MATH 8510 Galois Theory

LU Junyu

Winter 2021

Contents

Week 1

1.1 Review on polynomial rings

Let's agree on some facts and conventions from elementary abstract algebra, in particular those with polynomial rings before we dig into Galois theory.

A ring is always commutative with multiplicative identity 1 unless otherwise stated. R^* is the multiplicative group of units in R and $R^\times = R \setminus \{0\}$. We can use these two notations interchangeably when R is a field.

Let F be a field. A polynomial ring $F[X]$ with an indeterminate X is an F-vector space with basis $1, X, X^2, \cdots, X^n, \cdots$, with the multiplication

$$(\sum_i a_i X^i)(\sum_j b_j X^j) = \sum_k (\sum_{i+j=k} a_i b_j) X^k,$$

where X^0 is defined to be 1. Alternatively, we can identify $R[X]$ with

$$R^{(\mathbb{N})} = \{(a_i)_{i\in\mathbb{N}} : a_i \in R, a_i = 0 \text{ for all but finitely many } i \in \mathbb{N}\}$$

in an obvious way. But usually, we want to say R embeds into $R[X]$ although the most formal way is to identify R with a subring of $R[X]$. We will also use notations like $F[x], k[x]$ and $k[X]$ for polynomial rings as long as there is no confusion.

The degree function has the following properties:

1. $\deg(f+g) \leq \max(\deg f, \deg g)$,
2. $\deg(fg) = \deg f + \deg g$.

There are plenty results by arguing over the degree of a polynomial. We have $(R[X])^* = R^*$ if R is an integral domain. We have the division algorithm on $R[X]$.

Theorem 1.1.1. *Let F be a commutative ring. Then $F[X]$ is a PID if and only if F is a field.*

Hence or otherwise, $\mathbb{Z}[X]$ is not a PID. Indeed, $\langle 2, X\rangle$ is an example of an ideal that cannot be generated by a single polynomial. $K[X, Y]$ is not a PID as $\langle X, Y\rangle$ is not principal.

Theorem 1.1.2. *An ideal in a PID is prime if and only if it is maximal.*

Definition 1.1.3. If $f(X) \in F[X]$ where F is a field, then a *root* of f in F is an element $\alpha \in F$ such that $f(\alpha) = 0$.

Given a polynomial $f[X] \in F[X]$ and any $u \in F$, the division algorithm give us:

$$f(X) = q(X)(X - u) + f(u).$$

And lying in the center of proving that every finite subgroup of $F^\times$ is cyclic is counting the roots of polynomial $X^n - 1$.

Theorem 1.1.4. *Let F be a field and $f[X] \in F[X]$ a polynomial of degree n. Then f has at most n roots.*

Definition 1.1.5. Let F be a field. A nonzero polynomial $p(X) \in F[X]$ is said to be *irreducible* over F (or *irreducible* in $F[X]$) if $\deg p \geq 1$ and there is no factorization $p = fg$ in $F[X]$ with $\deg f < \deg p$ and $\deg g < \deg p$.

A quadratic or cubic polynomial is irreducible in $F[X]$ if and only if it has no root in F.

Theorem 1.1.6 (Gauss's Lemma)**.** *A polynomial $f(X) \in \mathbb{Z}[X]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[X]$.*

Theorem 1.1.7 (Eisenstein's Criterion)**.** *Let $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ be a polynomial over integers with $a_n \neq 0$. Suppose that there exists a prime p such that*

1. *$p \nmid a_n$,*
2. *$p \mid a_i$ for $i = 0, 1, \cdots, n-1$,*
3. *$p^2 \nmid a_0$.*

Then $f(X)$ is irreducible in $\mathbb{Z}[X]$.

A typical application of Eisenstein's Criterion is to prove the irreducibility of the p-th cyclotomic polynomial $\Phi_p(X) = \frac{X^p-1}{X-1}$, where p is a prime. The idea is to apply the criterion to $\Phi(X + 1)$.

Theorem 1.1.8. *Let F be a field and $f(X)$ a polynomial in $F[X]$. Then $(f(X))$ is a prime ideal in $F[X]$ if and only if $f(X)$ is irreducible. Equivalently, f is irreducible if and only if $F[X]/(f)$ is a field.*

Theorem 1.1.9. *Any ring homomorphism between two fields is injective.*

One sentence proof: there is no non-trivial proper ideal in a field.

1.2 Extensions of Fields

Most of this course will involve studying fields relative to certain subfield which we feel we understand better. For example, if $\alpha \in \mathbb{C}$ is the root of some polynomial with coefficients in $\mathbb{Q}$, we might wish to study $\mathbb{Q}(\alpha)$, the smallest subfield of $\mathbb{C}$ containing α and all of $\mathbb{Q}$. Certainly, if we want to understand how "complicated" the number α is, it makes sense to consider how "complicated" the field $\mathbb{Q}(\alpha)$ is as an extension of $\mathbb{Q}$. If $F \subset E$ are fields, we will denote the extension by E/F (this just means that F is a subfield of E, and that we're considering E relative to F, in particular, E/F is not a quotient or anything too formal). Note that often we will consider E to be an extension of F even if $F \nsubseteq E$, as long as there is an obvious embedding of F into E (an embedding is a homomorphism with is injective).

We will make a lot of use of the observation that if E/F is an extension of fields, then we may view E as a vector space over F.

Definition 1.2.1. Let E/F be an extension of fields. We say that E is a *finite extension* of F if E is finite-dimensional as a vector space over F. In this case we denote the dimension by $[E : F]$. We say that E is an *infinite extension* of F if E is infinite-dimensional as a vector space over F, and we write $[E : F] = \infty$.

Example 1.2.2. $\{1, i\}$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$. So $\mathbb{C}$ is a finite extension of $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.

Example 1.2.3. It is widely known that $\sqrt{2} \notin \mathbb{Q}$. Thus $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$. On the other hand $(\sqrt{2})^2 \in \mathbb{Q}$ and then any polynomial in $\sqrt{2}$ with rational coefficients is just a $\mathbb{Q}$-linear combinations of 1 and $\sqrt{2}$. Since

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$

every rational function of $\sqrt{2}$ can be written as a $\mathbb{Q}$-linear combinations of 1 and $\sqrt{2}$. It follows immediately that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ and $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Example 1.2.4. We can show $[\mathbb{C}(x) : \mathbb{C}] = \infty$ by arguing $\{1, x, x^2, \cdots\}$ is a linear independent set.

Example 1.2.5. To show $[\mathbb{R} : \mathbb{Q}] = \infty$, we make use of the unique factorization theorem of integers and argue that $\{\ln(p) : p \text{ is a prime}\}$ is a linearly independent set.

Theorem 1.2.6. *Let $K \subseteq F \subseteq E$ be fields. Then E/K is a finite extensions if and only if both F/K and E/F are, and when this is the case, we have*

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

Sketch of proof. If $\{a_i\}$ and $\{b_j\}$ are bases for E/F and F/K respectively, then $\{a_i b_j\}$ is a basis for E/K. □

Example 1.2.7. Consider field extensions $\mathbb{Q} \subset E = \mathbb{Q}[\sqrt{2}] \subset F = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. We already know $[E : \mathbb{Q}] = 2$ and since $\sqrt{3} \notin E$ and it is a root of $x^2 - 3 \in E[x]$ (so $1, \sqrt{3}$ form a E-basis of F), we also have $[F : E] = [E[\sqrt{3}] : E] = 2$. And then $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$.

Definition 1.2.8. Let E/F be a field extension. An element $\alpha \in E$ is *algebraic* over F if there is a non-zero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise we say that α is *transcendental* over F. The extension E/F is *algebraic* if every element of E is algebraic over F, and is *transcendental* otherwise.

Example 1.2.9. Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ as they are roots of $x^2 - 2$ and $x^2 + 1$. But π and e are transcendental. As you can see, it's much easier to show that something is algebraic over a subfield than to show that it isn't (since to show that it is, one simply needs to exhibit a non-trivial polynomial relation). This shows that $\mathbb{R}/\mathbb{Q}$ is a transcendental extension, but some more work is required to show that $\mathbb{Q}(\sqrt{2})$ is algebraic, namely, we need to make sure that the smallest field containing $\mathbb{Q}$ and $\sqrt{2}$ doesn't somehow contain transcendental elements over $\mathbb{Q}$.

Theorem 1.2.10. *Let E/F be a finite extension of fields and α a non-zero element in E. Then we have the following:*

1. *α is algebraic;*

2. *there is a unique non-zero monic irreducible polynomial* $f(x) \in F[x]$ *such that* $f(\alpha) = 0$*, moreover,* $\deg(f) \leq [E : F]$*;*

3. *if* α *is a root of a polynomial* $g(x) \in F[x]$*, then* $f \mid g$*;*

4. *if* $I = (f)$*, then* $F[x]/I \cong F(\alpha)$*; indeed, there exists an isomorphism* $\phi : F[x]/I \to f(\alpha)$ *with* $\phi(x + I) = \alpha$ *and* $\phi(a + I) = a$ *for all* $a \in F$*;*

5. *if* α' *is another root of* f *(in* E*), then* $F(\alpha) \cong F(\alpha')$

Proof. Suppose that E/F is a finite extension and $\alpha \in E$. Consider the elements

$$1, \alpha, \alpha^2, \cdots, \alpha^{[E:F]} \in E.$$

Since there are $[E : F] + 1$ elements, they must be linearly dependent over F. Hence we can find $c_i \in F$ such that

$$c_o \cdot 1 + c_1\alpha + \cdots + c_{[E:F]}\alpha^{[E:F]} = 0.$$

In other words, α is a root of the (non-zero) polynomial

$$g(x) = \sum_{i=0}^{[E:F]} c_i x^i \in F[x].$$

And the degree of g is at most $[E : F]$.

Now consider the evaluation map

$$\varphi : F[x] \to E, f(x) \mapsto f(\alpha),$$

where one may consider it as the restriction of $e_\alpha : E[x] \to E$. Then $\ker(\varphi)$ is non-empty since g lies in it and then $\ker(\varphi) = (f(x))$ for some monic $f(x) \in F[x]$ since $F[x]$ is a PID. Any polynomial $g(x) \in F[x]$ with a root α belongs to the kernel and hense is divisible by $f(x)$. Clearly, $\deg f$ is no bigger than $\deg g$ and then no bigger than $[E : F]$. Since E is a field as well, $\mathrm{im}(\varphi)$ is a domain. So the kernel is a prime (hence maximal) ideal and therefore f is irreducible and $\mathrm{im}(\varphi)$ is a field containing $\mathbb{Q}$ and α indeed. ϕ is the canonical isomorphism induced by φ.

Finally , notice both $F(\alpha), F(\alpha')$ are isomorphic to $F[x]/I$. □

Definition 1.2.11. The polynomial f constructed in Theorem 1.2.10 is called the *minimal polynomial* of α over F.

Remark. In some textbook, the minimal polynomial is denoted by $\mathrm{irr}(\alpha, F)$.

In other words, in a finite extension, every element is the root of some polynomial over the smaller field. The next theorem is a partial converse to this, and we will use it often.

Theorem 1.2.12. *Let* k *be a field and* $f[x]$ *a monic irreducible polynomial in* $k[x]$ *of degree* d*. Let* $K = k[x]/I$*, where* $I = (f)$*, and* $\beta = x + I \in K$*. Then:*

1. K *is a field and* $k' = \{a + I : a \in k\}$ *is a subfield of* K *isomorphic to* k*,*

2. β *is a root of* f *in* K*,*

3. *if* $g(x) \in k[x]$ *and* β *is a root of* g *in* K*, then* $f \mid g$ *in* $k[x]$*,*

4. *f is the unique monic irreducible polynomial in $k[x]$ having β as a root,*

5. *$1, \beta, \beta^2, \cdots, \beta^{d-1}$ form a basis of K as a vector space over k and so $\dim_k(K) = d$.*

Proof. With the knowledge form the warm-up part, we can prove this theorem easily.

1. I is a prime ideal hence maximal since $F[x]$ is a PID. So the quotient ring $K = k[x]/I$ is a field. Every field homomorphism is injective and so k embeds into K with its image k'.

2. Let $f(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d$, where $a_i \in k$ for all i. In $K = k[x]/I$, we have

$$\begin{aligned} f\beta) &= (a_0 + I) + (a_1 + I)\beta + \cdots + (1 + I)\beta^d \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (1 + I)(x + I)^d \\ &= (a_0 + I) + (a_1 x + I) + \cdots + (x^d + I) \\ &= a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^d + I \\ &= f(x) + I = 0 + I. \end{aligned}$$

   So β is a root of p.

3. If $f \nmid g$ in $k[x]$, then their $\gcd$ is 1 since f is irreducible. Therefore, we can find polynomials s, t in $k[x]$ such that $1 = sf + gt$. Treating them as polynomials in $K[x]$ and evaluating at β, we get $1 = 0$, a contradiction.

