reducible. Since each irreducible factor of $f(x)$ is linear, it is separable. Thus $f(x)$ is separable.

   (b) Case II: Suppose that $a \notin F^p$.

   Claim: $f(x) = x^p - a$ is irreducible in $F[x]$.

   Write $x^p - a = g(x)h(x)$ where $g, h \in F[x]$ are monic polynomials. Let E/F be an extension where $x^p - a$ has a root, say $\beta \in E$. Note that since $a = \beta^p \notin F^p$, we have $\beta \notin F$. We have

$$x^p - a = x^p - \beta^p = (x - \beta)^p$$

   Thus, $g(x) = (x - \beta)^r$ and $h(x) = (x - \beta)^s$ for some $r, s, \in \mathbb{N} \cup \{0\}$. $r + s = p$. Write

$$g(x) = x^r - r\beta x^{r-1} + \dots$$

   Then $r\beta \in F$. Since $\beta \notin F$, as an element of F, we have $r = 0$. (If $r \neq 0$, then $r^{-1} \in F$ and $r^{-1}r\beta = \beta \in F$, a contradiction.) Thus as an integer, $r = 0$ or $r = p$, It follows either $g(x) = 1$ or $h(x) = 1$ in $F[x]$. Therefore $f(x)$ is irreducible.

   Since $f(x)$ is irreducible, and $f(x) = (x - \beta)^p \in E[x]$, it is not separable. In this case, since all roots of $f(x)$ are the same, we say $f(x)$ is purely inseparable.

   It is good you revisit the proof

Definition (Perfect): A field is perfect if every (irreducible) polynomial $r(x) \in F[x]$ is separable over F. What does the red in the bracket mean

Theorem (4.4.1.):
Let F be a field.

- If $ch(F) = 0$ then F is perfect.
- If $ch(F) = p$ and $F^p = F$ then F is perfect.

Proof:
Let $r(x) \in F[x]$ be irreducible. Then $gcd(r, r') = 1$ if $r' \neq 0$, (Why is the first implication true?) and

$gcd(r, r') \neq 1$ if $r' = 0$.
Suppose that $r(x)$ is not separable. Then by corollary 4.2.3., $gcd(r, r') \neq 1$. Thus $r'(x) = 0$.

- If $ch(F) = 0$, then from theorem 4.2.1.(1), $r'(x) = 0$ implies $r(x) = c \in F$. This is contradiction since $deg(r) \geq 1$. Thus $r(x)$ is separable and F is perfect.
- If $ch(F) = p$, then from theorem 4.2.1.(2), $r'(x) = 0$ implies that:

  $$r(x) = a_0 + a_1 x^p + a_2 x^{2p} + \ldots + a_m x^{mp}, a_i \in F$$

  Since $F = F^p$, we can write $a_i = b_i^p$ for $b_i \in F$. Thus

  $$r(x) = b_0^p + b_1^p x^p + b_2 p x^{2p} + \ldots + b_m^p x^{mp} = (b_0 + b_1 x + b_2 p x^2 + \ldots + b_m x^m)^p$$

  This is a contradiction since $r(x)$ is irreducible. Thus $r(x)$ is separable and F is perfect.

□

Remark: Let $ch(F) = p$ and $F^p \neq F$. (e.g.$F = F_p(x)$). If we take $a \in F \setminus F^p$, then the polynomial $x^p - a$ is purely inseparable. So if $ch(F) = p$, F is perfect if and only if $F^p = F$.

Corollary (4.4.2.):
Every finite field is separable.

Proof: Every finite field $F = \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ for some prime p and $n \in \mathbb{N}$. Thus for every $a \in F$,

$$a = a^{p^n} = (a^{p^{n-1}})^p$$

Since $a^{p^{n-1}} \in F, F = F^p$.

□

The Sylow Theorems

Review of Group Actions

In PM347, we saw the complete classifications of finite abelian groups. The Sylow theorems serve as a step towards understand arbitrary finite groups, not just the abelian ones.

Definition (Action): An action of a group G on a set S is a function $G \times S \to S, (g, x) \to gx$, such that for all $x \in S, g_1, g_2 \in G$, we have $ex = x$, and $g_1(g_2 x) = (g_1 g_2)x$.
If G acts on S, we denote the orbit of x as $G \cdot x = \{gx : g \in G\}$.
We denote the stabilizer of x as: $G_x = \{g \in G : gx = x\}$. The stabilizer is a subgroup of G, we have $|G \cdot x| = [G : G_x]$. Note that in here $[H : G] = |H|/|G|$ is the subgroup index.

Example

Let G be a group acting on itself by conjugation. $(g,x) = gxg^{-1}$. Then, for $x \in G$,

$$C_G(x) = G_x = \{g \in G : g \in G : gxg^{-1} = x\}$$

is the centralizer of x. That is $C_G(x)$ depends on the x. They are the group elements that fix x by applying above.
Let $Z(G)$ be the center of G, that is, $Z(G) = \{g \in G : gxg^{-1} = x, \forall x \in G\}$. The center is in $C_G(x)$ for every single x.
So, for $x \in G$, we have $|G \cdot x| = 1$ if and only if $G \cdot x = \{x\}$, if and only if $x \in Z(G)$. (so for $y \in G, yxy^{-1} = x \implies xy^{-1}x^{-1} = y^{-1}$, so the orbit only contains one element. So that x is in the center.) Therefore, we have the following class equations for G:

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $x_i \in G \setminus Z(G)$, the orbits $G \cdot x_i = \{gx_ig^{-1} : g \in G\}$ are distinct conjugacy classes of G and $|G \cdot x_i| = [G : C_G(x_i)] > 1$ for each i.
The above example is intersting, maybe review?

Lemma (5.1.1.):
Given a prime p, let G be a group of order p^n which acts on a finite set S. Let

$$S_0 = \{x \in S \mid gx = x, \forall g \in G\}$$

Then we have $|S| = |S_0| \pmod{p}$

Proof: For $x \in S$, $|G \cdot x| = 1$ if and only if $x \in S_0$. Thus S can be written as disjoint union

$$S = S_0 \cup G \cdot x_0 \cup \ldots \cup G \cdot x_m$$

with $|G \cdot x_i| > 1, \forall i$. Thus

$$|S| = |S_0| + |G \cdot x_1| + \ldots + G \cdot x_m$$

Since $|G \cdot x_i| > 1$, and $|G \cdot x_i| = [G : G_{x_i}]$ divides $|G| = p^n$, so $p \mid |G \cdot x_i|$ for all i. So $|S| = |S_0| \pmod{p}$.

□

Theorem (5.1.2 Cauchy):
Let p be a prime. Let G be a finite group. If $p \mid |G|$ then G contains an element of order p.

Proof: Define

$$S = \{(a_1, a_2 \ldots, a_p) : a_i \in G \text{ and } a_1a_2 \ldots a_p = e\}$$

Since a_p is uniquely determined by $a_1, a_2, \ldots, a_{p-1}$, if $|G| = n$, we have $|S| = n^{p-1}$. Since $p \mid n$, we have $|S| \equiv 0 \pmod{p}$. Let the group $\mathbb{Z}_p$ act on S by cyclic permutation. That is, for $k \in \mathbb{Z}_p$,

$$k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$$

One can verify that this action is well defined. Also $(a_1, a_2, \dots, a_p) \in S_0$ if and only if $a_1 = a_2 = \dots = a_p$. (That is because, all permutations fix them.) Clearly, $(e, e, \dots, e) \in S_0$ and hence $|S_0| \geq 1$. By lemma 5.1.1., we have $|S_0| \equiv |S| \equiv 0 \pmod p$. Since $|S_0| \geq 1$, $|S_0| \equiv 0 \pmod p$, we have $|S_0| \geq p$. Thus there exists $a \neq e$ such that $(a, a, \dots, a) \in S_0$. Which implies $a^p = e$. Since p is a prime, the order of a is p.

□

The Sylow Theorems

Definition (P group): Let p be a prime. A group in which every element has order of a non-negative power of p called p group.

Corollary (5.2.1):
As a corollary of 5.1.2..
A finite group G is a p group if and only if $|G|$ is a power of p.
I dont understand why this follows?
$\Longrightarrow$: Suppose that G is a p group. This means that every element has order of a nonnegative power of p. Now suppose towards contradiction that $|G|$ has a factor, prime, q, then by Cauchy's, there is an element with order q. Contradiction.
$\Longleftarrow$: If $|G|$ is a power of p, then note that the order of every element is a factor of $|G|$ (consider the cyclic group generated by the element and by Lagrange's theorem), so every element has order of power of p.

Lemma (5.2.2.):
The center $Z(G)$ of a non-trivial finite p group G contains more than one element.

Definition: Since G is a p group, by corollary 5.2.1., $|G|$ is a power of p. We recall the class equation of G:

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $[G : C_G(x_i)] > 1$. Since $|G|$ is a power of p, $[G : C_G(x_i)] \mid [G]$ ans $[G : C_G(x_i)] > 1$, we see that $p \mid [G : C_G(x_i)]$. It follows that $p \mid Z(G)$. Since $|Z(G)| \geq 1$, $Z(G)$ has at least p elements.
We recall that if H is a subgroup of a group G, then

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

is the normalizer of H in G. Particularly, $H \triangleleft N_G(H)$.

Lemma (Lemma 5.2.3.):
If H is a $p-$ subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod p$.

Proof: Let S be a set of all left cosets of H in G and let H act on S by left multiplication. Then $|S| = [G : H]$. For $x \in G$, we have

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hxH = H, \forall h \in H \\ &\iff x^{-1}Hx = H, \text{ this holds since above holds equality for all } h \in H \\ &\text{the above becomes } x^{-1}HxH = H \\ &\iff x \in N_G(H) \end{aligned}$$

Thus $|S_0|$ is the number of cosets xH with $x \in N_G(H)$, and hence $|S_0| = [N_G(H) : H]$.
By lemma 5.1.1.,

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod p$$

□

Corollary (5.2.4):
Let H be a $p-$ subgroup of a finite group G. If $p \mid [G : H]$, then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.

Proof: Since $p \mid [G : H]$, by Lemma 5.2.3., we have

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod p$$

Since $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. Thus $N_G(H) \neq H$.

□

Now we recall Cauchy's Theorem that states that if $p \mid |G|$, then G contains an element a of order p. Thus $|\langle a \rangle| = p$. The First Sylow Theorem can be viewed as a generalization of Cauchy's Theorem.

Theorem (5.2.5. First Sylow Theorem):
Let G be a group of order $p^n m$, p is a prime, $n \geq 1, \gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order p^i $(i < n)$ is normal in some subgroup of order p^{i+1}.

Proof: We prove this theorem by induction.
Base case: For $i = 1$, since $p \mid |G|$, by Theorem 5.1.2 (Cauchy), G contains an element a order p. So $|\langle a \rangle| = p$. (The statement about the normal subgroup holds trivially.)

Inductive step: Suppose that the statement holds for some $1 \leq i < n$, say H is a subgroup of G of order p^i. Then $p \mid [G : H]$. (WHY?). We have seen in proof of 5.2.4. that $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. By Theorem 5.1.2. $N_G(H)/H$ contains a subgroup of order p. Such a group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \triangleleft N_G(H)$, we have $H \triangleleft H_1$. Finally, $|H_1| = |H||H_1/H| = p^i \cdot p = p^{i+1}$.

not quite understand, should revisit. □

Definition (Sylow p subgroup): A subgroup P of a group G is said to be a Sylow P subgroup of G if P is a maximal P group of G. That is if $P \subseteq H \subseteq G$ with H being a p group, then $P = H$.

Now, as a corollary to theorem 5.2.5., we have the following corollary

Corollary (5.2.6.):
Let G be a group of order $p^n m$, where p is a prime, $n \geq 1, \gcd(p, m) = 1$. Let H be a p subgroup of G. Then

- H is a Sylow p subgroup if and only if $|H| = p^n$.
- Every conjugate of a Sylow p subgroup is a sylow p subgroup.
- If there is only one Sylow p subgroup P, then $P \triangleleft G$. What would happen if there are two such subgroups?

Theorem (5.2.7. Second Sylow Theorem):
If H is a p subgroup of a finite group G, and P is any Sylow p subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p subgroups of G are conjugate.

Proof: Let S be the set of all left cosets of P in G. Let H act on S by left multiplication. By Lemma 5.1.1., we have $|S_0| \equiv |S| = [G : P] \pmod{p}$. Since $p \nmid [G : P]$, we have $|S_0| \neq 0$. Thus there exists $xP \in S_0$ for some $x \in G$. Note that

$$\begin{aligned} xP \in S_0 &\iff hxP = xP, \forall h \in H \\ &\iff x^{-1}hxP = P, \forall h \in H \\ &\iff x^{-1}Hx \subseteq P \\ &\iff H \subseteq xPx^{-1} \end{aligned}$$

If H is a Sylow p subgroup, then $|H| = |P| = |xPx^{-1}|$. Thus $H = xPx^{-1}$. □

Theorem (Third Sylow Theorem):
If G is a finite group and p a prime with $p \mid |G|$. Then the number of Sylow p subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$.

Proof: By theorem 5.2.7, the number of Sylow p subgroups in G is the number of conjugates of any one of them, say P. This number is $[G : N_G(P)]$, which is a divisor of $|G|$.
Let $|S|$ be the set of all Sylow $p-$ subgroups of G and let P act on S by conjugation. Then $Q \in S_0$ if and

only if $xQx^{-1} = Q$ for all $x \in P$. The latter condition holds if and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow $p-$subgroups of G and hence of $N_G(Q)$.
By Corollary 5.2.6, they are conjugate in $N_G(Q)$. Since $Q \triangleleft N_G(Q)$, this can only occur if $Q = P$. Thus $S_0 = \{P\}$. By lemma 5.1.1., $|S| \equiv |S_0| \equiv 1 \pmod p$. So $|S| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. □

Remark Suppose that G is a group with $|G| = p^r m$ and $\gcd(p, m) = 1$. Let n_p be the number of Sylow $p-$subgroups of G. By the third Sylow theorem, we see that $n_p \mid p^r m$ and $n_p \equiv 1 \pmod p$. Since $p \nmid n_p$, we have $n_p \mid m$.
Example
Claim: every subgroup of order 15 is cyclic.
Proof: Let G be a group of order $15 = 3 \cdot 5$. Let n_p be the number of Sylow $p-$subgroups of G. By the third Sylow Theorem, we have $n_3 \mid 5, n_3 \equiv 1 \pmod 3$. So $n_3 = 1$. Similarly, $n_5 \mid 3, n_5 \equiv 1 \pmod 5$, so $n_5 = 1$. It follows there is only one Sylow 3 subgroup and one Sylow 5 subgroup in G, say P_3, P_5, respectively. Thus $P_3 \triangleleft G$ and $P_5 \triangleleft G$. Consider $|P_3 \cap P_5|$, which divides 3 and 5. So $|P_3 \cap P_5| = 1$. Also $|P_3 P_5| = 15 = |G|$. (Why is the product 15?) It follows that

$$G \simeq P_3 \times P_5 \simeq \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 5 \rangle \simeq \mathbb{Z}/\langle 15 \rangle$$

Example
Claim: there are two isomorphism classes of groups of order 21.
Let G be a group of order $21 = 7 \cdot 3$. Let n_p be the number of Sylow p subgroups of G. By the third Sylow theorem, we have $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$. Thus $n_3 = 1$ or 7.
Also $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$. So $n_7 = 1$. It follows that G has a unique Sylow 7 subgroup say P_7. Note $P_7 \triangleleft G$ and P_7 is cyclic, say $P_7 = \langle x \rangle$ with $x^7 = 1$. Let H be a sylow 3 group. Since $|H| = 3$, H is cyclic $H = \langle y \rangle$ with $y^3 = 1$. Since $P_7 \triangleleft G$, we have $yxy^{-1} = x^i$ for some $0 \leq i \leq 6$. It follows that

$$x = y^3 x y^{-3} = y^2 x^i y^{-2} = y x^{i^2} y^{-1} = x^{i^3}$$

Since $x = x^{i^3}$, $x^7 = 1$, we have $i^3 - 1 = 0 \pmod 7$ and since $0 \leq i \leq 6$, we have $i = 1, 2, 4$.

1. If $i = 1$, $yxy^{-1} = x$, that is, $yx = xy$. So G is an abelian group and $G \simeq \mathbb{Z}/\langle 21 \rangle$.
2. If $i = 2$, $yxy^{-1} = x^2$, $G = \{x^i y^i : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$
3. If $i = 4$ then $yxy^{-1} = x^4$. Note that

$$y^2 x y^{-2} = y x^4 y^{-1} = x^{16} = x^2$$

y^2 is also a genearator of H. Thus by replacing y with y^2, we get back to case 2. This gives us two isomorphism classses of groups order 21.

Solvable Groups

Definition: A group G is solvable if there exists a tower

$$G \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{1\}$$

With $G_{i+1} \triangleleft G_i$ and G_i / G_{i+1} abelian for all $0 \leq i \leq m - 1$. I don't see why this one holds?

Remark
G_{i+1} is not necessarily a normal subgroup of G. If G_{i+1} is a normal subgroup of G, we get $G_{i+1} \triangleleft G_i$ for free.

Example

Consider the symmetric group S_4. (24 elements, the group where elements act on $1, 2, 3, 4$ permutation.) Let A_4 be the alternating subgroup of S_4 (subgroup of even permutations) and $V \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$ the Klein 4 group. Note that A_4 and V are normal subgroups of S_4. We have

$$S_4 \supseteq A_4 \supseteq V \supseteq \{1\}$$

Since $S_4/A_4 \cong \mathbb{Z}/\langle 2\rangle$ and $A_4/V \cong \mathbb{Z}/\langle 3\rangle$, S_4 is solvable.

Before moving onto solvable groups, we recall theorems about groups

Theorem (Second Isomorphism Theorem):
If H and N are subgroups of a group G with $N \triangleleft G$, then $H/H \cap N \cong NH/N$, which is a set. However, if either H or N is a normal subgroup of G, then $NH = HN$ and it is a subgroup of G.

Theorem (Third Isomorphism Theorem):
If H and N are normal subgroups of a group G such that $N \subseteq H$, then H/N is a normal subgroup of G/N and $(G/N)/(H/N) \cong G/H$. (This is an explanation why the above remark holds).

Theorem (6.0.1.):
Let G be a solvable group.

1. If H is a subgroup of G, then H is solvable.
2. Let N be a normal subgroup of G. Then the quotient group G/N is solvable.

Proof: Since G is solvable, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{1\}$$

with $G_{i+1} \triangleleft G_i$ with G_i/G_{i+1} abelian for all $0 \leq i \leq m-1$.

1. Define $H_i = H \cap G_i$. Since $G_i \triangleleft G_{i+1}$, we have a tower

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_m = \{1\}$$

with $H_{i+1} \triangleleft H_i$. Note that both H_i and G_{i+1} are subgroups of G_i and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. Applying the second isomorphism theorem to G_i, we have

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \cong H_iG_{i+1}/G_{i+1} \subseteq G_i/G_{i+1}$$

Since G_i/G_{i+1} is abelian, so is H_i/H_{i+1}. It follows that H is solvable.

2. Consider the towers

$$G = G_0N \supseteq G_1N \supseteq G_2N \supseteq \ldots \supseteq G_mN = N$$

and

$$G/N = G_0N/N \supseteq G_1N/N \supseteq G_2N/N \supseteq \ldots \supseteq G_mN/N = \{1\}$$

Since $G_{i+1} \triangleleft G_i$ and $N \triangleleft G$, we have

$$G_{i+1}N \triangleleft G_iN, \text{ which implies } G_{i+1}N/N \triangleleft G_iN/N$$

By the third isomorphism theorem

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N$$

By the second isomorphism theorem,

$$G_iN/G_{i+1}N \cong G_i/(G_i \cap G_{i+1}N)$$

Consider the natural quotient map $G_i \to G_i/(G_i \cap G_{i+1}N)$ which is surjective. Since $G_{i+1} \subseteq G_i \cap G_{i+1}N$, it induces a surjective map $G_i/G_{i+1} \to G_i/(G_i \cap G_{i+1}N)$.

Remark: the above result comes from the Universal Property of Groups

Universal property of groups: Let G, G' be groups and let $f : G \to G'$ be a group homomorphism. If $N \lhd G$ satisfies $N \subseteq \ker(f)$, then there exists a unique map $\overline{f} : G/N \to G'$ such that $f = \overline{f} \circ \pi$ where $\pi : G \to G/N$ is the natural quotient map. I dont understand this part, why does the above follow from the universal property? I drew comm diagram but does not seem to match up.

Let us resume back to the proof.

Since G_i/G_{i+1} is abelian, so is $G_i/(G_i \cap G_{i+1}N)$. Thus $(G_iN/N)/(G_{i+1}N/N)$ is abelian. It follows that G/N is solvable.

□

The following theorem goes in the opposite direction of 6.0.1.

Theorem (6.0.2.):
Let N be a normal subgroup of a group G. If both N and G/N are solvable, then G is solvable. In particular, a direct product of finitely many solvable groups is solvable.

Proof: Since N is solvable, we have a tower

$$N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \ldots \supseteq N_m = \{1\}$$

With $N_{i+1} \lhd N_i$ and N_i/N_{i+1} abelian. For a subgroup $H \subseteq G$ with $N \subseteq H$, we denote $\overline{H} = H/N$.
Since G/N is solvable, we have a tower

$$G/N = \overline{G} = \overline{G_0} \supseteq \overline{G_1} \supseteq \ldots \supseteq \overline{G_r} = N/N = \{\overline{1}\}$$

with $\overline{G_{i+1}} \lhd \overline{G_i}$ and $\overline{G_i}/\overline{G_{i+1}}$ abelian. Let $Sub_N(G)$ denote the subgroups of G that contains N. Consider the map

$$\sigma : Sub_N(G) \to Sub(G/N) : H \mapsto H/N$$

For all $i = 0, 1, \ldots, r$, define $G_i = \sigma^{-1}(\overline{G_i})$. Since $N \lhd G$ and $\overline{G_{i+1}} \lhd \overline{G_i}$, we have

$$G_{i+1} \lhd G_i,$$

morevoer, by the third isomorphism theorem,

$$G_i/G_{i+1} \cong \overline{G_i}/\overline{G}_{i+1}$$

It follows that we have a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \ldots \supseteq G_r = N = N_0 \supseteq N_1 \supseteq N_2 \supseteq \ldots \supseteq N_m = \{1\}$$

With $G_{i+1} \triangleleft G_i, N_{i+1} \triangleleft N_i$ and $G_i/G_{i+1}, N_i/N_{i+1}$ are all abelian. Thus G is solvable. □

Example S_4 contains subgroups isomorphic to S_3 and S_2. Since S_4 is solvable, by theorem 6.0.1., S_3, S_2 are both solvable.

Definition (Simple): A group G is simple if it is not trivial and has no normal subgroups except $\{1\}$ and G. (Recall this from Pmath 347.)

Example: One can show that the alternating group A_5 is simple. Since $A_5 \supseteq \{1\}$ is the only tower and $A_5/\{1\}$ is not abelian, A_5 is not solvable. Thus by theorem 6.0.1., S_5 is also not solvable. Moreover, since for all S_n with $n \geq 5$, it contains a subgroup isomorphic to S_5 which is not solvable. By Theorem 6.0.1., S_n are not solvable for $n \geq 5$.

Corollary (6.0.3.):
Let G be a finite solvable group. Then there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_m = \{1\}$$

with $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} a cyclic group.

Proof: If G is solvable, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{1\}$$

with $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq n-1$. Consider $A = G_i/G_{i+1}$, a finite abelian group. We have

$$A \cong C_{k_1} \times C_{k_2} \times \ldots \times C_{k_r}$$

where C_k is a cyclic group of order k. Since each G_i/G_{i+1} can be written as product of cyclic groups, i dont think product of cyclic groups is cylic? the result follows. □

Remark
In the above proof, given a finite cyclic group C, by Chinese Remainde Theorem, we have

$$C \cong \mathbb{Z}/\langle p_1^{\alpha_1}\rangle \times \mathbb{Z}/\langle p_2^{\alpha_2}\rangle \times \ldots \times \mathbb{Z}/\langle p_r^{\alpha_r}\rangle$$

where p_i are distinct primes. Also, for a cyclic group whose order is a prime power, say $\mathbb{Z}/\langle p^\alpha\rangle$, we have a tower of subgroups

$$\mathbb{Z}/\langle p^\alpha\rangle \supseteq \mathbb{Z}/\langle p^{\alpha-1}\rangle \supseteq \ldots \supseteq \mathbb{Z}/\langle p\rangle \supseteq \{1\}$$

So we can further require the quotient G_i/G_{i+1} in the above corollary to be a cyclic group of prime order.

Week 7. Autmorphism Groups

In this chapter, we will associate field extensions to groups. We focus on automorphism groups of splitting fields.

7.1 General Automorphism groups

Definition (F-automorphism): Let E/F be a field extension. If ψ is an automorphism of E, that is $\psi : E \to E$ is an ismomorphism, and $\psi \mid_F = 1_F$, we say ψ is an $F-$automorphism of E. By maps composition, the set

$$\{\psi : E \to E \mid \psi \text{ is an F automorphism}\}$$

is a group. We call it the automorphism group of E/F, denoted by $Aut_F(E)$.

Lemma (7.1.1):
Let E/F be field extensions, $f(x) \in F[x]$, and $\psi \in Aut_F(E)$. If $\alpha \in E$ is a root of $f(x)$ then $\psi(\alpha)$ is also a root of $f(x)$.

Proof: Write $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F[x]$. Then

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

So $\psi(\alpha)$ is a root of $f(x)$. □

Lemma (7.1.2):
Let $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a field extension of F. For $\psi_1, \psi_2 \in Aut_F(E)$, if $\psi_1(\alpha_i) = \psi_2(\alpha_i)$ for all $\alpha_i (1 \leq i \leq n)$, then $\psi_1 = \psi_2$.