4. Let g be a monic irreducible polynomial in $k[x]$having β as a root. Then by part (3) we have $f \mid g$. Since g is irreducible, we have $g = ch$ for some constant c. But both f, g are monic, we have $c = 1$ and $f = g$.

5. Every element of K has the form $g + I$, where $g(x) \in k[x]$. By the division algorithm, we have $g = qf + r$ with either $r = 0$ or $\deg(r) < \deg(f)$. Then $g + I = r + I$ since $g - r = qf \in I$. By the calculation similar in part (2), it follows that $r + I = b_0 + b_1\beta + \cdots + b_{d-1}\beta^{d-1}$ if we express $r(x) = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$.

   If $\{1, \beta, \beta^2, \cdots, \beta^{d-1}\}$ is not linearly independent, then we can find coefficients $c_i \in k$ not all zero such that

$$c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1} = 0.$$

   Define $g(x) \in k[x]$ by $f(x) = \sum_{i=0}^{d-1} c_i x^i$. Then $g(\beta) = 0$ and $\deg(g) \leq d - 1 < \deg(f) = d$. By part (3) says $\deg(f) \leq \deg(g)$ since $f \mid g$. We reach a contradiction.

□

Remark. The pair (K, β) is called the *stem field* (of f) in Milner.

Example 1.2.13. The polynomial $x^2 + 1 \in \mathbb{R}[x]$ is irreducible so $K = \mathbb{R}[x]/(x^2 + 1)$ is a finite extension of $\mathbb{R}$ with degree 2. If β is a root of $x^2 + 1$ in K, then $\beta^2 = -1$. Moreover, every element of K has a unique expression $a + b\beta$, where $a, b \in \mathbb{R}$.

Example 1.2.14. Let $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[X]$. This is an irreducible polynomial: it has no rational roots (if r/s in lowest form was one, then $r \mid 1$ and $r \mid 1$; the only possible rational root was

$r/s = \pm 1/1 = \pm 1$) and a direct factorization $f(x) = (x^2 + ax + b)(x^2 - ax + c)$ is also impossible. (One can show, however, f is reducible in $\mathbb{F}_p[x]$ for any prime p.) The roots of f are

$$\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}.$$

Let β be one of the roots. Consider the field extensions $\mathbb{Q} \subset \mathbb{Q}[\beta] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. We already know from pervious example

$$[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4 = [\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\beta]][\mathbb{Q}[\beta] : \mathbb{Q}].$$

But β is a root of irreducible polynomial of degree 4 and therefore

$$[\mathbb{Q}[\beta] : \mathbb{Q}] = 4.$$

We see that $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}[\beta]] = 1$ and then

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\beta].$$

And hence all roots of f lies in $\mathbb{Q}[\beta]$.

1.3 Automorphisms

When one is first introduced to the complex numbers, it is usually as a superset of the reals. We're introduced to $\mathbb{C}$ as a vector space over $\mathbb{R}$ with basis $\{1, i\}$ which happens to also admit the structure of a field. One function which helps with the very basic study of $\mathbb{C}$ from this perspective is the complex conjugation:

$$\overline{x + yi} = x - yi$$

for $x, y \in \mathbb{R}$. The important properties of this function are that it is an automorphism of $\mathbb{C}$ and that it fixes real numbers (and only real numbers. We would like to identify functions of this form for arbitrary field extensions.

Definition 1.3.1. Let F be a field, and let $X \subset F$ be a subset. Then $\varphi : F \to F$ is an automorphism if it is a bijection and a homomorphism, namely, $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$. We denote the group of automorphisms of F by $\mathrm{Aut}(F)$. We say that $\varphi \in \mathrm{Aut}(F)$ fixes X if $\varphi(x) = x$ for all $x \in X$, and we denote the set of automorphisms of F fixing X by $\mathrm{Aut}(F/X)$.

It's worth noting that this definition of fixing a set is what might more rightly be referred to as fixing X pointwise. It is sometimes useful to consider functions which fix X setwise, meaning that $\varphi(x) \in X$ for all $x \in X$. Unless otherwise stated, "fix" means "fix pointwise". Note that, in the lemma below, we make no special assumptions about the nature of $X \subset F$.

Proposition 1.3.2. *For any field F, and any set $X \subset F$, the set $\mathrm{Aut}(F/X)$ is a group under composition.*

Proof. Just straightforward verifications. □

Example 1.3.3. Consider $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$. Every element of $\mathbb{C}$ can be written as $x + yi$ with $x, y \in \mathbb{R}$. For any $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$, we must have $\sigma(x + yi) = x + y\sigma(i)$. Furthermore, we also have

$$-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2,$$

and hence $\sigma(i) = \pm i$. So $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ contains exactly two elements: the trivial one and the complex conjugation. It is clear that $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ is group — we need to check the complex conjugation is an automorphism of $\mathbb{C}$ and twice the complex conjugation is just the identity map.

This example gives us a feeling about how $\mathrm{Aut}(E/F)$ will be for a field extension E/F. In general, if E/F is a finite extension with $[E : F] = n$, then we can choose a basis $\alpha_1, \cdots, \alpha_n \in E$ for E/F. Any element of E can be written uniquely in the form

$$c_1\alpha_1 + \cdots + c_n\alpha_n,$$

with $c_i \in F$. If $\sigma \in \mathrm{Aut}(E/F)$, then we have

$$\sigma(c_1\alpha_1 + \cdots + c_n\alpha_n) = c_1\sigma(\alpha_1) + \cdots + c_n\sigma(\alpha_n).$$

In other words, the automorphism σ is entirely defined by the n values $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$. Moreover, if $f_i(x) \in F[x]$ is the minimal polynomial for α_i, then

$$f_i(\sigma(\alpha_i)) = \sigma(f_i(\alpha_i)) = \sigma(0) = 0.$$

So $\sigma(\alpha_i)$ is one of the (finitely many) roots of f_i in E. So there are only finitely many possible values for $\sigma(\alpha_i)$, for each i. We won't count how many automorphisms the can be (this will become easier later), but we've just made the following useful observation:

Theorem 1.3.4. *Let E/F be a finite extension of fields. Then Aut(E/F) is a finite group. Moreover, if we have $E = F(\alpha)$ for some $\alpha \in E$, then Aut(E/F) naturally embeds into the group of permutations of the roots of the minimal polynomial of α over F.*

Note that E/F does not need to be a finite extension for us to define $\mathrm{Aut}(E/F)$ (indeed, F need not even be a field).

Unfortunately, there are interesting extensions E/F for which the group $\mathrm{Aut}(E/F)$ is trivial and hence not interesting. Here is an example:

Example 1.3.5. Let α be the real cube root of 2, and let $E = \mathbb{Q}(\alpha)$. Then $[E : \mathbb{Q}] = 3$ (since the minimal polynomial of α, which is $f(x) = x^3 - 2$, is irreducible over $\mathbb{Q}$). Now suppose that $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$. We've seen that σ is entirely determined by $\sigma(\alpha)$. But $E \subset \mathbb{R}$, and $\sigma(\alpha)$ has to satisfy

$$\sigma(\alpha)^3 = \sigma(\alpha^3) = 2.$$

In particular, $\sigma(\alpha)$ is a real cube root of 2, and so the only possibility is $\sigma(\alpha) = \alpha$. In other words, the only element of $\mathrm{Aut}(E/\mathbb{Q})$ is the trivial element $\sigma(x) = x$ for all $x \in E$.

Example 1.3.6. We can show $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ is also trivial. Let $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. From the observation that

$$\sigma(a^2) = \sigma(a)^2 > 0,$$

we see σ must take positive to positive and hence order-preserving. And then it must be continuous (by more detailed arguments) but any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map (again you may fill the details if you want).

Our next example says something about finite fields. We do a quick catch-up here.

Recall there is a natural ring homomorphism $\pi : \mathbb{Z} \to F$ determined by $\pi(1) = 1_F$ for any field F. The image is a integral domain, hence $\ker(\pi)$ is trivial or is (p), where p is prime. We say the field is of characteristic 0 in former case and p latter. And the image is again a field — we call it the *prime field* of F.

We denote the finite field of order exactly p, where p is a prime, by $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$. If F be a finite field with q elements and suppose that $F \subset K$ where K is also a finite field. Then K (isomorphic to F^n as a vector space) has q^n elements where $n = [K : F]$ from the knowledge on finite field extensions. Hence a finite field is isomorphic to $\mathbb{F}_{p^n}$ where p is its characteristic and $n \in \mathbb{N}$.

Since $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$, we have $a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}$. The polynomial $x^{p^n} - x$ has at most $\deg = p^n$ roots and we conclude

$$x^{p^n} - x = \prod_{a \in \mathbb{F}_{p^n}} (x - a) \in \mathbb{F}_{p^n}[x], \tag{1.1}$$

in other words, $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$. However, we do not need this terminology yet at this stage.

On the other hand, by Theorem 1.2.12, we have the following proposition:

Proposition 1.3.7. *For a prime p and a monic irreducible $f(x)$ in $\mathbb{F}_p[x]$ of degree n, the ring $\mathbb{F}_p[x]/(f(x))$ is a field of order p^n.*

Example 1.3.8. Two fields of order 8 are $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$. Two fields of order 9 are $\mathbb{F}_3[x]/(x^2 + 1)$ and $\mathbb{F}_3[x]/(x^2 + x + 2)$.

Theorem 1.3.9. *Let $f(x) \in \mathbb{F}_p[X]$ be irreducible and of degree n. Then f has no repeated roots and f divides $X^{p^n} - X$. (Hence or otherwise, $X^{p^n} - X$ has a factorization $X^{p^n} - X = \prod_{d|n} \prod_{f_d} f_d$, where f_d runs over all irreducible polynomials of degree d.)*

Sketch of proof. Combining Equation 1.1 and Proposition 1.3.7, we know f and $X^{p^n} - X$ share a root. So f divides $X^{p^n} - X$ by Theorem 1.2.10. Moreover, $X^{p^n} - X$ has no repeated roots and so is f. □

Theorem 1.3.10. *Every finite field F is isomorphic to $\mathbb{F}_p[x]/(f)$ for some prime p and some irreducible polynomial $f(x) \in \mathbb{F}_p[x]$.*

Proof. Combining what we discussed just now, we have $|F| = p^n$ and an embedding $\mathbb{F}_p \hookrightarrow F$. $F^\times$ is cyclic, say, it is generated by α. Then f is the minimal polynomial of α over $\mathbb{F}_p$. □

Theorem 1.3.11. *Two finite fields E, F of the same size are isomorphic.*

Proof. Since $|E| = p^m$ and $|F| = q^n$, where p, q are primes and m, n positive integers, we must have $p = q$ and $m = n$. They are both isomorphic to $\mathbb{F}_{p^n}$. □

Example 1.3.12. Let p be a prime, and consider the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. We define a function $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by $\sigma(x) = x^p$. By the binomial theorem, and the fact that p divides the binomial coefficient $\binom{p}{j}$ for any $1 \leq j \leq p-1$, we have

$$\sigma(x + y) = (x + y)^p = x^p + y^p + p \cdot (\text{something}) = \sigma(x) + \sigma(y).$$

And of course $\sigma(xy) = \sigma(x)\sigma(y)$. So σ is a homomorphism. We wish to show that σ is an automorphism of $\mathbb{F}_{p^n}$. Since $\mathbb{F}_{p^n}$ is finite, we simply need to show that σ is either surjective or injective. We'll show that it's injective. To see this, suppose to the contrary that there's some non-zero $x \in \mathbb{F}_{p^n}$ with $\sigma(x) = 0$. Since the group of non-zero elements $\mathbb{F}_{p^n}$ is cyclic, say, generated by γ. If $x = \gamma^j$, then

$$x^{p^n} = (\gamma^j)^{p^n} = (\gamma^{p^n})^j = \gamma^j = x.$$

On the other hand,

$$x^{p^n} = \sigma^{(n)}(x) = \sigma^{n-1}(\sigma(x)) = \sigma^{(n-1)}(0) = 0,$$

where $\sigma^{(n)}$ means compose σ with itself n times. We reach a contradiction. Also, note that σ fixes $\mathbb{F}_p$, so really $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. It's possible to show that σ generates this group (laster).

σ is usually referred to as the *Frobenius homomorphism*.

Week 2

2.4 Algebraic Closure

Although we can get by with constructing fields like $\mathbb{Q}(i)$ as quotients:

$$\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2+1),$$

it is often useful to think of all of the possible algebraic extensions as being subfields of one large (infinite) extension.

Definition 2.4.1. A field F is said to be *algebraically closed* if every non-constant polynomial $f(x) \in F[x]$ has a root in F or, equivalently, if every polynomial in $F[x]$ factors as a product of linear terms. An *algebraic closure* of a field k is an algebraic extension $\overline{k}$ of k that is algebraically closed.