Proof: Note that for $\alpha \in E$, α is of the form

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots \alpha_n)}$$

$f, g \in F[x_1, \ldots, x_n]$ so the lemma follows. That is, everything in the field can be written as a polynomial with coefficients in F and variables in E with those alphas. So the $F-$homomorphisms fix them. □

Corollary (7.1.3.):
If E/F is finite extension then $Aut_F(E)$ is a finite group.

Proof: Since E/F is a finite extension, by theorem 2.2.4. $E = F(\alpha_1, \alpha_2, \dots \alpha_n)$ such that each α_i are algebraic over F. For $\psi \in Aut_F(E)$, by lemma 7.1.1., $\psi(\alpha_i), (1 \leq i \leq n)$, is a root of the minimal polynomial of α_i. Thus it has only finitely many choices. By lemma 7.1.2, since $\psi \in Aut_F(E)$ is completely determined by $\psi(\alpha_i)$, there are only finitely many choices for ψ. Hence $Aut_F(E)$ is finite.

□

Remark

The converse of the above Corollary is false. For example $\mathbb{R}/\mathbb{Q}$ is an infinite extension, but $Aut_{\mathbb{Q}}(\mathbb{R}) = \{1\}$. Indeed, we will show in Assignment 7 that $Aut_{\mathbb{Q}}(\mathbb{R}) = \{1\}$, $\psi \in Aut(\mathbb{R})$ with $\psi(1)$ will imply that $\psi \mid_{\mathbb{Q}} = 1_{\mathbb{Q}}$.

7.2 Automorphism Groups with Splitting Fields

Definition (Automorphism group): Let F be a field and $f(x) \in F[x]$. The automorphism group of $f(x)$ over F is defined to be the group $Aut_F(E)$ where E is the splitting field of $f(x)$ over F.

We recall theorem 3.2.1. Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring isomorphism which extends ϕ, and maps $x \mapsto x$. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there exists an isomorphism $\psi : E \to E_1$ that extends ϕ.
In A3, we prove that the number of such ψ is $\leq [E : F]$. And equality holds if and only if $f(x)$ is separable over F. As a direct consequence we have

Theorem (7.2.1.):
Let E/F be the splitting field of a non-zero polynomial $f(x) \in F[x]$. We have $|Aut_F(E)| \leq [E : F]$ and equality holds if and only if $f(x)$ is separable.

Theorem (7.2.2.):
If $f(x) \in F[x]$ has n distinct roots in the splitting field E, then $Aut_F(E)$ is isomorphic to a subgroup of the symmetric group S_n. In particular, $|Aut_F(E)|$ divides $n!$.

Proof: Let $X = \{\alpha_1, \dots, \alpha_n\}$ be distinct roots of $f(x) \in E$. By lemma 7.1.1., if $\psi \in Aut_F(E)$, then $\psi(X) = X$. Let $\psi \mid_X$ be the restriction of ψ in X and S_X the permutation group of X. The map

$$Aut_F(E) \to S_X \cong S_n, \psi \mapsto \psi \mid_X$$

is a group homomorphism. Moreover, by lemma 7.1.2., it is injective. Thus $Aut_F(E)$ is isomorphic to a subgroup of S_n. □

Example 1.

Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. And $E/\mathbb{Q}$ the splitting field of $f(x)$. Thus $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and $[E : F] = 6$. Since $ch(\mathbb{Q}) = 0$, $f(x)$ is separable. By theorem 7.2.1.

$$|Aut_{\mathbb{Q}}(E)| = [E : F] = 6$$

Also, since $f(x)$ has 3 distinct roots in E, by theorem 7.2.2, $Aut_{\mathbb{Q}}(E)$ is a subgroup of S_3. Since the only subgroup of S_3 which is of order 6 is S_3 so

$$Aut_{\mathbb{Q}}(E) \cong S_3$$

Example 2.
Let F be a field with $ch(F) = p, F^p \neq F$. and $f(x) = x^p - a, a \in F \setminus F^p$. Let E/F be the splitting field of $f(x)$. We have seen in section 4.4. that $f(x) = (x - \beta)^p$ for some $\beta \in E \setminus F$. Thus, $E = F(\beta)$. Since β can only map to β, $Aut_F(E)$ is trivial. So $|Aut_F(E)| = 1$ and $[E : F] = p$.
We have $|Aut_F(E)| \neq [E : F]$. The reason why they are unequal is because $f(x)$ is not separable.

7.3. Fixed Fields

Now we introduce the fixed fields of a group.

Definition (Fixed field): Let E/F be a field extension and $\psi \in Aut_F(E)$. Define

$$E^{\psi} = \{a \in E, \psi(a) = a\}$$

which is a subfield of E containing F. We call E^{ψ} the fixed field of ψ.
If $G \subseteq Aut_F(E)$, then the fixed field of G is defined by:

$$E^G = \bigcap_{\psi \in G} E^{\psi} = \{a \in E, \psi(a) = a, \forall \psi \in G\}$$

Theorem (7.3.1.):
Let $f(x) \in F[x]$ be a separable polynomial and E/F is its splitting field. If $G = Aut_F(E)$ then $E^G = F$.

Proof: Set $L = E^G$. Since $F \subseteq L$, we have $Aut_L(E) \subseteq Aut_F(E)$. (because for every $g \in Aut_L(E)$, it fix all elements in $L = E^G$, by definition it fix all elements in F.)

On the other hand, if $\psi \in Aut_F(E)$, by the definition of L, for all $a \in L$, we have $\psi(a) = a$. This implies that $\psi \in Aut_L(E)$.
Thus

$$Aut_F(E) = Aut_L(E).$$

Note that since $f(x)$ is separable over F and splits over E, $f(x)$ is also separable over L and has E as its spliitting field over L. Thus by theorem 7.2.1.

$$|Aut_F(E)| = [E : F], \text{ and } |Aut_L(E)| = [E : L]$$

It follows that $[E : F] = [E : L]$. Since $[E : F] = [E : L][L : F]$ we have $[L : F] = 1$ and $L = F$. So $E^G = F$.

□

Week 8. Separable Extensions and Normal Extensions

In this chapter, we will talk about separable extensions and normal extensions. We will talk about Galois extensions in the next chapter.

8.1 Separable extensions

Definition: Let E/F be an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be minimal polynomial of α. We say that α is separable over F if $p(x)$ is separable. If for all $\alpha \in E$, α is separable, then we say that E/F is separable.

Example:
If $ch(F) = 0$, by theoerm 4.4.1., F is perfect and every polynomial $f(x) \in F(x)$ is separable. Thus, if $Ch(F) = 0$, then any algebraic extension E/F is separable.

Theorem (8.1.1.):
Let E/F be the splitting field of $f(x) \in F[x]$. If $f(x)$ is separable, then E/F is separable.

Proof: Note that in this case α in E is arbitrary. We will show that the min poly is separable with respect to all the αs.
Let $\alpha \in E$ and $p(x) \in F[x]$ be the minimal polynomial of α. Let $\{\alpha = \alpha_1, \dots, \alpha_n\}$ be all of the distinct roots of $p(x)$ in E. Now, define

$$\tilde{p}(x) = (x - \alpha_1) \dots (x - \alpha_n)$$

Now we claim that $\tilde{p}(x) \in F[x]$.
Let $G = Aut_F(E)$ and $\psi \in G$. Since ψ is an automorphism, $\psi(\alpha_i) \neq \psi(\alpha_j)$ if $i \neq j$. By lemma 7.1.1., ψ permutes $\alpha_1, \dots, \alpha_n$. Thus by extending $\psi : E \to E$ to $\psi : E[x] \to E[x]$, we have

$$\psi(\tilde{p}(x)) = (x - \psi(\alpha_1)) \dots (x - \psi(\alpha_n))$$

$$= (x - \alpha_1) \dots (x - \alpha_n) = \tilde{p}(x)$$

It follows that $\tilde{p}(x) \in E^{\psi}[x]$. (Recall, this means the fixed field, the field of elements fixed under permutation of ψ) Since $\psi \in G$ is arbitrary, $\tilde{p}(x) \in E^G[x]$. Since E/F is the splitting field of the separable polynomial $f(x)$, by theorem 7.3.1.,$\tilde{p}(x) \in F[x]$. Thus the claim is true.

Therefore, we have $\tilde{p}(x) \in F[x]$ with $\tilde{p}(\alpha) = 0$. Since $p(x)$ is the minimal polynomial of α over F, so we have $p(x) \mid \tilde{p}(x)$. Also since $\alpha_1, \dots, \alpha_n$ are all distinct roots of $p(x)$, we have $\tilde{p}(x) \mid p(x)$. Since both $p(x), \tilde{p}(x)$ are monic, they are equal. Hence $p(x)$ is separable.

□

Corollary (8.1.2.):
Let E/F be a finite extension and $E = F(\alpha_1, \alpha_2 \dots, \alpha_n)$. If each α_i is separable over F with $(1 \leq i \leq n)$, then E/F is separable.

Proof: Let $p_i(x) \in F[x]$ be the minimal polynomial α_1, with $(1 \leq i \leq n)$. Let $f(x) = p_1(x)p_2(x)\ldots p_n(x)$. Since each $p_1(n)$ is separable, so is $f(x)$. Let L be the splitting field of $f(x)$ over F. By Theorem 8.1.1, L/F is separable. Since $E = F(\alpha_1, \ldots, \alpha_n)$ is a subfield of L, E is also separable. Here, why does subfield mean separable? □

Corollary (8.1.3.):
Let E/F be an algebraic extension and L the set of all $\alpha \in E$ which are separable over F. Then L is an intermediate field.

Proof: Let $\alpha, \beta \in L$. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta, (\beta \neq 0), \in F(\alpha, \beta)$. By corollary 8.1.2, $F(\alpha, \beta)$ is separable and hence it is contained in L. So $\alpha \pm \beta, \alpha\beta, \alpha/\beta(\beta \neq 0) \in L$.

□

In fact, we have seen in theorem 2.2.4, that a finite extension is a composition of simple extensions.

Definition: If $E = F(\gamma)$, is a simple extension, then γ is a primitive element of E/F.

Theorem (8.1.4. Primitive Element Theorem):
If E/F is a finite separable extension, then $E = F(\gamma)$ for some $\gamma \in E$. In particular if $ch(F) = 0$, then any finite extension E/F is a simple extension.

Proof:
If F is a finite field:
We have seen in Cor 4.3.3., that a finite extension of a finite field is always simple.
If F is an infinite field:
Suppose F is an infinite field. Since $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$. So it suffices to consider when $E = F(\alpha, \beta)$, and the general case can be proven by inductin. So for now we assume $E = F(\alpha, \beta)$, where $\alpha, \beta \notin F$.
We claim that there exists $\lambda \in F$ such that $\gamma = \alpha + \lambda\beta, \beta \in F(\gamma)$.
If the claim is true, then we would have $\alpha = \gamma - \lambda\beta \in F(\gamma)$ so $F(\alpha, \beta) \subseteq F(\gamma)$. Since $\gamma = \alpha + \lambda\beta$, we also have $F(\gamma) \subseteq F(\alpha, \beta)$. This means $E = F(\alpha, \beta) = F(\gamma)$.

Now let us prove the claim. We let $a(x), b(x)$ be minimal polynomials of α and β over F respectively. Since $\beta \notin F$, $\deg(b) > 1$. Therefore, there exists another root $\tilde{\beta}$ of $b(x)$ such that $\tilde{\beta} \neq \beta$. We can pick $\lambda \in F$ such that $\lambda \neq \frac{\tilde{\alpha}-\alpha}{\beta-\tilde{\beta}}$ for all the roots $\tilde{\alpha}$ of $a(x)$ and all roots $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} \neq \beta$ in some splitting field of $a(x)b(x)$ over F. The choice is possible since there are infinitely many elements in F, but only finitely many of $\tilde{\alpha}$ and $\tilde{\beta}$. Now we let $\gamma = \alpha + \lambda\beta$. Now consider the following:

$$h(x) = a(\gamma - \lambda x) \in F(\gamma)[x]$$

Then

$$h(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$$

However, for any other $\tilde{\beta} \neq \beta$, since by the choice of λ,

$$\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$$

so $h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0$. Therefore, $h(x), b(x)$ have β as a common root, but no other common root in any extension of $F(\gamma)$. Let $b_1(x)$ be the minimal polynomial of β over $F(\gamma)$. So $b_1(x)$ divides both $h(x)$ and $b(x)$. Since E/F is separable and $b(x) \in F[x]$ is irreducible, $b(x)$ has distinct roots, so does $b_1(x)$.
The roots of $b_1(x)$ are also common to $h(x)$ and $b(x)$. Since $h(x)$ and $b(x)$ has only β as a common root, we have $b_1(x) = x - \beta$. Since $b_1(x) \in F(\gamma)[x]$. We obtain $\beta \in F(\gamma)$ as required.

□

8.2 Normal Extensions

Definition (Normal Extension): Let E/F be an algebraic extension. Then E/F is a normal extension if for any irreducible polynomial $p(x) \in F[x]$, either $p(x)$ has no root in E or $p(x)$ has all roots in E. In other words, if $p(x)$ has a root in E, $p(x)$ splits over E.