The Fundamental Theorem of Algebra says that $\mathbb{C}$ is algebraically closed; moreover, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. One may have seen a proof of Fundamental Theorem using fundamental group, but the simplest proof of the Fundamental Theorem is probably that using Liouville's Theorem in complex variables: every bounded entire function is constant.

Theorem 2.4.2. *Let F be a field. Then*

1. *there exists a field $\overline{F} \supset F$ which is algebraically closed and algebraic over F,*
2. *this field $\overline{F}$ is unique up to isomorphism.*

As you might guess, Zorn's lemma is inevitable in such kind proof. The problem is how to apply it.

One can imagine looking at the "set" of all algebraic extensions of F. This collection of fields is partially ordered under inclusion, and linearly ordered chains in the collection have least upper bounds (their union). If this were a set of fields, then it would follow form Zorn's Lemma that there is a maximal element, call it $\overline{F}$. This would be an algebraic extension of F: it would have no proper algebraic extension, and hence it would have to be algebraically closed. This is the algebraic closure of F. The problem with this argument is that the collection of algebraic extensions of F is too large to be a set, and hence one cannot apply Zorn's Lemma.

Lemma 2.4.3. *Let E/F be a field extension. If $\alpha_1, \cdots, \alpha_n \in E$ are algebraic over F, then $F(\alpha_1, \cdots, \alpha_n)$ is a finite extension over F.*

Proof. We can do induction on n. It is straightforward. □

Lemma 2.4.4. *If E is an algebraic extension of F and F is an algebraic extension of K then E is an algebraic extension of K.*

Proof. Take any non-zero element $\alpha \in E$. Since E/F is algebraic, there is a polynomial

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n \in F[x]$$

that has α as a root. By viewing $f(x)$ as an element in $K(c_0, \cdots, c_n)[x]$, we see that

$$K(\alpha, c_0, \cdots, c_n)/K(c_0, \cdots, c_n)$$

is a finite extension. But all the $c_i, i = 1, \cdots, n$ are in F hence algebraic over K,

$$K(c_0, \cdots, c_n)/K$$

is also a finite extension by Lemma 2.4.3. And so $K(\alpha, c_0, \cdots, c_n)/K$ is also a finite extension hence α is algebraic over K. □

Lemma 2.4.5. *Let k be a field, and let $k[T]$ be the polynomial ring in a set T of indeterminates (indeed, $|T|$ can be infinite). If $t_1, \cdots, t_n \in T$ are distinct, where $n \geq 2$, and $f_i(t_i) \in k[t_i] \subset k[T]$ are non-constant polynomials, then the ideal $I = (f_1(t_1), \cdots, f_n(t_n))$ in $k[T]$ is proper.*

Proof. If I is not a proper ideal in $k[T]$, then there exist $h_i(T) \in k[T]$ with

$$1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n).$$

Consider the extension field $k(\alpha_1, \cdots, \alpha_n)$, where α_i is a root of $f_i(t_i)$ for $i = 1, \cdots, n$ (the f_i are not constant. Denote the variables involved in the $h_i(T)$ other than $t_1, \cdots, t_n$, if any, by $t_{n+1}, \cdots, t_m$. Evaluating when $t_i = \alpha_i$ if $i \leq n$ and $t_i = 0$ if $i \geq n + 1$. The right side is 0, and we have the contradiction $1 = 0$. □

Proof of Theorem 2.4.2 part (1). Let T be a set in one-to-one correspondence with the family of non-constant monic polynomials in $k[x]$. (So T is a very very large set in general.) Let $R = k[T]$ be the big polynomial ring, and let I be the ideal in R generated by all elements of the form $f(t_f)$, where $t_f \in T$; that is, if

$$f(x) = x_n + a_{n-1}x^{n-1} + \cdots + a_0,$$

where $a_i \in k$, then

$$f(t_f) = (t_f)^n + a_{n-1}(t_f)^{n-1} + \cdots + a_0.$$

We claim that the ideal I is proper; if not, $1 \in I$, and there are distinct and finite! $t_1, \cdots, t_n \in T$ and polynomials $h_1(T), \cdots, h_n(T) \in k[T]$ with

$$1 = h_1(T)f_1(t_1) + \cdots + h_n(T)f_n(t_n),$$

contradicting Lemma 2.4.5. Therefore, there is a maximal ideal $\mathfrak{m}$ in R containing I. Define $K = R/\mathfrak{m}$. The proof is now completed in a series of steps.

1. K/k is an extension field.

   We know that $K = R/\mathfrak{m}$ is a field because $\mathfrak{m}$ is a maximal ideal. Let $i : k \to k[T]$ be the ring map taking $a \in k$ to the constant polynomial a, and let θ be the composite $k \to k[T] = R \to R/\mathfrak{m} = K$. Now θ is injective, (recall ring homomorphisms between fields are injective). We identify k with $\text{im}(\theta) \subset K$.

2. Every non-constant $f(x) \in k[x]$ has a root in $K[x]$, hence factors into linear terms in $K[x]$.

   By definition, for each $t_f \in T$, we have $f(t_f) \in I \subset \mathfrak{m}$, and so the coset $t_f + \mathfrak{m} \in R/\mathfrak{m} = K$ is a root of $f(x)$. By induction on the degree of f

3. The extension K/k is algebraic.

   It suffices to show that each $t_f + \mathfrak{m}$ is algebraic over k (for $K = k(\text{all } t_f + \mathfrak{m})$); but this is obvious, for t_f is a root of $f(x) \in k[x]$.

4. K is algebraically close.

   Let $\pi(x) \in K[x]$ be a monic irreducible polynomial and α one of the roots in some extension K'. Since both $K(\alpha)/K$ and K/k are algebraic, $K(\alpha)/k$ is also algebraic by Lemma 2.4.4. Hence α is a root of some polynomial in $k[x]$. But polynomials in $k[x]$ factors into linear terms in $K[X]$, we must have α lies in K as well.

□

Corollary 2.4.6. *If k is a countable field, then it has a countable algebraic closure. In particular, the algebraic closure of the prime fields $\mathbb{Q}$ and $\mathbb{F}_p$ are countable*

Proof. k is countable $\Longrightarrow$ T is countable $\Longrightarrow$ $k[T]$ is countable $\Longrightarrow$ $K = k[T]/\mathfrak{m}$ is countable. □

To prove the (non)uniqueness of a algebraic closure needs more work.

Definition 2.4.7. If F/k and K/k are extension fields, then a k-map is a ring homomorphism $\varphi : F \to K$ that fixes k pointwise.

Lemma 2.4.8. *If K/k is an algebraic extension, then every k-map $\varphi : K \to K$ is an automorphism of K.*

Proof. Since φ is a ring homomorphism between fields, φ is injective. To see that φ is surjective, let $a \in K$. Since K/k is algebraic, there is an irreducible polynomial $p(x) \in k[x]$ having a as a root. The k-map φ permutes the set A of all those roots of $p(x)$ that lie in K. Therefore, $a \in \varphi(A) \subset \text{im}(\varphi)$, since A is finite. □

Lemma 2.4.9. *Let k be a field and let K/k be an algebraic closure. If F/k is an algebraic extension, then there is an injective k-map $\psi : F \to K$. In particular, every k-map $F \to K$ extends to a k-map $K \to K$, which is an isomorphism indeed.*

If F is countably generated over k, namely, $F = k[\alpha_1, ..., \alpha_n]$, then we can extend the inclusion $\iota : k \to K$ to $k[\alpha_1]$, then to $k[\alpha_1, \alpha_2]$, and so on.

Proof. If E is an intermediate field, $k \subset E \subset F$, let us call an ordered pair (E, f) an approximation if $f : E \to K$ is a k-map. Define $X = \{\text{approximations } (E, f) : k \subset E \subset F\}$. Note that $X \neq \emptyset$ because $(k, i) \in X$. Partially order X by

$$(E, f) \preceq (E', f') \text{ if } E \subset E' \text{ and } f'|E = f.$$

That the restriction $f'|E$ is f means that f' extends f; that is, the two functions agree whenever possible: $f'(u) = f(u)$ for all $u \in E$.

It is easy to see that an upper bound of a chain

$$S = \{(E_j, f_j) : j \ \in J\}$$

is given by $(\cup E_j, \cup f_j)$. That E_j is an intermediate field is, by now, a routine argument. We can take the union of the graphs of the f_j, but here is a more down-to-earth description of $\varphi = \cup f_j$: if $u \in \cup E_j$, then $u \in E_{j_0}$ for some j_0, and $\varphi(u) = fj_0(u)$. Note that φ is well-defined: if $u \in E_{j_1}$, we may assume, for notation, that $E_{j_0} \subset E_{j_1}$, and then $f_{j_1}(u) = f_{j_0}(u)$ because f_{j_1} extends f_{j_0}. Observe that φ is a k-map because all the f_j are.

By Zorn's Lemma, there exists a maximal element (E_0, f_0) in X. We claim that $E_0 = F$, and this will complete the proof (take $\psi = f_0$). If $E_0 \subsetneq F$, then there is $a \in F$ with $a \notin E_0$. Since F/k is algebraic, we have F/E_0 algebraic, and there is an irreducible $p(x) \in E_0[x]$ having a as a root. Since K/k is algebraic and K is algebraically closed, we have a factorization in $K[x]$:

$$f_0^*(p(x)) = \prod_{i=1}^{n}(x - b_i),$$

where $f_0^* : E_0[x] \to K[x]$ is the map

$$f_0^* : e_0 + \cdots + e^n x^n \mapsto f_0(e_0) + \cdots + f_0(e^n)x^n.$$

If all the b_i lie in $f_0(E_0) \subset K$, then $f_0^{-1}(b_i) \in E_0 \subset F$ for some i, and there is a factorization of $p(x)$ in $F[x]$, namely, $p(x) = \prod_{i=1}^{n}[x - f_0^{-1}(b_i)]$. But $a \notin E_0$ implies $a \neq f_0^{-1}(b_i)$ for any i. Thus, $x - a$ is another factor of $p(x)$ in $F[x]$, contrary to unique factorization. We conclude that there is some $b_i \notin f_0(E_0)$. By Theorem 1.2.10, we may define $f_1 : E_0(a) \to K$ by

$$c_0 + c_1 a + c_2 a^2 + \cdots \mapsto f_0(c_0) + f_0(c_1)b_i + f_0(c_2)b_i^2 + \cdots .$$

A straightforward check shows that f_1 is a (well-defined) k-map extending f_0. Hence, $(E_0, f_0) \prec (E_0(a), f_1)$, contradicting the maximality of (E_0, f_0).

For the "in particular" part, note K/F is also algebraic and K is a algebraic closure of F as well. By previous lemma, such a k-map is an automorphism. □

Proof of Theorem 2.4.2 part (2). Let K and L be two algebraic closures of a field k. By Lemma 2.4.9, there are injective k-maps $\psi : K \to L$ and $\theta : L \to K$. By Lemma 2.4.8, both composites $\theta\psi : K \to K$ and $\psi\theta : L \to L$ are automorphisms. It follows that ψ (and θ) is a k-isomorphism. □

It is now permissible to speak of *the* algebraic closure of a field.

2.5 Splitting Fields

Most of the cases, the algebraic closure $\overline{k}$ of k is too big. We may want to a smaller but still big enough field extension E/k.

Definition 2.5.1. A *splitting field* of a non-constant polynomial $f(x) \in F[x]$ is a field extension E/F such that $f(x)$ factors into linear terms in $E[x]$, namely,

$$f(x) = c(x - \alpha_1)\cdots(x - \alpha_n),$$

and such that $E = F(\alpha_1, \cdots, \alpha_n)$.

This is, the splitting field is the smallest field (unique up to isomorphism) extension containing all the roots of $f(x)$. If f is irreducible and separable, the all linear terms above are distinct. This may not be true if f is inseparable.

Example 2.5.2. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of f, since it does not contain all the root. The splitting field is $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2},)$ where ω is a third of unity, in other words, $1, \omega, \omega^2$ are roots of $x^3 - 1$. Note that we also have $E = \mathbb{Q}(\omega, \sqrt[3]{2})$. The symbol $\sqrt[3]{2}$ is ambiguous, but we can either take the real cube root, or simply note that any choice defines the same field (only now that we've thrown in ω).

Theorem 2.5.3 (Kronecker)**.** *If k is a field and $f(x) \in k[x]$ a non-constant polynomial, there exists an extension field K/k with f a product of linear polynomials in $K[x]$.*

Proof. The proof is induction on $\deg(f)$. If $\deg(f) = 1$, then f is linear and we can choose $K = k$. If $\deg(f) > 1$, write $f = pg$, where $p, q \in k[x]$ and p irreducible. Now Theorem 1.2.12 provides a field F containing k and a root z of p. Hence, in $F[x]$, there is $h(x)$ with $p(x) = (x - z)h(x)$ and so $f(x) = (x - z)h(x)g(x)$. By induction, there is a field K containing F so that hg, and hence f, is a product of linear factors in $K[x]$. □

Corollary 2.5.4. *If k is a field and $f(x) \in k[x]$ a non-constant polynomial, then a splitting field of f over k exists.*

Let's see an example but with some definitions first.