Example:
Let $\alpha \in \mathbb{R}$ with $\alpha^4 = 5$. The roots of $x^4 - \alpha$ are $\pm\alpha, \pm\alpha i$, and $\mathbb{Q}(\alpha)$ is real, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal. If we let $\beta = (1+i)\alpha$. Then $\mathbb{Q}(\beta)/\mathbb{Q}$ is also not normal. Note that

$$\beta^2 = 2i\alpha^2, \beta^4 = -4\alpha^4 = -20$$

Now, since $\pm\beta, \pm i\beta$ all satisfy that $x^4 = -20$, to show that $\mathbb{Q}(\beta)$ is not normal, we suffice to show that $i \notin \mathbb{Q}(\beta)$. Since the minimal polynoimal of β over $\mathbb{Q}$ is $x^4 + 20$, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Also the roots of $p(x)$ are $\pm\beta, \pm i\beta$. Since the minimal polynomial of α is $x^4 - 5$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
Note that if $\alpha \in \mathbb{Q}(\beta)$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$, it implies $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ which is impossible as $\beta = \alpha + i\alpha \notin \mathbb{Q}(\alpha)$. Therefore we have $\alpha \notin \mathbb{Q}(\beta)$. So it implies $i \notin \mathbb{Q}(\beta)$ (if $i \in \mathbb{Q}(\beta)$ then $\alpha = \beta/(1+i) \in \mathbb{Q}(\beta)$, contradiction.)

It follows that the factorization of $p(x)$ over $\mathbb{Q}(\beta)$ is

$$(x - \beta)(x + \beta)(x^2 + \beta^2)$$

Since $p(x)$ does not split over $\mathbb{Q}(\beta)$ we have $\mathbb{Q}(\beta)/\mathbb{Q}$ is not normal.

Theorem (8.2.1):
A finite extension E/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.

Proof:
$\Longrightarrow$
Suppose that E/F is normal. We write $E = F(\alpha_1, \ldots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of $\alpha_i (1 \leq i \leq n)$.

Define

$$f(x) = p_1(x)p_2(x)\dots p_n(x).$$

Since E/F is normal, each $p_i(x)$ splits over E. Let $\alpha_i = \alpha_{i,1}, \alpha_{i,2}\dots, \alpha_{i,r_i}, 1 \leq i \leq n$ be roots of $p_i(x)$ in E. Then

$$E = F(\alpha_1, \dots, \alpha_n)$$
$$= F(\alpha_{1,1},\alpha_{1,2}, \dots \alpha_{1,r_1}, \alpha_{2,1}, \dots \alpha_{n,r_n}),$$

Which is the splitting field of $f(x)$ over F.

$\Longleftarrow$

Let E/F be the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ be irreducible and has root $\alpha \in E$. Let K/E be the splitting field of $p(x)$ over E. Write

$$p(x) = c(x - \alpha_1)\dots(x - \alpha_n)$$

where $0 \neq c \in F, \alpha = \alpha_1 \in E, \alpha_2, \dots \alpha_n \in K = E(\alpha_1, \dots, \alpha_n)$. Since

$$F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\alpha_2)$$

Why is this isomorphic to $F(\alpha_2)$????

Therefore we have the $F-$isomorphism

$$\theta : F(\alpha) \to F(\alpha_2), \theta(\alpha) = \alpha_2$$

Note that $p(x) \in F[x] \subseteq F(\alpha)[x]$ and $p(x) \in F(\alpha_2)[x]$.

So we can view K as the splitting field of $p(x)$ over $F(\alpha)$ and $F(\alpha_2)$ respectively. SO by theorem 3.2.1. there exists an isomorphism

$$\psi : K \to K$$

that extends θ. In particular, $\psi \in Aut_F(K)$:

$$\begin{tikzcd}
K \arrow[r, "\psi", "\text{iso extending } \theta"'] \arrow[d, dash] & K \arrow[dd, dash] \\
E \arrow[d, dash] & \\
F(\alpha) \arrow[r, "\theta", "F\text{-iso}"'] \arrow[d, dash] & F(\alpha_2) \arrow[d, dash] \\
F \arrow[r, "1"'] & F
\end{tikzcd}$$

$\boxed{\theta(\alpha) = \alpha_2}$

Since $\psi \in Aut_F(K)$, ψ permutes the roots of $f(x)$. Since E is generated over F by roots of $f(x)$, lemma 7.1.1. we have $\psi(E) = E$. It follows that for $\alpha \in E, \alpha_2 = \psi(\alpha) \in E$. Similarly we can prove that $\alpha_i \in E$ for $3 \leq i \leq n$. So $K = E$ and $p(x)$ splits over E. It follows E/F is normal.

□

Example:

Claim: every quadratic extension is normal.

Let E/F be a field extension with $[E : F] = 2$. For $\alpha \in E \setminus F$, we have $E = F(\alpha)$. Let $p(x) = x^2 + ax + b$ be

the minimal polynomial of α over F. If β is another root of $p(x)$ then we would have $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$.
Therefore $\beta = -a - \alpha = b/\alpha$, is the other root of $p(x)$ and $\beta \in E$. This means that E/F is normal.

Example: The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the irreducible polynomial $p(x) = x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$ but $p(x)$ does not split over $\mathbb{Q}(\sqrt[4]{2})$. Note that this extension is made of two quadratic extensions, which are $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, both of them are normal. So if E/K and K/F are normal extensions, E/F is not always normal.

Proposition (8.2.2.):
If E/F is a normal extension and K is an intermediate field, then E/K is normal.

Proof: Let $p(x) \in K[x]$ be irreducible and has a root $\alpha \in E$. Let $f(x) \in F[x] \subseteq K[x]$ be the minimal polynomial of α over F. Then, $p(x) \mid f(x)$. Since E/F is normal, $f(x)$ splits over E, so does $p(x)$. So E/K is a normal extension. □

Remark:
In Prop 8.2.2., K/F is not always normal. For example, if $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[4]{2})$ and $E = \mathbb{Q}(\sqrt[4]{2}, i)$, then E/F is the splitting field of $x^4 - 2$ and hence normal. Also, E/K is normal but K/F is not normal.

Proposition 2.9 (8.2.3.):
Let E/F be a finite normal extension and $\alpha, \beta \in E$. Then the following conditions are equivalent:

1. There exists $\psi \in Aut_F(E)$ such that $\psi(\alpha) = \beta$.
2. The minimal polynomials of α and β are the same

In this case, we say that α, β are conjugates over F.

Proof:
$1 \implies 2$
Let $p(x)$ be the minimal polynomial of α over F and $\psi \in Aut_F(E)$ with $\psi(\alpha) = \beta$. By Lemma 7.1.1., β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Hence α and β have the same minimal polynomials.
$2 \implies 1$
Suppose that the minimal polynomial of α and β are the same. Say $p(x)$. Since

$$F(\alpha) \cong F[x]/\langle p(x) \rangle \cong F(\beta)$$

we have $F-$isomorphism $\theta : F(\alpha) \to F(\beta)$ with $\theta(\alpha) = \beta$. Since E/F is a finite normal extension. By Theorem 8.2.1., E is the splitting field of some $f(x) \in F[x]$ over F. We can also view E as the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively. Thus by theorem 3.2.1, there exists an isomorphism $\phi : E \to E$ which extends θ. It follow $\psi \in Aut_F(E)$ and $\psi(\alpha) = \beta$. □

Example: The complex numbers $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2$ are all conjugates over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Note that the normal extensions are “nice” in some aspects. Not all finite extensions are normal. We can try to construct normal extensions for finite extensions, and we want to do it in the “minimal way” whereas the associated group $Aut_F(E)$ is as small as possible.

Definition (Normal Closure): A normal closure of a finite extension E/F is a finite normal extension N/F satisying the following properties:

1. E is a subfield of N
2. Let L be an intermediate field of N/E. If L is normal over F then $L = N$.

Example: The normal closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$.

Theorem (8.2.4.):
Every finite extension E/F has a normal closure N/F which is unique up to E isomorphism.

Proof:
We first write $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.
Existence:
Let $p_i(x)$ be the minimal polynomial of α_i over F for $1 \leq i \leq n$. Write $f(x) = p_1(x)p_2(x)\dots p_n(x)$ and let N/E be the splitting field of $f(x)$ over E. Since $\alpha_1, \dots, \alpha_n$ are roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By theorem 8.2.1, N is normal over F. Let $L \subseteq N$ be a subfield containing E. Then L contains all of α_i. If L is normal over F, each $p_i(x)$ splits over L. Thus $N \subseteq L$ and it follows $L = N$.

Uniqueness:
Let N/E be the splitting field of $f(x)$ over E defined as above. Let N_1/F be another normal closure of E/F. Since N_1 is normal over F and contains all α_i, N_1 must contain a splitting field $\tilde{N}$ of $f(x)$ over F, hence over E. By corollary 3.2.2., N and $\tilde{N}$ are E-isomorphic. Since $\tilde{N}$ is a splitting field of $f(x)$ over F, by theorem 8.2.1, $\tilde{N}$ is also normal over F. By definition of a normal closure, $N_1 = \tilde{N}$. So N, N_1 are E-isomorphic.

□

Week 9. Galois Correspondence

9.1 Galois extensions

Recall the two following theorems: Given finite extensions E/F, we have proven the two following theorems

- 8.2.1. E is the splitting field of some $f(x) \in F[x] \iff E/F$ is normal.
- 8.1.1. E is the splitting field of some separable polynonmial $f(x) \in F[x] \implies E/F$ is separable.

Now, if E is the splitting field of some polynomial $f(x) \in F[x]$, then we have $\iff$ in 8.1.1., as the opposite side holds trivially.

Definition 2.12: An algebraic extension E/F is Galois if it is normal and separable. If E/F is a Galois extension, the Galois group of E/F, $Gal_F(E)$, is defined to be the automorphism group of $Aut_F(E)$.

Definition 2.13: A Galois extension E/F is called abelian, cyclic, or solvable if $Gal_F(E)$ has the corresponding properties.

Remark

1. By theorem 8.1.1, 8.2.1, a finite Galois extension E/F is equivalent to the splitting field of a separable polynomial $f(x) \in F[x]$.
2. If E/F is a finite Galois extension, 7.2.1. states that
$$|Gal_F(E)| = [E : F]$$
3. If $E.F$ is the splitting field of a separabale polynomial $f(x) \in F[x]$ with $def(f) = n$, by theorem 7.2.2, $Gal_F(E)$ is a subgroup of S_n.

Example
Let E be the splitting field of $(x^2 - 2)(x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$. Then $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $[E : \mathbb{Q}] = 8$. For $\psi \in Gal_{\mathbb{Q}}(E)$: we have

$$\psi(\sqrt{2}) \in \{\pm\sqrt{2}\}, \psi(\sqrt{3}) \in \{\pm\sqrt{3}\}, \psi(\sqrt{5}) \in \{\pm\sqrt{5}\}$$

since $|Gal_{\mathbb{Q}}(E)| = [E : \mathbb{Q}] = 8$ we have

$$Gal_{\mathbb{Q}}(E) \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$$

Definition: Let $t_1, t_2, \dots, t_n$ be variables. We define the elementary symmetric function in $t_1, t_2, \dots t_n$ as

- $s_1 = t_1 + \dots + t_n$
- $s_2 = \sum_{1 \le i < j \le n} t_i t_j$
- $\dots$
- $s_n = t_1 t_2 \dots t_n$

Then it follows that $f(x) = (x - t_1)(x - t_2) \dots (x - t_n) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \dots + (-1)^n s_n$.

Theorem (9.1.1. (E. Artin)):
Let E be a field and G a finite group of $Aut(E)$, the automorphism group of E. Let $E^G = \{\alpha \in E, \psi(\alpha) = \alpha, \forall \psi \in G\}$. (fixed elements under all the automorphisms of the field) Then E/E^G is a finite Galois extension and $Gal_{E^G}(E) = G$. In particular,

$$[E : E^G] = |G|$$

Proof:
Let $n = |G|$ and $F = E^G$. For $\alpha \in E$, consider the G orbit of α

$$\{\psi(\alpha) \mid \psi \in G\} = \{\alpha = \alpha_1, \alpha_2, \dots, \alpha_m\}$$

where the α_is are distinct.
Note that $m \le n$. Let $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$. For any $\psi \in G, \psi$ permutes the roots of

$\{\alpha_1, \ldots, \alpha_m\}$. Since the coefficients of $f(x)$ are symmetric with respect to α_i $(1 \leq i \leq m)$. They are fixed by all $\psi \in G$. Thus

$$f(x) \in E^G[x] = F[x]$$

Showing it is minimal polynomial

To show $f(x)$ is actually the minimal polynomial of α, we need to show it is irreducible. Consider a factor $g(x) \in F[x]$ of $f(x)$. WLOG write $g(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_l)$

If $l \neq m$, since $\alpha_i (1 \leq i \leq m)$ are in the G orbit of α there exists $\psi \in G$ such that

$$\{\alpha_1, \ldots, \alpha_l\} \neq \{\psi(\alpha_1), \psi(\alpha_2), \ldots, \psi(\alpha_l)\}$$

It follows that

$$\psi(g(x)) = (x - \psi(\alpha_1)) \ldots (x - \psi(\alpha_l)) \neq g(x)$$

Thus, if $l \neq m$, $g(x) \notin F[x]$. It follows that $f(x)$ is the minimal polynomial of α over F.

Showing it is Galois extension

Since $f(x) \in F[x]$ is separable and splits over E, E/F is a Galois extension.

Showing $[E : F] \leq n$

Now suppose for contradiction, $[E : F] > n = |G|$, then we can choose $\beta_1, \beta_2, \ldots, \beta_{n+1} \in E$ which are linearly independent over F.

Consider the system

$$\psi(\beta_1)v_1 + \ldots + \psi(\beta_{n+1})v_{n+1} = 0, \forall \psi \in G$$

of n linear equations in $n+1$ variables $v_1, \ldots, v_{n+1}$. Thus it has a nonzero solution in E. Let $(\gamma_1, \ldots, \gamma_{n+1})$ be such a solution which has the minimal number of nonzero coordinates, say we have r coordinates. Clearly $r > 1$. WLOG we assume

$$\gamma_1, \ldots, \gamma_r \neq 0, \gamma_{r+1}, \ldots, \gamma_{n+1} = 0$$

This means that

$$\psi(\beta_1)\gamma_1 + \ldots + \psi(\beta_r)\gamma_r = 0 \ (1)$$

for all $\psi \in G$.

Assume $\gamma_r = 1$ (by dividing). Also since $(\beta_1, \ldots, \beta_r)$ are independent over F and $\beta_1\gamma_1 + \ldots + \beta_r\gamma_r = 0$, there exists at least one $\gamma_i \notin F$ (if all of the $\gamma \in F$ then $\beta_1\gamma_1 + \ldots + \beta_r\gamma_r = 0$ would imply all $\gamma = 0$)

Since $r \geq 2, WLOG$, we can assume $\gamma_1 \notin F$. Pick $\psi \in G$ such that $\psi(\gamma_1) \neq \gamma_1$. Applying ψ into (1), we get

$$\sum_{i=1^n} (\phi \circ \psi)(\beta_i)\phi(\gamma_i) = 0, \forall \psi \in G$$

$$\sum_{i=1}^{r} \psi(\beta_i)\phi(\gamma_i) = 0, \forall \psi \in G$$

Subtracting we get

$$\sum_{i=1}^{r} \psi(\beta_i)(\gamma_i - \phi(\gamma_i)) = 0$$

Since $\gamma_r = 1$, we have $\gamma_r - \phi(\gamma_r) = 0$. Also, since $\gamma_1 \notin F$ we have $\gamma_1 - \phi(\gamma_1) \neq 0$. This shows all the $\gamma_i - \phi(\gamma_i), 1 \leq i \leq r$ are all zero, but presents a solution to the system

$$\sum_{i=1}^{n+1} \psi(\beta_i)\phi(\gamma_i) = 0, \forall \psi \in G$$

This contradicts that $(\gamma_1, \dots, \gamma_{n+1})$ having minimal number of nonzero coordinates. So $[E : F] \leq n$.

More observations

We have shown E/F is a finite Galois extension. So E is the splitting field of some separable polynomial over F. Also since $F = E^G = \{\alpha \in E, \psi(\alpha) = \alpha, \forall \psi \in G\}$, G is a subgroup of $Gal_F(E)$. By theorem 7.2.1.

$$n = |G| \leq |Gal_F(E)| = [E : F] \leq n$$

So $[E : F] = n$ and $Gal_F(E) = G$. This completes the proof. □

Remark

Let E be a field and G a finite subgroup of $Aut(E)$. For $\alpha \in E$, let

$$\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m\}$$

be the G orbit of α, i.e. the set of all conjugates of α. Then we see from the proof of theorem 9.1.1. that the minimal polynomial of α over E^G is

$$(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m) \in E^G[x]$$

Example

Let $E = F(t_1, t_2, \dots, t_n)$ be the function field in n variables $t_1, t_2, \dots, t_n$ over a field F. Consider the symmetric group S_n as the subgroup of $Aut(G)$ which permutes the variables $t_1, t_2, \dots, t_n$ that fixes the field F.

We are interested in finding $E^{S_n} = E^G$ where $G = S_n$. From the proof of 9.1.1., the coefficients of the minimal polynomial of t_1 lies in E^G. By considering the minimal polynomial of t_1, we can get some hints about E^G. The $G-$orbit of t_1 is $\{t_1, t_2, \dots t_n.\}$

By the above remark, we see that

$$f(x) = (x - t_1) \dots (x - t_n)$$

is the minimal polynomial of t_1 over E^G. Let $s_1, \dots, s_n$ be the elementary symmetric functions of $t_1, \dots, t_n$. So we have $f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-1} - \dots + (-1)^n s_n \in L[x]$ where $L = F(s_1, \dots, s_n) \subseteq E^G$.

Claim: $L = E^G$.

We now prove this claim. Since E is the splitting field of $f(x)$ over L, since the $def(f) = n$, theorem 3.3.1, we have $[E : L] \leq n!$. By theorem 9.1.1., $[E : E^G] = |G| = |S_n| = n!$

since $L \subseteq E^G$, it follows

$$n! = [E : E^G] \leq [E : L] \leq n! \implies E^G = L$$

9.2. The Fundamental Theorem

Theorem (9.2.1. The Fundamental Theorem of Galois Theory):
Let E/F be a finite Galois extension and $G = Gal_F(E)$. There is an order preserving bijection between the intermediate fields of E/F and the subgroups of G. More precisely, we let $Int(E/F)$ denote the set of intermediate fields of E/F and $Sub(G)$ the set of subgroups of G, the maps

$$Int(E/F) \to Sub(G), L \mapsto L^* := Gal_L(E)$$

and

$$Sub(G) \to Int(E/F), H \mapsto H^* := E^H$$

are inverse of each other and reverse in the inclusion relation. In particular, for $L_1, L_2 \in Int(E/F)$ with $L_2 \subseteq L_1$, $H_1, H_2 \in Sub(G)$ with $H_2 \subseteq H_1$, we have

$$[L_1 : l_2] = [L_2^* : L_1^*], [H_1 : H_2] = [H_2^* : H_1^*]$$

$$\begin{tikzcd}
E \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} = \mathrm{Gal}_E(E) \arrow[d, dash] \\
L_1 \arrow[r, leftrightarrow] \arrow[d, dash] & L_1^* = \mathrm{Gal}_{L_1}(E) \arrow[d, dash] \\
L_2 \arrow[r, leftrightarrow] \arrow[d, dash] & L_2^* = \mathrm{Gal}_{L_2}(E) \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & G = \mathrm{Gal}_F(E)
\end{tikzcd}$$

Proof: Let $L \in Int(E/F), H \in Sub(G)$. Recall theorem 7.3.1., which states if $G_1 = Gal_{G_1}(E_1)$ then $E_1^{G_1} = F_1$. So we have

$$(L^*)^* = (Gal_L(E))^* = E^{Gal_L(E)} = L$$

Theorem 9.1.1. states that if $G_1 \subseteq Aut(E_1)$, then $Gal_{E^H}(E_1) = G_1$, so we have

$$(H^*)^* = (E^H)^* = Gal_{E^H}(E) = H$$

So

$$H \mapsto H^* \mapsto H^{**} = H, L \mapsto L^* \mapsto L^{**} = L$$

Particularly, $L \mapsto L^*$ and $H \mapsto H^*$ are inverse of each other.
Let $L_1, L_2 \in Int(E/F)$. Since E/F is the splitting field of some separable polynomial $f(x) \in F[x]$, $E/L_1, E/L_2$ are also Galois extensions since E is the splitting field of $f(x)$ over L_1, and L_2 respectively. We have

$$L_2 \subseteq L_1 \implies Gal_{L_1}(E) \subseteq Gal_{L_2}(E) \ i.e. \ L_1^* \subseteq L_2^*$$

This is true because $L_2 \subseteq L_1$ so any automorphism that fix L_1 would automatically also fix L_2.
Also,

$$[L_1 : L_2] = \frac{[E : L_2]}{[E : L_1]} = \frac{|Gal_{L_2}(E)|}{|Gal_{L_1}(E)|} = \frac{|L_2^*|}{|L_1^*|} = [L_2^* : L_1^*]$$

For $H_1, H_2 \in Sub(G)$,

$$H_2 \subseteq H_1 \implies E^{H_1} \subseteq E^{H_2},\ i.e.\ H_1^* \subseteq H_2^*$$

Also

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{|Gal_{E^{H_1}}(E)|}{|Gal_{E^{H_2}}(E)|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*]$$

This completes the proof of the theorem. □

Remark

Though it is unclear how many intermediate fields are between two fields, if we know a f.e. is finite and Galois, there are only finitely many subgroups of the Galois group and finitely many intermediate fields. So the theorem essentially allows us to transform a hard question (of infinite fields) into an easy question (of finite groups).

We have seen before that E/F is a finite Galois extension, and $L \in Int(E/F)$, then L/F is not always Galois. For example, $E = \mathbb{Q}(\sqrt[3]{2}), L = \mathbb{Q}(\sqrt[3]{2}), F = Q$, we have L/F is not Galois.

$$\begin{tikzcd}
E \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} = \mathrm{Gal}_E(E) \arrow[d, dash] \\
L \arrow[r, leftrightarrow] \arrow[d, dash] & L^* = \mathrm{Gal}_L(E) \arrow[d, dash] \\
F \arrow[r, leftrightarrow] & G = \mathrm{Gal}_F(E)
\end{tikzcd}$$

From the above picture, if L/F is Galois, we will see that it corresponds to the group G/L^*, which is well defined only if L^* is a normal subgroup of G.

Proposition (9.2.2.):
Let E/F be a finite Galois extension with $G = Gal_F(E)$. Let L be an intermediate field. For $\psi \in G$, we have

$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$

Proof: For any $\alpha \in \psi(L)$, we have $\psi^{-1}(\alpha) \in L$. If $\phi \in Gal_L(E)$, then

$$\phi\psi^{-1}(\alpha) = \psi^{-1}(\alpha)\ so\ \psi\phi\psi^{-1}(\alpha) = \alpha$$

It follows that

$$\psi\phi\psi^{-1} \in Gal_{\psi(L)}(E), \forall \phi \in Gal_L(E)$$

thus

$$\psi Gal_L(E)\psi^{-1} \subseteq Gal_{\psi(L)}(E)$$

since

$$|\psi Gal_L(E)\psi^{-1}| = |Gal_L(E)| = [E : L] = [E : \psi(L)] = |Gal_{\psi(L)}(E)|$$

The third inequality can be seen by considering the basis of E over L, it follows

$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$

□

The following theorem gives a criterion about when L/F is a Galois extension.

Theorem (9.2.3.):
Let $E/F, L, L^*$ be defined as in theorem 9.2.1. Then L/F is a Galois extension if and only if L^* is a normal subgroup of L. In this case

$$Gal_F(L) \cong G/L^*$$

Proof: Note that

$$\begin{aligned} L/F \text{ is normal } &\iff \psi(L) = L \text{ for all } \psi \in Gal_F(E) \\ &\iff Gal_{\psi(L)}(E) = Gal_L(E) \text{ for all } \psi \in Gal_F(E) \\ &\iff \psi Gal_L(E)\psi^{-1} = Gal_L(E) \text{ for all } \psi \in Gal_F(E),\ 9.2.2. \\ &\iff L^* = Gal_L(E) \text{ is a normal subgroup of } G \end{aligned}$$

If L/F is a Galois extension, the restriction map

$$G = Gal_F(E) \to Gal_F(E), \psi \mapsto \psi \mid_L$$

is well defined. Moreover, it is surjective and its kernel is $Gal_L(E) = L^*$. Thus

$$Gal_F(L) \cong G/L^*.$$

□

Example 1
For a prime p, let $q = p^n$. Consider the finite field $\mathbb{F}_q$ of q elements which is an extension of $\mathbb{F}_p$ of degree n. We have seen in Assignment 4 that Frobenius automorphism of $\mathbb{F}_q$ is defined by

$$\sigma_p : \mathbb{F}_q \to \mathbb{F}_q, \alpha \mapsto \alpha^p$$

For $\alpha \in \mathbb{F}_q$, we have

$$\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$$

So $\sigma_p^n = 1$. For $1 \leq m < n$, we have $\sigma_p^m(\alpha) = a^{p^m}$. Since the polynomial $x^{p^m} - x$ has at most p^m roots in $\mathbb{F}_q$, there exists $\alpha \in E$ such that $\alpha^{p^m} - \alpha \neq 0$. Thus, $\sigma_p^m \neq 1$. Hence σ_p has order n.
Let $G = Gal_{\mathbb{F}_p}(\mathbb{F}_q)$. It follows that

$$n = |\langle \sigma_p \rangle| \leq |G| = [\mathbb{F}_q : \mathbb{F}_p] = n$$

Thus,

$$G = \langle \sigma_p \rangle = \text{ a cyclic group order } n$$

Consider a subgroup H of G of order d, thus

$$d \mid n,\ [G : H] = \frac{n}{d}$$

By theorem 9.2.1, we have

$$\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_q^G] = [\mathbb{F}_q^H : \mathbb{F}_p]$$