Definition 2.5.5. If $n \geq 1$ is a positive integer, then an n-th *root of unity* in a field k is an element $\zeta \in k$ with $\zeta^n = 1$.

The (complex) numbers $e^{\frac{2\pi ik}{n}} = \cos(2\pi k/n) + i\sin(2\pi k/n)$ for some k with $0 \leq k \leq n - 1$ are *all* the complex n-th roots of unity (in $\mathbb{C}$). Just as there are two square roots of a number a, namely, $\sqrt{a}$ and $-\sqrt{a}$, there are n different n-th roots of a, namely, $e^{\frac{2\pi ik}{n}}\sqrt[n]{a}$ for $k = 0, 1, \cdots, n-1$. (We can assume $\sqrt[n]{a}$ to be the real root if one wants.) Every n-th root of unity is, of course, a root of the polynomial $x^n - 1$. Therefore,

$$x^n - 1 = \prod_{\zeta^n=1} (x - \zeta). \tag{2.2}$$

Definition 2.5.6. If ζ is an n-th root of unity and n is the smallest positive integer for which $\zeta^n = 1$, we say that ζ is a *primitive* n-th root of unity.

Example 2.5.7. i is an 8-th root of unity (for $i^8 = 1$), but not a primitive 8-th root of unity; i is a primitive 4-th root of unity.

Example 2.5.8. Let $f(x) = x^n - 1 \in k[x]$ for some field k and E/k a splitting field. The set of all n-th roots of unity is a cyclic group and a primitive n-th root ω generates it. It follows that $E = k(\omega)$ is a splitting field of f.

We say "a" splitting field instead of "the" splitting field because it is not obvious whether any two splitting fields of f over k are isomorphic (they are). Analysis of this technical point will not only prove uniqueness of splitting fields, it will enable us to prove that any two finite fields with the same number of elements are isomorphic.

Theorem 2.5.9. *Let p be a prime and k a field. If $f(x) = x^p - c \in k[x]$ and α is a p-th root of c (in some splitting field), then either f is irreducible in $k[x]$ or c has a p-th root in k. In either case, if k contains the p-th root of unity, then $k(\alpha)$ is a splitting field of f.*

Proof. By Kronecker's Theorem, there exists an extension field K/k that contains all the roots of f, namely, K contains all the p-th root of c. If $\alpha^p = c$, then every such root has the form $\zeta\alpha$, where ζ is a p-th root of unity.

If f is not irreducible in $k[x]$, then there is a factorization $f = gh$ in $k[x]$, where $g(x), h(x)$ are non-constant polynomials with $d = \deg(g) < \deg(f) = p$. Now the constant term b of g is, up to sign, the product of some of the roots of f:

$$\pm b = \alpha^d \zeta',$$

where ζ', which is a product of p-th roots of unity, is itself a p-th root of unity. It follows that

$$(\pm b)^p = (\alpha^d \zeta')^p = \alpha^{dp} = c^d.$$

But p being prime and $d < p$ force $\gcd(d, p) = 1$; hence, there are integers s and t with $1 = sd + tp$. Therefore,

$$c = c^{sd+tp} = c^{sd} c^{tp} = (\pm b)^{ps} c^{tp} = [(\pm b)^s c^t]^p,$$

and c has a p-th root in k.

We now assume that k contains the set Ω of all the p-th roots of unity. If $\alpha \in K$ is a p-th root of c, then $f(x) = \prod_{\omega \in \Omega}(x - \omega\alpha)$ shows that f splits over K and that $k(\alpha)$ is a splitting field of f over k. □

Observe that if $\varphi : F \to F'$ is a homomorphism, then

$$\varphi_* : F[x] \to F'[x], a_0 + \cdots + a_n x^n \mapsto \varphi(a_0) + \cdots + \varphi(a_n) x^n$$

is a ring homomorphism. If $\varphi : F \to F'$ is an isomorphism, then φ_* is also an isomorphism, and for any $f \in F[x]$, it sends the ideal $\langle f \rangle$ to the ideal $\langle \varphi_*(f) \rangle$.

Lemma 2.5.10. *Let $\varphi : F \to F'$ be an isomorphism between two fields, and $f \in F[x]$ be irreducible in $F[x]$. If α is a root of f in some extension of F, and β is a root of $\varphi_*(f)$ in some extension of F', then there is an isomorphism $\phi : F(\alpha) \to F'(\beta)$ such that $\phi(\alpha) = \beta$, and $\phi|_F = \varphi$.*

Proof. Because f is irreducible in $F[x]$, $\varphi(f)$ is irreducible in $F'[x]$. Because φ_* the ideal $\langle f \rangle$ to the ideal $\langle \varphi_*(f) \rangle$, the map $F[x] \to F'[x]/\varphi_*(f)\rangle$ will have kernel equal to $\langle f \rangle$, so we have an isomorphism

$$F(\alpha) \cong F[x]/\langle f \rangle \cong F'[x]/\langle \varphi_*(f) \rangle \cong F'(\beta).$$

□

Theorem 2.5.11. *Let $\varphi : F \to F'$ be an isomorphism, and f be a non-constant polynomial in $F[x]$. If E is a splitting field for f in F, and E' is a splitting field for $\varphi_*(f)$ in F', then there is an isomorphism $\phi : E \to E'$ such that $\phi|_F = \varphi$.*

Proof. Let p be an irreducible factor of f of degree ≥ 2. Let $\alpha_1 \in E$ be a root of p and $\beta_1 \in E'$ be root of $\varphi_*(p)$. By the previous lemma, there is an isomorphism $F(\alpha_1) \to F'(\beta_1)$ that restricts to φ on F. If we repeat this process (until f no longer has any irreducible factors of degree ≥ 2), then we have a isomorphism $F(\alpha_1, \cdots, \alpha_k) \cong F'(\beta_1, \cdots, \beta_k)$ that restricts to φ on F. Because f splits in $F(\alpha_1, \cdots, \alpha_k)$, and $\varphi(f)$ splits in $F'(\beta_1, \cdots, \beta_k)$, it follows that $E = F(\alpha_1, \cdots, \alpha_k)$ and $E' = F'(\beta_1, \cdots, \beta_k)$, which completes the proof. □

The following theorem, which is perhaps surprising, says that the splitting field of a polynomial contains a splitting field for the minimal polynomial of any element of that field.

Theorem 2.5.12. *Let E/F be a finite extension of fields. The following are equivalent:*

1. *E is the splitting field of some polynomial over F;*
2. *every irreducible polynomial $g(x) \in F[x]$ with a root in E factors completely over E;*
3. *any embedding $\sigma : E \to \overline{E}$ fixing F is an automorphism of E, namely, $im(\sigma) = E$.*

Definition 2.5.13. A finite extension E/F is *normal* if it satisfies any of the equivalent conditions in Theorem 2.5.12.

Remark. In Theorem 2.5.12, you can replace a *finite extension* by an *algebraic extension*, and then what we need is a possibly infinite set of polynomials.

Proof of Theorem 2.5.12. We show that

$$(3) \Longrightarrow (2) \Longrightarrow (1) \Longrightarrow (3).$$

(2) $\Longrightarrow$ (1): For a primitive extension $E = F(\alpha)$, E is the splitting field of the minimal polynomial of α over F. If $E = F(\alpha_1, \cdots, \alpha_n)$, the E is the splitting field of the products of the minimal polynomials of α_i over F for $i = 1, \cdots, n$.

(3) $\Longrightarrow$ (2): Let $g(x) \in F[x]$ be an irreducibility polynomial with a root $\beta \in E$. For each root $\beta' \in \overline{E}$, we obtain an embedding: $F(\beta) \to \overline{E}$ with $\phi(\beta) = \beta'$. By Lemma 2.4.9, we can extend to an embedding $\sigma : E \to \overline{E}$ (fixing F). The image of σ is E by assumption. In other words, $\beta' = \phi(\beta)$ is in E. As β' runs over all possible roots, E contains all the roots of g and so g factors completely in $E[x]$.

(1) $\Longrightarrow$ (3): Let E be the splitting field of $f(x) \in F[x]$ and $\sigma : E \to \overline{E}$ an embedding fixing F. We know that σ permutes the roots of $f(x)$ in $\overline{E}$, so the image of σ contains all the roots of f. But E is exactly generated by the roots of f, so the im(σ) is as well. It follows that $\sigma(E) = E$. □

Definition 2.5.14. A *normal closure* of an algebraic field extension L/K is a field extension field L' of L such that L'/L is algebraic and L'/K is normal with the property that there is no proper subfield of L' satisfying these conditions.

Theorem 2.5.15. *Let L/K be an algebraic field extension. Then we have:*

1. *L/K admits a normal closure L'/K, where L' is unique up to isomorphism over L.*
2. *L'/K is finite if L/K is finite*
3. *If M/L is an algebraic field extension such that M/K is normal, we can choose L' as an intermediate field of M/L. In this case, L' is unique. More precisely, if $(\sigma_i)_{i\in I}$ is the family of all K-homomorphisms from L to M, then $L' = K(\sigma_i(L) : i \in I)$. We call L' the normal closure of L in M.*

Proof. Note the only difference when we pass from a finite extension to an algebraic extension is that $L = K(S)$ and S is a (possibly infinite) set of algebraic elements over K.

Let f_j be the minimal polynomial of a_j over K. If M is an algebraic extension field of L such that M/K is normal (we can set $M = \overline{L}$), then the polynomials f_j decompose in $M[X]$ into a product of linear factors. Now let L' be the subfield of M that is generated over K by the zeros of the f_j. Then L'

is defined as a splitting field of the f_j. Furthermore, we have $L \subset L' \subset M$, and it is clear that L'/K is a normal closure of L/K. Also we see that L'/K is finite if L/K is finite. On the other hand, if L'/K is a normal closure of L/K, then the field L' contains necessarily a splitting field of the f_j and thus, due to the minimality condition, is a splitting field of the f_j over K.

To establish the uniqueness assertion, consider two normal closures L_1'/K and L_2'/K of L/K. As we have just seen, L_1' and L_2' are splitting fields of the polynomials f_j over K and hence also splitting fields of the f_j over L. Then the uniqueness of splitting fields says L_1 and L_2 are isomorphic.

For the last piece of the statement, consider a K-homomorphism $\sigma : L \to M$. σ maps the zeros of the f_j to zeros of f_j. Since L' is generated over K by these zeros, we see that $K(\sigma_i(L) : i \in I) \subset L'$. Conversely, for every zero $a \in L'$ of one of the polynomials f_j we can define a K-homomorphism $K(a_j) \to L'$ such that $a_j \mapsto a$. This can be extended by Lemma 2.4.9 to a K-automorphism of an algebraic closure of L' and subsequently be restricted to a K-homomorphism $\sigma : L \to L'$, using the normality of L'/K. Thus, a lie in $K(\sigma_i(L) : i \in I)$, and the equality $L' = K(\sigma_i(L) : i \in I)$ is clear. $\square$

Week 3

3.6 Separable Extensions

Let $f(x) \in F[x]$ be an irreducible polynomial and $(E = F[\alpha], \alpha)$ its stem field (or E a possibly larger field containing all the roots). From what we have learnt from the first week, we know an element in $\mathrm{Aut}(E/F)$ shall permute the roots of f. It then follows not surprisingly that we want the distinctness of the roots; in other words, we want the roots to be separable.

Definition 3.6.1. Let k be a field. A nonzero polynomial $f(x) \in k[x]$ is called *separable* if it has no repeated roots (in any extension field).

Recall that the derivative of a polynomial $f(x) = \sum a_i x^i$ is defined to be $f'(x) = \sum i a_i x^{i-1}$. When f has coefficients in $\mathbb{R}$, this agrees with the definition in calculus. The usual rules for differentiating sums and products still hold, but note that in characteristic p the derivative of x^p is zero.

Theorem 3.6.2. *Let K be a field and $f(X) \in K[X]$ a non-constant polynomial. Then f is separable if and only if $\gcd(f, f') = 1$ in $K[X]$. In particular, when f is irreducible, then*

1. *if $\mathrm{char}(K) = 0$, then f is separable;*
2. *if $\mathrm{char}(K) = p > 0$, then f has a multiple root if and only if $f'(X) = 0$ if and only if $f(X) = g(X^{p^r})$ for some $g(X) \in K[X]$ where the integer r can be chosen to be maximal such that every zero of f has multiplicity p.*

Proof. Let $f(X)$ be a non-constant polynomial in $K[X]$. Suppose $f(X)$ is separable, and let α be a root of $f(X)$ (in some extension of K. Then $f(X) = (X - \alpha)h(X)$ for some $h(x) \neq 0$. Since $f'(\alpha) = h(\alpha) \neq 0$, f and f' cannot have any common roots as α runs all possible roots of f. Hence $\gcd(f, f') = 1$.