Thus

$$H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{\frac{n}{d}}}$$

We have

$$\begin{tikzcd}
\mathbb{F}_q \arrow[r, leftrightarrow] \arrow[d, dash] & \{1\} \arrow[d, dash] & \\
H^* = \mathbb{F}_{p^{\frac{n}{d}}} \arrow[r, leftrightarrow] \arrow[d, dash] & H \arrow[d, dash] & |H| = d \\
\mathbb{F}_p \arrow[r, leftrightarrow] & G & |G| = n
\end{tikzcd}$$

Example 2

Let E be the splitting field of $x^5 - 7$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $E = \mathbb{Q}(\alpha, \zeta_5)$ with $\alpha = \sqrt[5]{7}$ and $\zeta_5 = e^{\frac{2\pi i}{5}}$. The minimal polynomials of α and ζ_5 over $\mathbb{Q}$ are $(x^5 - 7)$ and $(x^4 + x^3 + x^2 + x^1 + 1)$ respectively. So

$$\begin{tikzcd}
& E = \mathbb{Q}(\alpha, \zeta_5) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "5"'] & & \mathbb{Q}(\zeta_5) \arrow[dl, dash, "4"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$, are divisors of $[E : \mathbb{Q}]$, it shows that $[E : \mathbb{Q}]$ is divisible by 20. Thus, $[E : \mathbb{Q}(\zeta_5)] \geq 5$. Also, $E = \mathbb{Q}(\alpha, \zeta_5) = \mathbb{Q}(\zeta_5)(\alpha)$ and the minimal polynomial of α over $\mathbb{Q}(\zeta_5)$ divides $(x^5 - 7)$. Thus $[E : \mathbb{Q}(\zeta_5)] \leq 5$.
It follows that

$$[E : \mathbb{Q}(\zeta_5)] = 5 \implies [E : \mathbb{Q}] = 20$$

It follows that $G = Gal_{\mathbb{Q}}(E)$ is a group (subgroup of S_5 of order 20.)
For each $\psi \in G$, its action is determined by $\psi(\alpha)$ and $\psi(\zeta_5)$. We write $\psi = \psi_{k,s}$ if

$$\psi(\alpha) = \alpha\zeta_5^k, k \in \mathbb{Z}_5 \text{ and } \psi(\zeta_5) = \zeta_5^s, s \in \mathbb{Z}_5^*$$

Define

$$\sigma = \psi_{1,1} = \begin{cases} \alpha \mapsto \alpha\zeta_5 \\ \zeta_5 \mapsto \zeta_5 \end{cases} \quad \tau = \psi_{0,2} = \begin{cases} \alpha \mapsto \alpha \\ \zeta_5 \mapsto \zeta_5^2 \end{cases}$$

We check $\tau\sigma = \sigma^2\tau$, and we have

$$G = \langle \sigma, \tau \mid \sigma^5 = 1 = \tau^4, \tau\sigma = \sigma^2\tau \rangle$$

It follows that

$$G = \{\sigma^a\tau^b, a \in \{0, 1, 2, 3, 4\}, b \in \{0, 1, 2, 3\}\}$$

Since $|G| = 20$, by Lagranges theorem, the possible subgroups of G are of order $1, 2, 4, 5, 10, 20$.

We have $|G| = 20 = 4 \cdot 5$, let n_p be the number of Sylow p subgroups of G. By third sylow theorem, we have $n_2 \mid 5, n_2 \equiv 1 \mod 2$, so $n_2 = 1$ or 5. Also, we have $n_5 \mid 4$ and $n_5 \equiv 1 \mod 5$ so $n_5 = 1$. It follows G has unique sylow 5 subgroup, say P_5 of order 5. Since $\langle\sigma\rangle$ is a subgroup of order 5, we have $P_5 = \langle\sigma\rangle \cong \mathbb{Z}_5$. note that by second sylow theorem, $P_5 \triangleleft G$. Note that if $n_2 = 1$, then there is only one Sylow 2-group. Say $P_4 = \langle\gamma\rangle \cong \mathbb{Z}/\langle 4\rangle$. Then $P_4 \triangleleft G$. Since $|P_4 \cap P_5| = 1$, it follows

$$G \cong P_4 \times P_5 \cong \mathbb{Z}/\langle 4\rangle \times \mathbb{Z}/\langle 5\rangle \cong \mathbb{Z}/\langle 20\rangle$$

This contradicts the fact that G is not abelian. So there are actually 5 sylow 2 groups.
We have seen τ has order 4, thus the cylic group $\langle\tau\rangle$ is a Sylow 2 subgroup and all other sylow 2 groups are its conjugate. Note that since all elements of G are of the form $\sigma^a\tau^b$, we have

$$\sigma^a\tau^b\tau\tau^{-b}\sigma^{-a} = \sigma^a\tau\sigma^{-a}, a = \{0, 1, 2, 3, 4\}$$

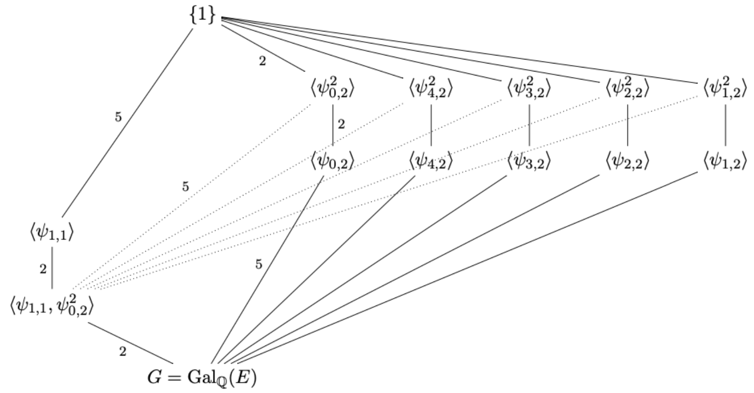
Using the fact $\tau\sigma = \sigma^2\tau$, we have

$$\langle\sigma^4\tau\sigma^{-4}\rangle = \langle\sigma^{-1}\tau\sigma\rangle = \langle\sigma\tau\rangle = \langle\phi_{1,2}\rangle$$

Using the same arguments we ssee the sylow 2 groups are $\langle\psi_{0,2}\rangle, \langle\psi_{1,2}\rangle, \langle\psi_{2,2}\rangle, \langle\psi_{3,2}\rangle, \langle\psi_{4,2}\rangle$. Moreover since a subgroup of G of order 2 are contained in a Sylow 2group,

$$\langle\psi_{0,2}^2\rangle, \langle\psi_{1,2}^2\rangle, \langle\psi_{2,2}^2\rangle, \langle\psi_{3,2}^2\rangle, \langle\psi_{4,2}^2\rangle$$

are all subgroups of G of order 2. For a subgroup H of G of order 10, since P_5 is the only subgroup of G of order 5, $H \supseteq P_5 = \langle\sigma\rangle$. So $\sigma^a\tau^b \in H$ if and only if $\tau^b \in H$. The only element of the form τ^b which is of order 2 is τ^2. So $H = \langle\sigma, \tau^2\rangle$.
Combining all arguments, we obtain the following diagram


$\{1\}$
$\langle\psi_{0,2}^2\rangle$
$\langle\psi_{4,2}^2\rangle$
$\langle\psi_{3,2}^2\rangle$
$\langle\psi_{2,2}^2\rangle$
$\langle\psi_{1,2}^2\rangle$
$\langle\psi_{0,2}\rangle$
$\langle\psi_{4,2}\rangle$
$\langle\psi_{3,2}\rangle$
$\langle\psi_{2,2}\rangle$
$\langle\psi_{1,2}\rangle$
$\langle\psi_{1,1}\rangle$
$\langle\psi_{1,1}, \psi_{0,2}^2\rangle$
$G = \mathrm{Gal}_{\mathbb{Q}}(E)$
2
5
2
5
2
5
2

For an intermediate field L of $E/\mathbb{Q}$, we consider $L^* = Gal_L(E)$. For example, $\mathbb{Q}(\zeta_5)$, note that $\psi_{1,1}(\zeta_5) = \zeta_5$. So $\mathbb{Q}(\zeta_5)^* \supseteq \langle\psi_{1,1}\rangle$. Since

$$|\langle\psi_{1,1}\rangle| = [\langle\psi_{1,1}\rangle : \{1\}] = 5$$

and

$$5 = [E; \mathbb{Q}(\zeta_5)] = [\mathbb{Q}(\zeta_5)^* : \{1\}]$$

we have

$$\mathbb{Q}(\zeta_5)^* = \langle\psi_{1,1}\rangle$$

Also,

$$\psi_{1,2}(\alpha\zeta_5^r) = \alpha\zeta_5\zeta_5^{2r} = \alpha\zeta_5^{2r+1}$$

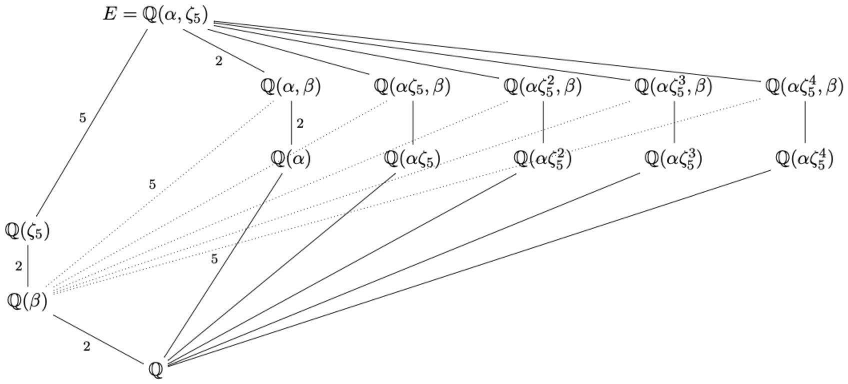
If $\psi_{1,2}$ fixes $\alpha\zeta_5^r$ then $r = 2r+1 \mod 5$ so $r \equiv 4 \mod 5$. So $\mathbb{Q}(\alpha\zeta_5^4)^* \supseteq \langle\psi_{1,2}\rangle$. Since

$$|\langle\psi_{1,2}\rangle| = [\langle\psi_{1,2}\rangle : \{1\}] = 4, [E : \mathbb{Q}(\alpha\zeta_5^4] = 4$$

thus

$$\mathbb{Q}(\alpha\zeta_5^4)^* = \langle\psi_{1,2}\rangle$$

Using the same argument, we can get $\langle\psi_{r,2}\rangle^*$ for $r \in \{0,1,2,3,4\}$. Consider $\beta = \zeta_5 + \zeta_5^{-1} \in \mathbb{R}$. We have $\beta^2+\beta-1 = 0$. Since $x^2+x-1 = 0$ has no rational root, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Similarly, $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] = 2$. So


$E = \mathbb{Q}(\alpha,\zeta_5)$
2
$\mathbb{Q}(\alpha,\beta)$
$\mathbb{Q}(\alpha\zeta_5,\beta)$
$\mathbb{Q}(\alpha\zeta_5^2,\beta)$
$\mathbb{Q}(\alpha\zeta_5^3,\beta)$
$\mathbb{Q}(\alpha\zeta_5^4,\beta)$
5
2
$\mathbb{Q}(\alpha)$
$\mathbb{Q}(\alpha\zeta_5)$
$\mathbb{Q}(\alpha\zeta_5^2)$
$\mathbb{Q}(\alpha\zeta_5^3)$
$\mathbb{Q}(\alpha\zeta_5^4)$
5
$\mathbb{Q}(\zeta_5)$
2
5
$\mathbb{Q}(\beta)$
2
$\mathbb{Q}$

Week 10. Cyclic extensions

Lemma (10.0.1 Dedekind's lemma):
Let K and L be fields and let $\psi_i : L \to K$ be distinct nonzero homomorphisms $(1 \le i \le n)$. If $c_i \in K$ and

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) + \ldots + c_n\psi_n(\alpha) = 0, \forall\alpha \in L$$

then $c_1 = c_2 = \ldots = c_n = 0$.

Theorem (10.0.2):
Let F be a field, $n \in \mathbb{N}$. Suppose $ch(F) = 0$ or p with $p \nmid n$. Assume also that $x^n - 1$ splits over F.

1. If the Galois extension E/F is cyclic of degree n, then $E = F(\alpha)$ for some $\alpha \in E$ with $\alpha^n \in F$. Particularly, $x^n - \alpha^n$ is minimal polynomial of α over F.
2. If $E = F(\alpha)$ with $\alpha^n \in F$, then E/F is a cyclic extension of degree d with $d \mid n$ and $\alpha^d \in F$. In particular, $x^d - \alpha^d$ is the minimal polynomial of α over F.

Theorem (10.0.3):
Let F be a field with $ch(F) = p$, where p is a prime.

1. If $x^p - x - a \in F[x]$, is irreducible, then its splitting field E/F is a cyclic extension of degree p.
2. If E/F is a cyclic extension of degree p, then E/F is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.

Week 11. Solvability by Radicals

11.1 Radical Extension

Definition 2.14: A finite extension E/F is radical if there exists a tower of fields

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}, 1 \leq i \leq m$.

Lemma 2.10 (11.1.1):
If E/F is a finite separable radical extension, then its normal closure N/F is also radical.

Remark
By Theorem 11.1.1., to consider a finite separable radical extension, we could instead consider its normal closure, which is Galois.

Definition 2.15 (Solvable by radicals): Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is solvable by radicals if there exists a racial extension E/F such that $f(x)$ splits over E.

Remark It is possible that $f(x) \in F[x]$ is solvable by radicals, but its splitting field is not a radical extension. (A11Q2.)
Remark We recall that an expression involving only $+, -, \times, /, \sqrt[n]{}$ is a radical. Let F be a field, $f(x) \in F[x]$ is separable. If $f(x)$ is solvable by radicals, by definition of radical extensions, $f(x)$ has a radical root. COnversely, if f has a radical root, it is inn some radical extension E/F, by the lemma 11.1.1, the normal closure N/F of E/F is radical. Since $f(x)$ splits over N/F, f is solvable by radicals.

11.2 Radical Solutions

Lemma 2.11 (11.2.1):
Let E/F be a field extension, K, L be intermediate fields of E/F. Suppose K/F is a finite Galois extension, then KL is a finite Galois extension of L and $Gal_L(KL)$ is isomorphic to a subgroup of $Gal_F(K)$.

Definition 2.16 (Galois group): E/F be splitting field of a separable polynomial $f(x) \in F[x]$. The Galois group of $f(x)$ is defined to be $Gal_F(E)$, denoted by $Gal(f)$.

Theorem 2.12 (11.2.2):
Let F be a field with $ch(F) = 0$. $f(x) \in F[x] \setminus \{0\}$. Then $f(x)$ is solvable by radicals if and only if its Galois group $Gal(f)$ is solvable,

Proposition 2.13 (11.2.2):
Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. If $f(x)$ contains precisely two nonreal roots in $\mathbb{C}$ then $Gal(f) \cong S_p$.

Theorem 2.14 (The Abel Ruffini Theorem):
A general polynomial $f(x)$ with $deg(f) \geq 5$ is nor solvable by radicals.

The following is review material

Week 1.

Definitions

- Commutative ring with 1
- Field
- Integral domain
- Ideal
- Principal Ideal Domain
- Quotient ring
- Maximal ideal, prime ideal

Theorems

- Every subring of a field is an integral domain.
- First isomorphism theorem
- Every maximal ideal is prime. In PID, every prime ideal is maximal.
- In $\mathbb{Z}$, $\langle n\rangle$ is maximal $\iff$ n is prime. In $F[x]$, $\langle f(x)\rangle$ is maximal $\iff$ $f(x)$ is irreducible.
- I is an ideal of R, $R \neq I$, then
  1. I maximal $\iff$ R/I is a field
  2. I is prime $\iff$ R/I is ID
- Gauss' lemma for $\mathbb{Z}[x]$.
- Eisenstein's criterion for $\mathbb{Z}[x]$.
- Eisenstein's criterion for PID.

Observations and remarks

- Only ideals of a field F is $\{0\}$ and F
- Any ring homomorphism whose domain is a field is either injective or zero.

Week 2. Field extensions

Definitions

- Field extension
- Degree of a field extension: degree of E/F as a vector space
- Finite/ infinite field extension: refers to the degree
- $F[x], F(x)$ where the former is all polynomials (ring), and latter is all rational functions (field).
- $F[a], F(a)$ given finite extension, the former means smallest subring and latter means smallest subfield.
- α is algebraic/ transcendental over F: algebraic if there is a polynomial, not zero, such that α is a root. Otherwise transcendental
- Simple extension: $E = F(\alpha)$ for some $\alpha \in E$
- If R, R_1 are two rings that contain F, a ring homomorphism $\psi : R \to R_1$ is a F homomorphism if its restriction to F is identity.
- Minimal polynomial over field F: in the sense of 2.2.2.
- Algebraic and transcendental extensions: algebraic if every element in E is algebraic over F, transcendental otherise.
- Algebraic closure: given E/F, the algebraic closure is $\{\alpha \in E : [F(\alpha) : F] < \infty\}$.
- Algebraically closed: any algebraic extension is the field itself.

Theorems

- 2.1.1. $E/K, K/F$ finite extensions then E/F is finite with
$$[E : F] = [E : K][K : F]$$
- 2.2.1 Relationships between $F[a], F(a), F[x], F(x)$ for transcendental a.
$$F[a] \cong F[x], f(a) \cong f(x), F[a] \ncong F(a)$$
where $a \in E$, with extension E/F
- 2.2.2. If a is algebraic, there exists a unique monic irreducible polynomial $f \in F[x]$ such that there exists F isomorphism
$$\psi : F[x]/\langle p(x)\rangle \to F[\alpha], \psi(x) = \alpha$$
and $F[\alpha] = F(\alpha)$.
- 2.2.3. Let E/F be a field extension, $\alpha \in E$. Then:
  1. α is transcendental over $F \iff [F(\alpha) : F] = \infty$
  2. α is algebraic over $F \iff [F(\alpha) : F] < \infty$
  3. If $p(x)$ is the minimal polynomial of α over F, then $[F(\alpha) : F] = deg(p)$ and $\{1, \alpha, \dots, \alpha^{deg(p)-1}\}$ is a basis for $[F(\alpha) : F]$
- 2.2.4 Given a finite extension, we can always write it as a chain of simple extensions. That is, if E/F is finite, $[E : F] < \infty$, exists $\alpha_1, \dots, \alpha_n \in E$ such that
$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \dots \subsetneq F(\alpha_1, \dots, \alpha_n) = E$$

- 2.2.5. Finite extensions are algebraic.

- 2.2.6. Algebraic closure is an intermediate field.

Observations and remarks

- Converse of 2.2.5 is false. The algebraic extension $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C}, \alpha \text{ is algebraic over } \mathbb{Q}\}$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Since any $\zeta_p \in \overline{\mathbb{Q}}$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] > [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Week 3

Definitions

- Given E/F a field extension. $f(x) \in F[x]$ splits over E.
- E is a splitting field of $f(x) \in F[x]$.
- Extending homomorphism

Theorems

- 3.1.1. Let $p(x) \in F[x]$ be irreducible. Then $F[x]/\langle p(x)\rangle$ is a field containing F and a root of $f(x)$.
- 3.1.2. Let $f(x) \in F[x]$. There exists a field $E \supseteq F$ such that $f(x)$ splits over E.
- 3.1.3. Every $f(x) \in F[x]$ has a splitting field, which is a finite extension of F.
- 3.2.1. Given F, F_1, an iso $\phi : F \to F_1$, let Φ be extended homomorphism. Given $f(x) \in F[x], f_1(x) \in F_1[x]$, let $E/F, E_1/F_1$ be splitting field of f, f_1 respectively, then there exists $\psi : E \to E_1$ that extends ϕ.

$$\begin{tikzcd}
\boldsymbol{E} \arrow[r, "\psi"] \arrow[d, "\supseteq"] & \boldsymbol{E_1} \arrow[d, "\supseteq"] \\
\boldsymbol{F} \arrow[r, "\phi"] \arrow[d] & \boldsymbol{F_1} \arrow[d] \\
\boldsymbol{F[x]} \arrow[r, "\Phi"] & \boldsymbol{F_1[x]}
\end{tikzcd}$$

- 3.2.2. Any two splitting fields of $f(x) \in F[x]$ over F are $F-$isomorphic.
- 3.3.1. Let F be field and $f(x) \in F[x], deg(f) = n \geq 1$. If E/F is the splitting field of f then $[E : F] \mid n!$.
- $A3Q1$: the number of such ψ in 3.2.1. is $\leq [E : F]$.
- $A3Q2$: $\mathbb{C}$ is not the splitting field of some polynomial over $\mathbb{Q}$.

Week 4

Definitions

- The prime field of a field F: intersection of all its subfields.
- Characteristic of a field
- The formal derivative: $D(f) = f'$ as a linear operator.
- Repeated root
- Irreducible polynomial being separable
- General polynomial being separable.
- A field is perfect if every irreducible polynomial is separable.

Theorems

- 4.1.1. The prime field of a field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p, p$ prime.
- 4.1.2. Let F be a field with $ch(F) = p$ and let $n \in \mathbb{N}$. The map $\psi : F \to F$ given by $u \mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$ homomorphism of fields. If F is finite, then ψ is a $\mathbb{Z}_p$ isomorphism of F.
- 4.2.1. Let F be a field and $f(x) \in F[x]$.
  - If $ch(F) = 0$, then $f'(x) = 0$ if and only if $f(x) = c, c \in F$
  - If $ch(F) = p$, then $f'(x) = 0$ if and only if $f(x) = g(x^p), g \in F[x]$.
- 4.2.2. Given E/F a field extension, α is a repeated root of $f(x) \iff (x - \alpha) \mid gcd(f, f')$.
- 4.2.3. $f(x) \in F[x]$ has no repeated roots in any extension if and only if $gcd(f, f') = 1$.
- 4.3.1. If F is a finite field, then $ch(F) = p$ for some prime p and $|F| = p^n, n \in \mathbb{N}$.
- 4.3.2. Let F be a field, G a finite subgroup of F^*. Then G is a cyclic group. If F is finite, then F^* is cyclic.
- 4.3.3. If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$.
- 4.3.4. Let p be a prime, $n \in \mathbb{N}$.
  1. F is a finite field with $|F| = p^n \iff F$ is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.
  2. Let F be a finite field with $|F| = p^n$. Let $m \in \mathbb{N}, m \mid n$, then F contains a subfield K with $|K| = p^m$.
- 4.3.5. Let p be a prime, $n \in \mathbb{N}$. Any two finite fields are p^n isomorphic. We denote it by $\mathbb{F}_{p^n}$.
- 4.4.1. Let F is a field
  1. If $ch(F) = 0$, then F is perfect
  2. If $ch(F) = p$, and $F^p = F$, F is perfect.
- 4.4.2. Every finite field is perfect.
- A4Q1: Let F be a field with $ch(F) = p$. Consider the Frobenius map ϕ of F, defined by $\psi(x) = x^p$. Then
  - ψ is an injective field homomorphism

    - If F is finite, then ψ is automorphism.
    - If F is not finite, then ψ might not be surjective.

- A4Q2: $g(x)$ is irreducible polynomial over $\mathbb{F}_p$, $g(x)$ divides $x^{p^n} - x$. Prove $\deg(g(x)) \mid n$.

Observations and remarks

- With $Ch(F) = p$, given $a, b \in F$, we always have $(a+b)^p = a^p + b^p$
- Consider the polynomial $f(x) = x^n - a \in F[x], n \geq 2$. If $a = 0$, the only irreducible factor is x. Since $gcd(x, x') = 1$, it is separable. Now assume $a \neq 0 . f'(x) = nx^{n-1}$ so the only irreducible factor of $f'(x)$ is x given $n \neq 0$.
    1. If $ch(F) = 0$, $gcd(f, f') = 1$, f is separable
    2. If $ch(F) = p$, $gcd(n, p) = 1$, f is separable
    3. If $ch(F) = 0$,
        (a) If $a \in F^p$, it is separable
        (b) If $a \notin F^p$, it is not separable. All roots of f are the same and it is purely inseparable.
- Regarding 4.4.1. If $ch(F) = p$, $F^p \neq F$, then taking $a \in F \setminus F^p$ we have $x^p - a$ is purely inseparable. So if $ch(F) = p$, F is perfect if and only if $F^p = F$.

Week 5 Part 1. Group Actions

Definitions

- Group action
- Stabilizer of a x, denoted G_x. The set of group elements that stabilize teh set element x.
- Centralizer and center are the concepts when the group is acting on itself.
- Centralizer of x, denoted G_x is the set of group elements such that g commutes with x.
- Center of G, denoted $Z(G)$, is the set of group elements that commutes with every group element.

Theorems

- The class equation.
$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$
where $x_i \in G \setminus Z(G)$, the orbits $G \cdot x_i = \{g x_i g^{-1} : g \in G\}$ are distinct conjugacy classes of G and $|G \cdot x_i| = [G : C_G(x_i)] > 1$ for each i.
- 5.1.1. Given prime p, let G be a group of order p^n which acts on a finite set S. Let
$$S_0 = \{x \in S : gx = x, \forall g \in G\}$$
Then we have $|S| \equiv |S_0| \pmod{p}$.
- 5.1.2. Let p be a prime and G a finite group. If $p \mid |G|$, G contains an element of order p.

Week 5 Part 2. Sylow Theorems

Definitions

- p-group: every element has order of a non-negative power of p.
- Given $H \leq G$, we have
$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$
is normalizer of H in G. particularly, $H \lhd N_G(H)$.
- Sylow $p-$subgroup: $P \leq G$ is a Sylow $p-$subgroup of G is P is a maximal $p-$group of G.