Now suppose $f(X)$ is not separable and α is a repeated root (in an extension field). Then we can write $f(X) = (X-\alpha)^2 g(X)$, where $g(x)$ is non-zero, and then $f'(X) = (X-\alpha)^2 g'(X) + 2(X-\alpha)g(x)$. It follows that $f'(\alpha) = 0$. By Theorem 1.2.10, both f, f' are divisible by the minimal polynomial of α in $K[X]$ and then $\gcd(f, f') \neq 1$.

Let's discuss the in "particular part". Assume f is irreducible.

1. Note $\deg(f') = \deg(f) - 1 \neq 0$. Then by the irreducibility of f, it follows immediately that $\gcd(f, f') = 0$. Hence f is irreducible.
2. Suppose f is not separable. Since $\gcd(f, f') \neq 1$ and f is irreducible, the only possibility is $f' = 0$. Take
$$f(X) = \sum_{i=0}^{n} a_i X^i \text{ and then } f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}.$$

The coefficients of f' must vanish, namely, $ia_i = 0$, but then either $a_i = 0$ or i is a multiple of p. We conclude that $f(X) = g(X^p)$ for some $g(X) \in K[X]$.

Now assume $f(X) = g(X^{p^r})$ where r is chosen to be maximal. Then $g' \neq 0$, otherwise, we can repeat above reasoning for g. Since f is irreducible, so is g. And therefore $\gcd(g, g') = 0$ and then g is separable. We can say

$$g(X) = \prod_{i=1}^{n}(X - a_i) \in \overline{K}[X],$$

where we can assume f and hence g are monic and $\overline{K}$ is a algebraic closure of K. Let b_i be the p^r-th root of a_i, then we have

$$f(X) = \prod_{i=1}^{n}(X^{p^r} - b_i^{p^r}) = \prod_{i=1}^{n}(X - b_i)^{p^r} \in \overline{K}[X].$$

It is clear to see that the zeros of f are all of multiplicity p^r.

□

Definition 3.6.3. A field F is said to be *perfect* if every irreducible polynomial in $F[x]$ is separable.

Fortunately, almost all the fields we have good feelings at are perfect, for example, Theorem 1.3.9 says $\mathbb{F}_p$ is perfect for any prime p.

Theorem 3.6.4. *A field F is perfect if and only if either F has characteristic 0, or F has characteristic p and the Frobenius map $\sigma : F \to F, x \mapsto x^p$ is an isomorphism.*

Proof. Suppose that F has characteristic 0. Let f be an irreducible polynomial. Then $\deg(f') = \deg(f) - 1 \neq 0$ and it follows from the irreducibility of f that $\gcd(f, f') = 1$. Therefore, f is separable by Theorem 3.6.2.

Now consider the case when the characteristic of F is a prime p. We already see σ is a field homomorphism last week. Since field homomorphisms are injective, we only need to consider the surjectivity of σ.

Suppose that σ is not surjective and $a \in F$ is not in the image. Then the polynomial $f(x) = x^p - a$ has no roots in F.

Claim: $f(x)$ is irreducible.

Proof of claim: By Theorem 1.2.12, let E/F be a finite extension containing a root β of f and so that

$$f(x) = x^p - a = x^p - \beta^p = (x - \beta)^p \in E[x].$$

Thus if f factors non-trivially in $F[x]$, then a factor of f looks like $(x - \beta)^j \in F[x]$ for some $1 \leq j < p$. The coefficient of x^{j-1} in $(x - \beta)^j$ is $-j\beta$. Since $j \neq 0$ in F, we conclude β lies in F and reach a contradiction.

Notice that $f'(x) = px^{p-1} = 0$ in $F[x]$ and then $\gcd(f, f') = f \neq 1$ and f is inseparable. We have shown f is irreducible and inseparable and then F is not perfect.

For another direction, suppose that σ is surjective and that $f \in F[x]$ is irreducible and inseparable. Similarly to the argument in Theorem 3.6.2, we get f divides f'. If f' was not the zero polynomial, then $\deg(f') < \deg(f)$, which is impossible given $f \mid f'$. Let $f(x) = \sum_{i=0}^{d} a_i x^i$ then we get

$$0 = f'(x) = \sum_{i=1}^{d} i a_i x^{i-1} \in F[x].$$

Therefore, $ia_i = 0$ for each i, which says $a_i = 0$ or $i = 0$ in F. In other words, $a_i = 0$ unless $p|i$ and then we can write

$$f(x) = \sum_{i=0}^{m} a_{ip} x^{ip}.$$

But σ is surjective, then $a_{ip} = (\alpha^i)^p$ for some $\alpha_i \in F$ for each i and

$$f(x) = \sum_{i=0}^{m} (\alpha_i)^p x^{ip} = (\sum_{i=1}^{m} \alpha_i x^i)^p.$$

This polynomial is definitely reducible and we reach a contradiction. □

This theorem says that fields of characteristic 0 and finite fields are perfect. One has to work fairly hard to come up with an example of an inseparable extension. But these do come up naturally in algebraic geometry over fields of positive characteristic.

Now the discussion on finite fields in Week 1 makes more sense now.

Theorem 3.6.5 (Galois)**.** *If p is prime and n is a positive integer, then there exists a field having exactly p^n elements.*

Proof. Look at a splitting field of $g(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. The roots of $g(x)$ are all distinct and forms a subfield of the splitting field by checking addition and multiplication. □

Theorem 3.6.6 (Moore)**.** *Any two finite fields having exactly p^n elements are isomorphic.*

Proof. They are all the splitting fields of $g(x) = x^{p^n} - x \in \mathbb{F}_p[x]$, and hence isomorphic. □

Remark. It follows immediately that $\mathbb{F}^{p^n}/\mathbb{F}_p$ is normal.

A lot of results about field theory that are valid in characteristic 0 carry over to perfect fields in characteristic p (but not everything), and the reader should be attentive to this point when reading texts which try to make life easy by always assuming fields have characteristic 0. You should always check if the theorems (and even proofs) go through to general perfect fields.

Definition 3.6.7. Let E/F be an algebraic extension of fields, and let $\alpha \in E$ be algebraic over F. We say that α is *separable* over F if the minimal polynomial of α over F is separable. We say that E/F is *separable* if every element of E is separable over F.

Theorem 3.6.8. *A field K is perfect if and only if every finite extension of K is a separable extension.*

Proof. Suppose K is perfect: every irreducible in $K[X]$ is separable. If L/K is a finite extension then the minimal polynomial in $K[X]$ of every element (which is algebraic) of L is irreducible and therefore separable, so L/K is a separable extension.

Now suppose every finite extension of K is a separable extension. To show K is perfect, let $f(X) \in K[X]$ be irreducible. Consider the stem field $L = K(\alpha)$ from Theorem 1.2.12, where $f(\alpha) = 0$. This field is a finite extension of K, so a separable extension by hypothesis, so α is separable over K. Since $f(X)$ is the minimal polynomial of α in $K[X]$, it is a separable polynomial. □

It is clear that extensions of fields of characteristic 0 have characteristic 0, and that finite extensions of finite fields are finite, so this theorem is only non-trivial if F is infinite, but has a positive characteristic.

3.7 The Primitive Element Theorem

In this section we prove a result which is not entirely necessary for the discourse, but simplifies the proofs of several other theorems.

Definition 3.7.1. A field extension E/F is *primitive* if there is an element $\alpha \in E$ such that $E = F(\alpha)$.

Example 3.7.2. We already show $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is primitive.

Theorem 3.7.3 (Primitive Element Theorem)**.** *Let E/F be a finite, separable extension of fields. Then E/F is a primitive extension,*

Proof. We will first note that the theorem is trivial if F is a finite field, since in this case E is also finite, and $E^\times$ is a cyclic group. Any generator α will clearly satisfy $E = F(\alpha)$.

We also note that it suffices to prove the theorem in the case $E = F(\alpha, \beta)$, since the general case follows by induction (E will always have some finite basis over F). So we'll suppose that F is infinite and that $E = F(\alpha, \beta)$ for some $\alpha, \beta \in E$. Let $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of the minimal polynomial $f(x)$ of α over F (in $\overline{F}$), and $\beta = \beta_1, \beta_2, \cdots, \beta_m$ the roots of the minimal polynomial $h(x)$ of β over F (in $\overline{F}$). All the roots are distinct since E is separable. Since F is infinite, we may choose some $a \in F$ such that

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

for any i and any $j \neq 1$. Let $\gamma = \alpha + a\beta$

Claim: $F(\alpha, \beta) = F(\gamma)$.

The theorem follows from the claim (and inductions) immediately.

Proof of Claim: Note that since $\gamma = \alpha + a\beta$, we have $F(\alpha, \beta) = F(\gamma, \beta)$. It is enough to show β is in $F(\gamma)$. Let $g(x) = f(\gamma - ax) \in F(\gamma)[x]$. Note that

$$g(\beta) = f(\gamma - a\beta) = f((\alpha + a\beta) - a\beta) = f(\alpha) = 0.$$

On the other hand, we cannot have $g(\beta_j) = 0$ for $j \neq 1$, as $f(\gamma - a\beta_j) = 0$ would imply $\gamma - a\beta_j = \alpha_i$ for some i. Substituting $\gamma = \alpha + a\beta$ inside, we reach at

$$a(\beta - \beta_j) = \alpha_i - \alpha.$$

This contradicts to our initial assumption about a. Thus $\gcd(g(x), h(x)) \in F(\gamma)[x]$ has exactly one root, namely $x = \beta$. And since $h(x)$ has no repeated root, neither does $\gcd(g(x), h(x))$. It follows that $\gcd(g(x), h(x)) \in F(\gamma)[x]$ is a linear polynomial vanishing at β, and in fact $\beta \in F(\gamma)$. (A hidden fact here is that if E/F is a field extension and $g(x), f(x)$ are in $F[x]$, then $\gcd_{F[x]}(g, f) = \gcd_{E[x]}(g, f)$. A simple explanation is that $\gcd(g, f)$ can be computed with the Euclidean algorithm, which operates on the coefficients of g and g and so never leaves F.) □

The next theorem gives a complete description of field extensions which admit a primitive element.

Theorem 3.7.4 (Steinitz)**.** *Let E/F be a finite extension of fields. Then $E = F(\alpha)$ for some $\alpha \in E$ if and only if there exist only finitely many distinct intermediate fields $F \subset K \subset E$.*

Proof. We have seen that the primitive element property trivially holds in all finite fields, and the property of there only being finitely many intermediate fields does as well. We will suppose, then, that F is infinite. Suppose that there are only finitely many intermediate fields. We will show that $E = F(\alpha)$ for some α,

and just as in the proof of Theorem 3.7.3 (which is very similar) we are free to suppose that $E = F(\beta, \gamma)$. Consider the fields $F(\beta + a\gamma)$, for $a \in F$. Since all of these fields lie between F and E, there must be distinct $a_1 \neq a_2 \in F$ with $F(\beta + a_1\gamma) = F(\beta + a_2\gamma)$. Now, since $\beta + a_1\gamma$ and $\beta + a_2\gamma$ are both in this field, so is $(a_2 - a_1)\gamma$, and hence γ (since $a_2 - a_1 \neq 0$). It follows $\beta = (\beta + a_1\gamma) - a_1\gamma$ is in $F(\beta + a_1)\gamma$ as well. Thus $E = F(\beta, \gamma) = F(\beta + a_1\gamma)$, and we are done.

For another direction, suppose that $E = F(\alpha)$. For each intermediate field $F \subset K \subset E$, we take $f_K(x) \in K[x] \subset E[x]$ to be the minimal polynomial of α over K. By unique factorization in $E[x]$, each $f_K(x)$ must be a (monic) divisor of $f_F(x)$ (where $f_F(x)$ is considered as a polynomial in $E[x]$), and there are only finitely many of these. It suffices to show, then, that this function $K \to f_K(x)$ is one-to-one. Let $F(f_K)$ be the field generated over F by the coefficients of $f_K(x)$. Then certainly $F(f_K) \subset K$. On the other hand, $f_K(x)$ is an irreducible monic polynomial with coefficients in $F(f_K)$, which vanishes at α, and so α has degree $\deg(f_K)$ over $F(f_K)$. It follows from the fact that

$$[F(\alpha) : F(f_K)] = [F(\alpha) : K][K : F(f_K)]$$

that $[K : F(f_K)] = 1$. In other words, $K = F(f_K)$, showing that the map is injective. It follows at once that there are only finitely many subfields $F \subset K \subset E$. □

Remark. Patrick Ingram refers Theorem 3.7.4 as the primitive element theorem. But Rotman labels it after Steinitz. And many textbooks (Rotman included) refers Theorem 3.7.3 as the primitive element theorem instead. We follow Rotman's conventions.