Theorems

- 5.2.1. A finite group G is a p-group if and only if $|G|$ is a power of p.
- 5.2.2. The center $Z(G)$ of a nontrivial finite p-group G contains more than one element.
- 5.2.3. If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.
- 5.2.4. H be a $p-$subgroup of a finite group G. If $p \mid [G : H]$ then $p \mid [N_G(H) : H]$ and $N_G(H) \neq H$.
- 5.2.5. (First Sylow Theorem)
Let G be a group of order $p^n m$, where p is a prime and $n \geq 1, \gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$. Moreover, every subgroup of G of order $p^i, i < n$ is normal in some subgroup of order p^{i+1}.

- 5.2.6. Let G be a group of order $p^n m$, where p is a prime. $n \geq 1, gcd(n, m) = 1$. Let H be a $p-$subgroup of G.
  1. H is a sylow $p-$subgroup if and only if $|H| = p^n$
  2. Every conjugate of a Sylow p-subgroup is a sylow $p-$subgroup.
  3. If there is only one Sylow $p-$subgroup P, then $P \lhd G$.
- 5.2.7. Second Sylow Theorem

  If H is a $p-$subgroup of a finite group G, and P is any Sylow $p-$subgroup of G, then there exist $g \in G$ such that $H \subseteq gPg^{-1}$. In particular any two Sylow $p-$subgroups of G are conjugate.
- 5.2.8. Third Sylow Theorem

  If G is a finite group and P a prime, $p \mid |G|$, then the number of Sylow $p-$subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$.
- A5Q1 G be finite group, $|G| = pq$, primes, $p > q$. If $p \not\equiv 1 \mod q$ then $g \cong \mathbb{Z}/\langle pq \rangle$.
- A5Q2 G be a group $|G| = p^2$, p prime, then G is abelian, either $G \cong \mathbb{Z}/\langle p^2 \rangle$ or $G \cong \mathbb{Z}/\langle p \rangle \times \mathbb{Z}/\langle p \rangle$.
- A5Q2. p, q primes, there are no simple groups of order pq.

Observations and remarks

- If $|G| = p^r m, gcd(p, m) = 1$ and n_p the number of Sylow p-subgroups of G, we have by third sylow theorem $n_p \mid p^r m$ and $n_p \equiv 1 \mod p$. Since $p \nmid n_p, n_p \mid m$.

Week 6

Definitions

- A solvable group: tower of normal subgroup and abelian quotient.
- Simple group

Theorems

- Recall the second and third isomorphism theorems.
- 6.0.1. G is solvable, then
  - If H is a subgroup of G, then H is solvable
  - N a normal subgroup of G, then G/N is solvable.
- 6.0.2. $N \triangleleft G$. If N, G/N are solvable then G is solvable. I.e. direct product of finitely many solvable groups is solvable.
- 6.0.3. If G is a finite solvable group, we can write the tower such that each quotient is cyclic, and even each quotient is of prime order.
- $A6Q1$ If H, K are solvable subgroups of G, $K \triangleleft G$, then HK is solvable.

Observations and remarks

- S_4 is solvable. For any $n \geq 5, S_n$ is not solvable.
- A_5 is not solvable, by this reasoning, S_5 is not solvable. So S_n is not solvable for $n \geq 5$.

Week7
Definitions

- Given E/F, and $\phi : E \to E$, ϕ is an F-automorphism
- The automorphism group of $E/F, Aut_F(E)$
- Given F field and $f(x) \in F[x]$. The automorphism group of $f(x)$ over F.
- Given E/F, $\phi \in Aut_F(E)$, Then E^{ϕ} is the fised field of ϕ.
- Given $G \subseteq Aut_F(E)$, what is the fixed field of G.

Theorems

- 7.1.1. Let E/F be field extension, $f(x) \in F[x]$, $\phi \in Aut_F(E)$. If $\alpha \in E$ is a root of $f(x)$, so is $\phi(\alpha)$.
- 7.1.2. Let $E = F(\alpha_1, \ldots, \alpha_n)$ be a field extension of F. If $\psi_1, \psi_2 \in Aut_F(E)$, we have $\psi_1(\alpha_i) = \psi_2(\alpha_i), \forall 1 \leq i \leq n$. Then $\psi_1 = \psi_2$.
- 7.1.3. If E/F is finite extension, so is $Aut_F(E)$ a finite group.
- 7.2.1. E/F be the splitting field of a nonzero polynomial $f(x) \in F[x]$. We have $|Aut_F(E)| \leq [E : F]$. Equality holds if and only if $f(x)$ is separable.
- 7.2.2. If $f(x) \in F[x]$ has n distinct roots in splitting field of E. Then $Aut_F(E)$ is isomorphic to a subgroup of S_n. $|Aut_F(E)| \mid n!$
- 7.3.1. $f(x) \in F[x]$ separapble, and E/F be its splitting field. If $G = Aut_F(E)$, then $E^G = F$.
- A7Q2: relationship between $\mathbb{F}_p(t)$ and $\mathbb{F}_p(t^p)$

Observations and remarks

- Converse of 7.1.3. is false. That is, $\mathbb{R}/\mathbb{Q}$ is infinite but $Aut_{\mathbb{Q}}(\mathbb{R}) = \{1\}$.

Week 8

Definitions

- Given an algebraic field extension E/F, we say $\alpha \in E$ is separable over F if minimal polynomial is. We say the extension is separable if all elements in E is separable.
- Primitive element of $E/F : \gamma$ such that $E = F(\gamma)$.
- Normal extension
- Normal closure

Theorems

- 8.1.1. Let E/F be splitting field of $f(x) \in F[x]$. If $f(x)$ is separable, E/F is separable. That is, splitting fields of separable polynomials are separable.
- 8.1.2. Let E/F be a finite extension, $E = F(\alpha_1, \dots, \alpha_n)$. If each α_i is separable over F then so is E/F.
- 8.1.3. Let E/F be an algebraic extension, L the set of all $\alpha \in E$ separable over F. Then L is an intermediate field.
- 8.1.4. Primitive element theorem. Finite separable extensions are of the form $F(\gamma)$. If $ch(F) = 0$, then any finite extension E/F is a simple extension.
- 8.2.1. A finite extension E/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.
- 8.2.2. If E/F is a normal extension, K intermediate field, then E/K is normal.
- 8.2.3. Let E/F be finite normal extension, $\alpha, \beta \in E$. TFAE:
  - Exists $\psi \in Aut_F(E)$ s.t. $\psi(\alpha) = \beta$
  - The minimal polynomials of α, β over F are the same.

  We say they are conjugates, in this case.
- 8.2.4. Every finite extension E/F has a normal closure N/F which is unique up to $E-$isomorphism.
- A8Q1: there is a finite extension that is not simple.
- A8Q2: Let E/F be a field extension and K, L two intermediate fields. Let KL be the compositum of K and L, i.e. the smallest field that contains K and L. Prove that if K/F and L/F are finite normal extensions, then KL/F is also a finite normal extension.

Observations and remarks

- If $ch(F) = 0$, the field is perfect and every polynomial is separable, hence any algebraic extension E/F is separable.
- Every quadratic extension is normal
- $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal.
- Composition of two normal extensions are not always normal.
- In prop 8.2.2., K/F is not always normal.

Week 9

Definitions

- Galois extension (only for algebraic extensions)
- Galois group
- Abelian, cyclic, solvable extensions
- Elementary symmetric functions

Theorems

- 9.1.1. (E.Artin). Let E be a field and G a finite subgroup of $Aut(E)$. Let E^G be E's elements fixed by all automorphisms in the group. Then E/E^G is a finite Galois extension and $Gal_{E^G}(E) = G$.
$$[E : E^G] = |G|$$
- 9.2.1. Fundamental Theorem of Galois Theory

  Let E/F be a finite Galois extension, $G = Gal_F(E)$. Then there is an order reversing bijection between intermediate fields of E/F and subgroups of G.
$$Int(E/F) \to Sub(G), L \mapsto L^* = Gal_L(E)$$
$$Sub(G) \to Int(E/F), H \mapsto H^* = E^H$$
  have: $L_1, L_2 \in Int(E/F), L_2 \subseteq L_1$ $H_1, H_2 \in Sub(G)$ $H_2 \subseteq H_1$, we have
$$[L_1 : L_2] = [L_2^* : L_1^*], [H_1 : H_2] = [H_2^* : H_1^*]$$
- 9.2.2. Let E/F be a finite Galois extension, $G = Gal_F(E)$, let L bea n intermediate field. Then for $\psi \in G$,
$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$
- 9.2.3. $E/F, L, L^*$ defined in 9.2.1. Then L/F is a Galois extension if and only if L^* is a normal subgroup of G. In this case, $Gal_F(L) \cong G/L^*$.
- A9: determine if various field extensions are Galois.

Observations and remarks

- Consider 8.1.1. If E is the splitting field of some $f(x) \in F[x]$, then we have $\iff$ in theorem 8.1.1.
- By 8.1.1.,8.1.2., a finite Galois extension is equivalent to the splitting field of a separable polynomial.
- Given finite Galois extension, 7.2.1. imply $|Gal_F(E)| = [E : F]$
- If E/F is splitting field of a separable polynomial degree n, then 7.2.2. imply $Gal_F(E)$ is a subgroup of S_n.
- Let E be a field, G a finite subgroup of $Aut(E)$, for $\alpha \in E$, consider the G orbit of α, $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$. Then the minimal polynomial of α over E^G is $(x - \alpha_1) \dots (x - \alpha_m) \in E^G[x]$.
- Consider $E = F(t_1, t_2, \dots, t_n)$ be function field in n variable $t_1, t_2, \dots, t_n$ over field F. Then $E^G = F(s_1, \dots, s_n)$ with degree $n!$.
- There are corresponding analysis for groups corresponding the Frobenius auromorphism and the splitting field of polynomial.

Week 10

Theorems

- 10.0.1. (Dedekind's lemma)

  Given K, L, fields. Let $\psi_i : L \to K$ be distinct nonzero homomorphisms. If $c_i \in K$, and $\sum_i c_i \psi(i)(\alpha) = 0$ for all $\alpha \in L$, then $c_1 = \ldots = c_n = 0$.

- 10.0.2. Let F be a field $n \in \mathbb{N}$. Suppose $ch(F) = 0$, or $p, p \nmid n$, then assume $x^n - 1$ splits over F.

  1. If the Galois extension E/F is cyclic of degree n, then $E = F(\alpha)$ for some $\alpha \in E, \alpha^n \in F$. In particular, $x^n - \alpha^n$ is the minimal polynomial of α over F.
  2. If $E = F(\alpha)$ with $\alpha^n \in F$, then E/F is a cyclic extension of degree d, $d \mid n, \alpha^d \in F$. In particular, $x^d - \alpha^d$ is the minimal polynomial of α over F.

- 10.0.3. Let F be a field, $ch(F) = p$, p is a prime.
  1. If $x^p - x - \alpha \in F[x]$ is irreducible, then its splitting field E/F is a cyclic extension of degree p.
  2. If E/F is a cyclic extension of degree p, then E/F is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.

- A10: construct cyclic Galois extension whos degree is k, where $2k + 1$ is prime.

- Field lattice and galois group correspondence of a certain Galois extension.

Week 11

Definitions

- Radical extension: existence of a tower of fields such that the adjacent ones have the form $F_i = F_{i-1}(\alpha_i)$, $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$.
- Given field F, $f(x) \in F[x]$, then $f(x)$ is solvable by radicals if... it splits over a radical extension of F.
- Galois group of a polynomial $f(x)$ where E/F is the splitting field of a separable polynomial $f(x)$.

Theorems

- 11.1.1. If E/F is a finite separable radical extension, then its normal closure N/F is also radical.
- 11.2.1. Let E/F be a field extension, K, L intermediate fields of E/F. Suppose K/F is a finite Galois extension. Then KL is also a finite Galois extension of L. $Gal_L(KL)$ is isomorphic to a subgroup of $Gal_F(K)$.
- 11.2.2. Let F be a field, $ch(F) = 0, f(x) \in F[x] \setminus \{0\}$. Then $f(x)$ is solvable by radicals if and only if $Gal(f)$ is solvable.
- 11.2.3. Let $f(x) \in \mathbb{Q}[x]$ be irreducible polynomial of prime degree p. If $f(x)$ contains precisely two nonreal roots in $\mathbb{C}$ then $Gal(f) \cong S_p$.
- 11.2.4. (Abel-Ruffini Theorem)

  A general polynomial $f(x)$ with $deg(f) \geq 5$ is not solvable by radicals.
- A11Q1: determine if a quintic is solvable by radical
- Note that is is possible that a polynomial is solvable by radicals but its splitting field is not a radical extension.

Observations and remarks

- To consider a finite separable radical extension, we could instead consider its normal closure, which is Galois.
- It is possible that a polynomial is solvable by radicals, but its splitting field is not a radical extension.
- An expression involving only $+, -, /, *, \sqrt{\cdot}$ is a radical.
- Given a separable polynomial, if it is solvable by radicals, then it has a radical root.
- Given a separable polynomial, if it has a radical root, by lemma 11.1.1. , f is solvable by radicals.
-

Template
Definitions

-

Theorems

-

Observations and remarks

-