Theorem 3.7.5. *Let F be a field, $\overline{F}$ its algebraic closure, and let $F \subset E \subset \overline{F}$ be a finite separable extension of F. Then there are precisely $[E : F]$ distinct embeddings $E \to \overline{F}$ which fix F.*

Proof. By the primitive element theorem, we may suppose that $E = F(\alpha)$, and let $f(x) \in F[x]$ be the minimal polynomial of α. For each root $\alpha' \in \overline{F}$, we have an isomorphism

$$E = F(\alpha) \cong F[x]/(f(x)) \cong F(\alpha') \subset \overline{F}.$$

This gives us $\deg(f) = [E : F]$ embeddings of E into $\overline{F}$, which must be distinct, since they send α to the $\deg(f)$ distinct roots of f (as E/F is separable). On the other hand, any embedding $F(\alpha) \to \overline{F}$ which fixes F is determined entirely by the value at α (which must be a root of the same minimal polynomials in $F[x]$ as α), and so these are the only possible embeddings of $E \to \overline{F}$. □

Corollary 3.7.6. *Let E/F be a finite separable extension. Then*

$$|Aut(E/F)| \leq [E : F].$$

Proof. Each distinct automorphism $\sigma \in \mathrm{Aut}(E/F)$ gives a distinct embedding $\sigma : E \to E \subset \overline{F}$, which fixes F. □

3.8 Separable Degree

We will now proceed with a slightly more detailed examination of extensions which are not separable.

Definition 3.8.1. Let E/F be a finite extension of fields, and let $\overline{F}$ be an algebraic closure of F (and fix an embedding $\iota : F \hookrightarrow \overline{F}$). We define the separable degree of E over F, denoted $[E : F]_s$, to be the number of distinct embeddings

$$\sigma : E \to \overline{F},$$

which fix F pointwise (indeed, $\sigma|_F = \iota$).

Lemma 3.8.2. *Let $K \subset L = K(\alpha)$ be a primitive algebraic field extension with minimal polynomial $f \in K[X]$ of α over K.*

1. *The separable degree $[L : K]_s$ equals the number of different zeros of f in an algebraic closure of K.*
2. *The element α is separable over K if and only if $[L : K] = [L : K]_s$.*
3. *Assume char$(K) = p > 0$ and let p^r be the multiplicity of the zero α of f. Then $[L : K] = p^r[L : K]_s$.*

Proof. Parts of the proof have appeared discretely many times.

1. This is just a reformulation of Lemma 2.5.10.
2. f have at most $\deg(f) = [L : K]$ roots and each distinct root gives a distinct embedding $L \to \overline{K}$. There are $[L : K]_s = [L : K]$ such embeddings hence all the roots are distinct.
3. If a root of f has multiplicity p^r, then $f(X) = g(X^{p^r})$ for some $g(X) \in K[X]$. Hence there are $\deg(f)/p^r$ distinct roots and so is the number of separation degree. In other words, $[L : K] = p^r[L : K]_s$.

□

Theorem 3.8.3. *Let $K \subset L \subset M$ be algebraic field extensions. Then*

$$[M : K]_s = [M : L]_s[L : K]_s.$$

Proof. Fix an algebraic closure $\overline{K}$ of K. Then $K \subset L \subset M \subset \overline{K}$, and we may view K also as an algebraic closure of M and of L. Furthermore, let

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i : i \in I\}, \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j : j \in J\},$$

where in each case, the σ_i as well as the τ_j are distinct. Now extend the K-homomorphisms $\sigma_i : L \to \overline{K}$ via Lemma 2.4.9 to K-automorphisms $\overline{\sigma_i} : \overline{K} \to \overline{K}$. The desired multiplicative formula will then be a consequence of the following two assertions:

1. The maps $\overline{\sigma_i} \circ \tau_j : M \to \overline{K}, i \in I, j \in J$, are distinct.
2. $\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma_i} \circ \tau_j; i \in I, j \in J\}$.

To verify assertion (1), consider an equation of type $\overline{\sigma_i} \circ \tau_j = \overline{\sigma_{i'}} \circ \tau_{j'}$. Since τ_j and $\tau_{j'}$ restrict to the identity on L, we can conclude that $\overline{\sigma_i} = \overline{\sigma_{i'}}$ and hence $i = i'$. The latter implies $\tau_j = \tau_{j'}$, and thus $j = j'$. It follows that the maps specified in (1) are distinct.

Since they are K-homomorphisms, it remains to show for (2) that every K-homomorphism $\tau : M \to \overline{K}$ is as specified in (1). For $\tau \in \mathrm{Hom}_K(M, \overline{K})$ we have $\tau|_L \in \mathrm{Hom}_L(M, \overline{K})$. Hence, there exists an index $i \in I$ such that $\tau|_L = \sigma_i$. Then we obtain $\overline{\sigma_i}^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$. Therefore, $\tau = \overline{\sigma_i} \circ \tau_j$ and (2) is clear. □

Put all the knowledge together, we get the following statement:

Corollary 3.8.4. *Let $K \subset L$ be a finite field extension.*

1. *If* $\text{char}(K) = 0$*, then* $[L : K] = [L : K]_s$.

2. *If* $\text{char}(K) = p > 0$*, then* $[L : K] = p^r[L : K]_s$ *for some integer* r*. In particular, if* $\text{char}(K) \nmid [L : K]$*, then* $[L : K]_s = [L : K]$.

Theorem 3.8.5. *For a finite field extension* $K \subset L$ *the following conditions are equivalent:*

1. L/K *is separable.*

2. *There exist elements* $a_1, \cdots, a_n \in L$ *that are separable over* K *and satisfy*

$$L = K(a_1, \cdots, a_n).$$

3. $[L : K]_s = [L : K]$.

Proof. The implication from (1) to (2) is trivial. If $a \in L$ is separable over K, then the same is true over every intermediate field of L/K. Therefore, using the multiplicative formulas, the implication from (2) to (3) can be reduced to the case of a simple field extension. However, that case was already dealt with in Lemma 3.8.2.

It remains to show that (3) implies (1). Consider an element $a \in L$ with its minimal polynomial $f \in K[X]$ over K. To show that a is separable over K, which amounts to showing that f admits only simple zeros, we are reduced to the case $\text{char}(K) = p > 0$. Then, by above corollary, there is a integer r such that every root of f has multiplicity r and

$$[K(a) : K] = p^r[K(a) : K]_s.$$

Using the multiplicative formulas in conjunction with the estimate between the degree and the separable degree, we obtain

$$[L : K] = [L : K(a)][K(a), K] \geq [L : K(a)]_s p^r [K(a) : K]_s = p^r[L : K]_s.$$

Now, if $[L : K]_s = [L : K]$, we must have $r = 0$. Then all zeros of f are simple and a is separable over K, which shows that (3) implies condition (1). □

Corollary 3.8.6. *Let* $K \subset L \subset M$ *be algebraic field extensions. Then* M/K *is separable if and only if* M/L *and* L/K *are separable.*

Corollary 3.8.7. *Let* K/F *be a finite algebraic extension. If* $K = F(\alpha_1, \cdots, \alpha_n)$ *and each* α_i *is separable, then* K/F *is separable.*

The usefulness of this corollary is that it gives a practical way to check a finite extension L/K is separable: rather than show every element of L is separable over K it suffices to show there is a set of field generators for L/K that are each separable over K.

3.9 Inseparable Extensions

A field of characteristic 0 is perfect. We assume in this section that the characteristic of a field is p.

Definition 3.9.1. A non-constant polynomial $f \in F[x]$ is *purely inseparable* if it admits precisely one root.

If f is irreducible and purely inseparable, then $f(x) = (x-\alpha)^{p^n} = x^{p^n} - c$.

Definition 3.9.2. Let L/K be an algebraic field extension. An element $\alpha \in L$ is *purely inseparable* over K if α is a zero of a purely inseparable polynomial, namely, the minim polynomial $\text{irr}(\alpha, K)$ is of the form $x^{p^n} - c$ from some integer n and $c \in K$. L is *purely inseparable* over K if every element in $L \setminus K$ is purely inseparable.

It follows immediately that purely inseparable field extensions are normal.

Theorem 3.9.3. *For a finite algebraic extension L/K, the following conditions are equivalent:*

1. *L is purely inseparable over K;*
2. *There are elements $a_1, \cdots, a_n \in L$ such that $L = K(a_1, \cdots, a_n)$ and each a_i is purely inseparable over K;*
3. *$[L : K]_s = 1$;*
4. *For every element $a \in L \setminus K$, there is an integer n such that $a^{p^n} \in K$.*

Proof. We will show $(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (4) \Longrightarrow (1)$.

(1) $\Longrightarrow$ (2) is clear.

(2) $\Longrightarrow$ (3): It is enough to show $[K(a_i) : K]_s = 1$ for all i, because any K-map $L \to \overline{K}$ is uniquely determined by the image of the elements α_i. On the other hand, the minimal polynomial of a_i admits only a single root in $\overline{K}$ and only one K-map $L \to \overline{K}$. Hence $[K(a_i) : K]_s = 1$ and so $[L : K]_s = 1$.

(3) $\Longrightarrow$ (4): For any $a \in L \setminus K$, we have

$$[L : K(a)]_s [K(a) : K]_s = [L : K]_s.$$

So $[K(a) : K]_s = 1$. So the minimal polynomial of a admits only one (repeated) root which is of the form $x^{p^n} - c$. Hence $a^{p^n} \in K$.

(4) $\Longrightarrow$ (1): For any $a \in L \setminus K$, we have $a^{p^n} = c \in K$. Hence $\text{irr}(a, K)$ divides $x^{p^n} - c$ which has only one (repeated) root. So is $\text{irr}(a, K)$ and then a is purely inseparable over K. □

Example 3.9.4. Consider the field extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^n)$. $x^p - t^p \in \mathbb{F}_p(t^n)[x]$ is irreducible (by Eisenstein's Criterion) and purely inseparable over $\mathbb{F}_p(t)$. It is indeed a purely inseparable extension by above theorem.

We finish this section by showing that every algebraic field extension can be decomposed into a separable extension, followed by a purely inseparable extension.

Theorem 3.9.5. *Let L/K be an algebraic field extension. Then there exists a unique intermediate field*

$$K_s = \{a \in L : a \text{ separable over} K\}$$

of L/K such that L/K_s is purely inseparable and K_s/K is separable. The field K_s is called the separable closure of K in L. We also have $[L : K]_s = [K_s : K]$. If L/K is normal, the extension K_s/K is normal, too.

Proof. We first note that K_s is a field. Indeed, for $a, b \in K_s$, that $K(a, b)$ is a separable extension of K, so that $K(a, b) \subset K_s$. Therefore, K_s is the biggest separable extension of K that is contained in L.

Now consider an element $a \in L$ and let $f \in K_s[X]$ be the minimal polynomial of a over K_s. Then, there exists a separable polynomial $g \in K_s[X]$ such that $f(x) = g(x^{p^r})$ for some integer r. Moreover, g is irreducible, since f is irreducible. It follows that g is the minimal polynomial of $c = a^{p^r}$ over K_s and that c is separable over K_s hence separable over K. However, then we must have $c \in K_s$ and therefore $g(x) = x - c$, as well as $f(x) = x^{p^r} - c$. Thus, a is purely inseparable over K_s, and the same is true for L over K_s.

Since L/K_s is purely inseparable and K_s/K is separable, we get the stated relation on degrees

$$[L : K]_s = [L : K_s]_s[K_s : K]_s = [K_s : K].$$

To justify the uniqueness of K_s, consider an intermediate field K' of L/K such that L/K' is purely inseparable and K'/K is separable. Then we have $K' \subset K_s$ by the definition of K_s, and the extension K_s/K' is separable. On the other hand, the latter extension is purely inseparable, since L/K' is purely inseparable.This shows that K_s/K' is trivial and hence that K_s is unique, as claimed.

It remains to show that K_s/K is normal if the same is true for L/K. To do this, consider a K-homomorphism $\sigma : K_s \to \overline{L}$ into an algebraic closure of L. Since we can view $\overline{L}$ as an algebraic closure of K as well, we can extend σ due to Lemma 2.4.9 to a K-homomorphism $\sigma' : L \to \overline{L}$. Now, assuming L/K to be normal, σ' restricts to a K-automorphism of L. Furthermore, the uniqueness of K_s implies that σ restricts to a K-automorphism of K_s, and it follows that K_s/K is normal. □

Example 3.9.6. Consider the function field $F = \mathbb{F}_x(x)$ and the field extension $E = F(x^{1/6})$. Then it is easily seen that $E = F(x^{1/2}, x^{1/3})$. $x^{1/2}$ is purely inseparable and $x^{1/3}$ is separable. Hence $F(x^{1/3})$ is the separable closure and $[E : F]_s = 3$.

Week 4

4.10 Galois Extensions

There is an alternate characterization of normal extensions in the separable case:

Theorem 4.10.1. *Let E/F be a finite separable extension. The E/F is normal if and only if*

$$|Aut(E/F)| = [E : F].$$

Proof. Suppose that E/F is normal. By Theorem 3.7.5 there are $[E : F]$ embeddings $E \to \overline{F}$ fixing F since E/F is finite and separable. And Theorem 2.5.12 says each of the embedding has image E as well since E/F is normal.

On the other hand, suppose $|\text{Aut}(E/F)| = [E : F]$. By Theorem 3.7.5 there are precisely $[E : F]$ distinct embeddings $E \to \overline{F}$ fixing F since E/F is finite and separable. But $|\text{Aut}(E/F)| = [E : F]$, so each embedding must give rise to an automorphism $E \to E$, since $|\text{Aut}(E/F)|$ is just the number of these embeddings under which the image of E is E. So $|\text{Aut}(E/F)| = [E : F]$ implies E/F is a normal extension. □

Indeed, the equality $|\text{Aut}(E/F)| = [E : F]$ is all we want.

Definition 4.10.2. Let E/F be a finite field extension. E/F is a *Galois extension* if E/F is separable and normal. The *Galois group* of the extension is simply $\text{Gal}(E/F) = \text{Aut}(E/F)$.

We will simply say E is Galois if F is clear in the context. The change of notation of the group $\text{Aut}(E/F)$ to $\text{Gal}(E/F)$ is simply to remind us this is a Galois extension.

In other words, a finite extension E/F is Galois if it is separable, and contains either no roots or all of the roots of a given irreducible polynomial $f(x) \in F[x]$. Since every finite separable extension is primitive, $E = F(\alpha)$, we see that E is Galois if and only if E contains all of the roots of the minimal polynomial of α (in some algebraic closure of F).

Example 4.10.3. We have seen that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois while $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

Proposition 4.10.4. *Let L/K be a finite extension. Then*

1. *if L/K is separable, then the normal closure L'/K is Galois;*
2. *if L/K is normal, then the separable closure K_s/K is Galois.*

Example 4.10.5 (Quadratic extensions)**.** Let F be a field of any characteristic other than 2 and let E/F be an extension with $[E : F] = 2$.

Claim: E/F is Galois.

Note that for any $\alpha \in E \setminus F$, we have $[F(\alpha) : F] > 1$. In the mean time,

$$2 = [E : F] = [E : F(\alpha)][F(\alpha) : F] > [E : F(\alpha)],$$

so we must have $[E : F(\alpha)] = 1$, namely, $E = F(\alpha)$. If the minimal polynomial of α is

$$f(x) = x^2 + bx + c,$$

we can replace α with $\alpha + b/2$ (char$(F) \neq 2$!) and assume with out of generality that $b = 0$ by noting that $F(\alpha) = F(\alpha + b/2)$. And then the minimal polynomial turns out to be $f(x) = x^2 - D$, for some non-zero $D \in F$. f is separable since $f'(x) = 2x \neq 0$ (char$(F) \neq 2$!) and then $\gcd(f, f') = 1$.

There are two embeddings $E \to \overline{F}$, namely that defined by $\alpha \mapsto \alpha$ and that defined by $\alpha \mapsto -\alpha$. But $-\alpha \in F(\alpha)$, so they are just automorphisms of E. Hence

$$\text{Gal}(E/F) \cong \mathbb{Z}/2\mathbb{Z}.$$

Example 4.10.6. Let E be the field $\mathbb{Q}(\sqrt[4]{2})$, where $\sqrt[4]{2}$ is the real positive fourth root of 2. Clearly, the minimal polynomial of $\sqrt[4]{2}$ is $f(x) = x^4 - 2$ in $\mathbb{Q}[x]$ and so $[E : \mathbb{Q}] = 4$. But $|\text{Aut}(E/\mathbb{Q})| = 2$ since $\sigma(\sqrt[4]{2})$ is also a fourth root of 2 and $E \subset \mathbb{R}$ contains two fourth root of 2 only. The non-trivial element $\sigma \in \text{Aut}(E/\mathbb{Q})$ is then defined by

$$\sigma(a_1 + a_2\sqrt[4]{2} + a_3\sqrt{2} + a_4(\sqrt[4]{2})^3) = a_1 - a_2\sqrt[4]{2} + a_3\sqrt{2} - a_4(\sqrt[4]{2})^3.$$

The splitting field of $f(x)$ is the larger field $K = \mathbb{Q}(\sqrt[4]{2}, i) = E(i)$, indeed, the normal closure of E. It is clear that this is the same field generated by the roots of $f(x)$, which are $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$. Note that $[K : E] = 2$ and so $[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 8$. By Theorem 4.10.1, $|\text{Gal}(K/\mathbb{Q})| = 8$.

The computations of Galois group will be discuss in details later on. Nevertheless, we can still investigate Gal$(K/\mathbb{Q})$ in this case. Since $K = \mathbb{Q}(\sqrt[4]{2}, i)$, an element $\sigma \in \text{Gal}(K/\mathbb{Q})$ is entirely determined by values $\sigma(\sqrt[4]{2})$ and $\sigma(i)$, where $\sigma(\sqrt[4]{2})$ is a root of $x^4 - 1$ and $\sigma(i)$ is a root of $x^2 + 1$. So there are 8 possible choices given by the combinations of

$$\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\} \text{ and } \sigma(i) \in \{i, -i\}.$$

There are 8 options only and indeed $|\text{Gal}(K/\mathbb{Q})| = 8$, so each combination must defines an element of Gal$(K/\mathbb{Q})$.

To simplify notations, let $\sigma_{a,b} \in \text{Gal}(K/\mathbb{Q})$ be the automorphism defined by $\sqrt[4]{2} \mapsto i^a\sqrt[4]{2}$ and $i \to (-1)^b i$. Note that $i^4 = 1$ and $(-1)^2 = 1$, so we can require $a \in \mathbb{Z}/4\mathbb{Z}$ and $b \in \mathbb{Z}/2\mathbb{Z}$. $\sigma_{0,1}$ and $\sigma_{2,0}$ are two elements of order 2, hence Gal$(K/\mathbb{Q})$ is not isomorphic to $\mathbb{Z}/8\mathbb{Z}$ nor the quaternion group Q_8. $\sigma_{1,0}$ is an element of order 4. So we suspect that Gal$(K/\mathbb{Q})$ is isomorphic to the dihedral group D_4 since it is not abelian. Indeed, we have

$$\sigma_{c,d} \circ \sigma_{a,b}(i) = \sigma_{c,d}((-1)^b i) = (-1)^{b+d} i$$

and

$$\begin{aligned}\sigma_{c,d} \circ \sigma_{a,b}(\sqrt[4]{2}) &= \sigma_{c,d}(i^a\sqrt[4]{2}) = \sigma_{c,d}(i^a)\sigma_{c,d}(\sqrt[4]{2}) \\ &= ((-1)^d i)^a i^c \sqrt[4]{2} = i^{a+c+2ad}\sqrt[4]{2}.\end{aligned}$$

That is

$$\sigma_{c,d} \circ \sigma_{a,b} = \sigma_{c+(1+2d)a, b+d}.$$

Therefore, Gal$(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

The following theorem of Artin gives a simple way of constructing examples of Galois extensions.

Theorem 4.10.7 (Artin)**.** *Let E be a field, and let $G \subset Aut(E)$ be a subgroup with n elements. If*

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\},$$

then E^G is a field, E/E^G is a Galois extension satisfying $G = Gal(E/E^G)$ and $[E : E^G] = n$.

We have to be somewhat careful with the theorem above. In particular, given an extension of fields E/F it is not always true (or even "usually true") that $F = E^{\text{Aut}(E/F)}$. The best one can say for sure is that $F \subset E^{\text{Aut}(E/F)}$. A good example of this is $E = \mathbb{R}$ and $F = \mathbb{Q}$, where $\text{Aut}(\mathbb{R}/\mathbb{Q})$ is trivial, and so

$$\mathbb{R}^{\text{Aut}(\mathbb{R}/\mathbb{Q})} = \mathbb{R} \neq \mathbb{Q}.$$

In this case, Artin's Theorem just says that $\mathbb{R}/\mathbb{R}$ is a Galois extension with trivial Galois group. This should actually be somewhat reassuring, since $[\mathbb{R} : \mathbb{Q}]$ is not finite!

Before proving Artin's Theorem, we will state a lemma which will be needed.

Lemma 4.10.8. *Let E/F be a separable, algebraic extension. Suppose that for some natural number n, every $\alpha \in E$ satisfies $[F(\alpha) : F] \leq n$. Then E/F is a finite extension, and $[E : F] \leq n$.*

Proof. Let n in the statement be as small as possible, and choose $\alpha \in E$ such that $[F(\alpha) : F] = n$.

We claim that, in fact, $E = F(\alpha)$.

If not, then there is some $\beta \in E \setminus F(\alpha)$, and so $F(\alpha, \beta)$ is a proper extension of $F(\alpha)$. Now, $F(\alpha, \beta)/F$ is a finite, separable extension of fields, and so by Theorem 3.7.3, there is a $\gamma \in F(\alpha, \beta)$ with $F(\alpha, \beta) = F(\gamma)$. But since $\beta \notin F(\alpha)$, we have $\gamma \in E$ and

$$[F(\gamma) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] > [F(\alpha) : F] = n.$$

This is impossible by the hypotheses of the theorem, and so we must have had $E = F(\alpha)$. □

Proof of Theorem 4.10.7. It is easy to check that E^G is a subfield of E. We need to show that E/E^G is a finite, separable, and normal extension. For each element $\alpha \in E$, choose a subset $S \subset G$ such that $\{\sigma(\alpha) : \sigma \in S\}$ is as large as possible, but such that $\sigma_1(\alpha) \neq \sigma_2(\alpha)$ for $\sigma_1 \neq \sigma_2$. Now define

$$f_\alpha(x) = \prod_{\sigma \in S} (x - \sigma(\alpha)) \in E[x].$$

Our first claim is that $f_\alpha(x) \in E^G[x]$. To see this, first note that if $\tau \in G$, then

$$\{\tau \circ \sigma(\alpha) : \sigma \in S\} \subset \{\sigma(\alpha) : \sigma \in S\}.$$

If not, then there is some $\sigma \in S$ such that $\tau \circ \sigma(\alpha)$ is distinct from all $\sigma'(\alpha)$ for $\sigma' \in S$, and so $S \sup\{\tau \circ \sigma\}$ contradicts the maximality of S. But τ is an injection, so

$$|\{\tau \circ \sigma(\alpha) : \sigma \in S\}| = |\{\sigma(\alpha) : \sigma \in S\}|$$

and hence the inclusion above shows that

$$\{\tau \circ \sigma(\alpha) : \sigma \in S\} = \{\sigma(\alpha) : \sigma \in S\}.$$

So applying $\tau \in S$ to the elements of $\{\sigma(\alpha) : \sigma \in S\}$ simply permutes them. But the coefficients of $f_\alpha(x)$ are symmetric in the $\sigma(\alpha)$, and so they are fixed by τ. Since $\tau \in G$ was arbitrary, the coefficients of $f_\alpha(x)$ are in E^G.

Now, we also note that $f_\alpha(\alpha) = 0$. If not, adding the identity map to S would again contradict the maximality of S. Thus α is the root of the polynomial $f_\alpha(x) \in E^G[x]$ which, by construction, has no repeated roots, and has degree at most $|G|$. As $\alpha \in E$ was arbitrary, we see that the extension E/E^G is algebraic and separable, and that for all $\alpha \in E, [E^G(\alpha) : E^G] \leq |G|$. By the preceding lemma, we may conclude that E/E^G is a finite extension of degree at most $|G|$. Now, note that any element of G fixes E^G (by definition), and so $G \subset \text{Aut}(E/E^G)$. But combining the fact E/E^G is a finite, separable extension this gives

$$|G| \leq |\text{Aut}(E/E^G)| \leq [E : E^G] \leq |G|.$$

And so in fact we have the equalities above and that the equality $\text{Aut}(E/E^G) = [E : EG]$ implies E/E^G is normal by Theorem 4.10.1. Therefore, E/E^G is Galois and $\text{Gal}(E/E^G) = G$. □

Artin's Theorem has an immediate, and very useful, corollary:

Corollary 4.10.9. *If E/F is a finite Galois extension, then $E^{Gal(E/F)} = F$.*

Proof. It's clear that $F \subset E^{\text{Gal}(E/F)} \subset E$, simply because every element of F is fixed by every element of $\text{Gal}(E/F)$. So we have

$$|\text{Gal}(E/F)| = [E : F] = [E : E^{\text{Gal}(E/F)}][E^{\text{Gal}(E/F)} : F] = |\text{Gal}(E/F)|[E^{\text{Gal}(E/F)} : F].$$

It must be the case that $[E^{\text{Gal}(E/F)} : F] = 1$, and so the fields are the same. □

Example 4.10.10. We know that $\mathbb{C}/\mathbb{R}$ is a Galois extension, with Galois group generated by complex conjugation. The corollary above shows that $\mathbb{R}$ is exactly the set of complex numbers fixed by complex conjugation (which, of course, we already knew).

By contrast, if $E = \mathbb{Q}(\sqrt[3]{2})$, we know that $E^{\text{Aut}(E/\mathbb{Q})} = E \neq \mathbb{Q}$.

Corollary 4.10.11. *For every finite group G, there is a Galois extension E/F such that*

$$\textit{Gal}(E/F) \cong G.$$

Proof. Write $G = \{g_1, \cdots, g_n\}$. Take $E = \mathbb{Q}(x_{g_1}, \cdots, x_{g_n})$ the fraction field of n indeterminates which are labeled by elements of G. Then we can extend the canonical the action of G on $\{x_{g_1}, \cdots, x_{g_n}\}$ to E via

$$\sigma_g : E \to E, \quad \frac{f(x_{g_1}, \cdots, x_{g_n})}{g(x_{g_1}, \cdots, x_{g_n})} \mapsto \frac{f(x_{gg_1}, \cdots, x_{gg_n})}{g(x_{gg_1}, \cdots, x_{gg_n})},$$

for each element $g \in G$. It is straightforward to check σ_g is an automorphism fixing $\mathbb{Q}$. By Artin's Theorem, E/E^{S_n} is Galois. By the fundamental theorem, E/E^G is also a Galois extension with Galois group G. □

4.11 The Fundamental Theorem

The original aim was to understand finite field extensions E/F using the group $\text{Aut}(E/F)$. In general, it's possible that E/F is non-trivial, but $\text{Aut}(E/F)$ is trivial, which means in general it's unlikely that $\text{Aut}(E/F)$ will shed a lot of light on the structure of E/F. In the case where E/F is Galois, though,

we know that $\text{Aut}(E/F)$ is as large as it possibly could be, and hence gives as much information as possible. One might expect, than, that Galois extensions are the ones for which $\text{Aut}(E/F)$ gives as much information as possible. The purpose of this section is to show that $\text{Gal}(E/F)$ gives a great deal of information about the intermediate fields. Artin's Theorem raises a natural question: Given a finite Galois extension E/F, for any subgroup $H \subset \text{Gal}(E/F)$, the field E^H is a subfield of E, and E/E^H is a Galois extension; what is the exact relation between H and E^H?

For one thing, if $H \subset \text{Gal}(E/F)$, then $F \subset E^H \subset E$, and E/E^H is a Galois extension of degree $|H|$. All of this follows from Artin's Theorem. Perhaps surprisingly, it turns out that this function is both injective and surjective (onto the collection of intermediate fields between E and F). This is, essentially, the fundamental theorem of Galois Theory. We will prove this theorem as a sequence of lemmas, and then state the complete result at the end of the section.

Lemma 4.11.1. *Let E/F be a finite Galois extension. Then the function $H \mapsto E^H$, defined on subgroups of Gal(E/F), is inclusion-reversing.*

Proof. We want to show that if $H_1 \subset H_2$ are two subgroups of E, then $E^{H_1} \supseteq E^{H_2}$. Suppose that $\alpha \in E^{H_2}$. Then for every $\sigma \in H_2$, we have $\sigma(\alpha) = \alpha$. But $H_1 \subset H_2$, so $\sigma(\alpha) = \alpha$ for every $\sigma \in H_1$. This shows that $\alpha \in E^{H_1}$. Since $\alpha \in E^{H_2}$ was arbitrary, we have $E^{H_1} \supseteq E^{H_2}$. □

Lemma 4.11.2. *Let E/F be a finite Galois extension. Then the function $H \mapsto E^H$ is a bijection between subgroups of Gal(E/F) and intermediate fields $F \subset K \subset E$.*

Proof. We will prove this by exhibiting an inverse for the function $H \mapsto E^H$. We claim that the inverse function is $K \mapsto \text{Gal}(E/K)$. One side of this is Artin's Theorem, which shows that E/E^H is a Galois extension, and $\text{Gal}(E/E^H) = H$. On the other hand, if $F \subset K \subset E$, then E/K is a finite, separable extension (separability follows from the fact that the minimal polynomial of any element of E over K divides the minimal polynomial over F, which will have no repeated roots). The extension E/K also has to be normal, because if E is the splitting field of $f(x) \in F[x]$ over F, then E is also the splitting field of $f(x)$ over K. So E/K is a Galois extension whenever $F \subset K \subset E$. It follows from Corollary 4.10.9 that $E^{\text{Gal}(E/K)} = K$. Thus we've shown that the maps $H \mapsto E^H$ and $K \mapsto \text{Gal}(E/K)$ are inverses. They are, then, both bijections. □

It is always true, when E/F is a finite Galois extension, and $F \subset K \subset E$, that E/K is a Galois extension, as noted in the proof above. It is *not* typically true that K/F is also a Galois extension. A lemma below tells us precisely when this happens, but first we'll see a simple example of the bijection above.

Example 4.11.3. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then E is the splitting field over $\mathbb{Q}$ of the polynomial $(x^2 - 2)(x^2 - 3)$, and hence is a Galois extension. As we've seen before, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. This confirms the plausible statement that $[E : \mathbb{Q}] = 4$. So there are four automorphisms of E fixing $\mathbb{Q}$, and they are defined by what they do to $\sqrt{2}$ and $\sqrt{3}$. If $\sigma \in \text{Gal}(E/\mathbb{Q})$, then $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$. So we see precisely what the four automorphisms are. Indeed, $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, by the isomorphism $(a, b) \mapsto \sigma_{a,b}$ defined by

$$\sigma_{a,b}(\sqrt{2}) = (-1)^a\sqrt{2} \text{ and } \sigma_{a,b}(\sqrt{3}) = (-1)^b\sqrt{3}.$$

The group $\text{Gal}(E/\mathbb{Q})$ has three distinct subgroups:

$$H_1 = \{id, \sigma_{1,0}\}, H_2 = \{id, \sigma_{0,1}\}, H_3 = \{id, \sigma_{1,1}\}.$$

We see that each of the fields $E^{H_1}, E^{H_2}, E^{H_3}$ are degree 2 extensions of $\mathbb{Q}$. Since $\sigma_{1,0}(\sqrt{3}) = \sqrt{3}, \sigma_{0,1}(\sqrt{2}) = \sqrt{2}$ and $\sigma_{1,1}(\sqrt{6}) = \sqrt{6}$, we see that

$$E^{H_1} = \mathbb{Q}(\sqrt{3}), E^{H_2} = \mathbb{Q}(\sqrt{2}), E^{H_3} = \mathbb{Q}(\sqrt{6}).$$

By the lemmas above, these three fields (along with F and E) are the only intermediate fields between F and E.

We now return to the question of when an intermediate field is a Galois extension of F.

Lemma 4.11.4. *Let E/F be a finite Galois extension, and let $F \subset K \subset E$. Then K/F is a Galois extension if and only if Gal$(E/K) \subset$ Gal(E/F) is a normal subgroup. Furthermore, in the case that K/F is a Galois extension, we have*

$$\textit{Gal}(K/F) \cong \textit{Gal}(E/F)/\textit{Gal}(E/K).$$

Before beginning the proof, we note that since E/F is separable, it is automatic that K/F is separable. Thus the lemma says that K/F is normal if and only if $\mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F)$ is normal.

Proof. First we suppose that K/F is a Galois (indeed, normal) extension of E, and define a homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$. Let $\sigma \in \mathrm{Gal}(E/F)$, and let $\alpha \in K$ have minimal polynomial $f(x) \in F[x]$ over F.

Since $f(\sigma(\beta)) = \sigma(f(\beta))$ for all $\beta \in E$, we see that $\sigma(\alpha)$ must be a root of $f(x)$. But $f(x)$ is an irreducible polynomial over F with a root in K and so, by the definition of a normal extension, all of the roots of $f(x)$ are in K. Thus $\sigma(\alpha) \in K$. So $\sigma|_K$, the restriction of σ to K, is an injective homomorphism whose image is contained in K. But it must also be a surjective map, since $\sigma^{-1}|_K$ has the same property. Thus $\sigma|_K$ is an automorphism of K for any $\sigma \in \mathrm{Gal}(E/F)$, and clearly this automorphism of K fixes F. This shows that $\sigma \mapsto \sigma|_K$ is a well-defined map $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$. It is easy to check that $(\sigma\circ\tau)|_K = \sigma|_K \circ \tau|_K$, so this map is a homomorphism. It also must be surjective, since any automorphism $\tau \in \mathrm{Gal}(K/F)$ is an embedding $K \to F$ fixing F, which extends to an embedding $E \to F$ fixing F by Lemma 2.4.9, and this extension will be an element of $\mathrm{Gal}(E/F)$ by Theorem 2.5.12. Thus we have a surjective homomorphism $\phi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$, and by the first isomorphism theorem,

$$\mathrm{Gal}(E/F)/\ker(\phi) \cong \mathrm{Gal}(K/F).$$

It remains to show that $\ker(\phi) = \mathrm{Gal}(E/K)$, which will also show that the latter subgroup is normal. But $\sigma \in \ker(\phi)$ if and only if $\sigma|_K$ is trivial, which happens if and only if $\sigma(x) = x$ for all $x \in K$. Thus $\sigma \in \ker(\phi)$ if and only if $\sigma \in \mathrm{Gal}(E/K)$. This completes one direction of the proof, and shows that in this case $\mathrm{Gal}(K/F)$ is the expected quotient.

The other direction, suppose that H is a normal subgroup of $\mathrm{Gal}(E/F)$. Then $\mathrm{Gal}(E/E^H) = H$. Fix an algebraic closure $\overline{F}$ of F. Note $\overline{F}$ is also an algebraic closure of E^H and E. Consider an F-map $\sigma : E^H \to \overline{F}$ and let us show $\sigma(E^H) = E^H$ and then by the equivalent conditions of normality, E^H/H is normal hence Galois. Extend σ to a F-map $\sigma' : E \to \overline{F}$. Since E/F is normal, $\sigma'(E) = E$, it follows that $\sigma(E^H) \subset E$. Now let $b \in \sigma(E^H)$, say $b = \sigma(a) = \sigma'(a)$ for some $a \in E^H$. To check $b \in E^H$, we need show b is fixed by all elements in H. Since H is normal, we have $\sigma' H = H\sigma'$. For any element $\tau \in H$, we can find another element $\tau' \in H$ such that

$$\tau \circ \sigma' = \sigma' \circ \tau'.$$

And then

$$\tau(b) = \tau \circ \sigma'(a) = \sigma' \circ \tau'(a) = \sigma'(a) = b,$$

since $a \in E^H$. It follows that $\sigma(E^H) \subset E^H$. Repeating the argument for σ^{-1}, we see that $\sigma^{-1}(E^H) \subset E^H$ and conclude that $\sigma(E^H) = E^H$ since $\sigma \circ \sigma^{-1} = id|_{\sigma(E^H)}$ and $\sigma^{-1} \circ \sigma = id|_{E^H}$. □

All in all, we've proven the following theorem.

Theorem 4.11.5 (The fundamental theorem of Galois Theory)**.** *Let E/F be a Galois extension. Then the function $H \mapsto E^H$ from subgroups of Gal(E/F) to intermediate fields of E/F is an inclusion-reversing bijection, and the inverse is given by $K \mapsto$ Gal(E/K). Moreover, $H \trianglelefteq$ Gal(E/F) if and only if $K = E^H$ is a Galois extension of F, in which case*

$$\textit{Gal}(E/F)/\textit{Gal}(E/K) \cong \textit{Gal}(K/F).$$

Corollary 4.11.6. *Every finite separable field extension L/K admits only finitely many intermediate fields.*

Proof. Pass to the normal closure L'/K. Then it is Galois and hence admits only finitely many intermediate fields. □

Example 4.11.7. In the example $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, as an extension of $\mathbb{Q}$, the Galois group is $C_2 \times C_2$. Three non-trivial proper subgroups are all normal. The corresponding intermediate fields are all Galois extensions of $\mathbb{Q}$.

Example 4.11.8. Let $E/\mathbb{Q}$ be the splitting field of $x^3 - 2$, so that $E = \mathbb{Q}(\alpha; \omega)$, where $\alpha^3 = 2$ (it does not matter, but we can specify $\alpha \in \mathbb{R}$), and ω is a primitive cube root of unity. As a splitting field over a perfect field, this is automatically a Galois extension, and since $[E : \mathbb{Q}] = 6$, we see that the Galois automorphisms are exactly the functions $\sigma_{a,b}$ defined by

$$\sigma_{a,b}(\alpha) = \omega^a \alpha, \sigma_{a,b}(\omega) = \omega^{2^b}.$$

Note that $\omega^3 = 1$ and $\omega^{2^2} = \omega$, we can take $a \in \mathbb{Z}/3\mathbb{Z}$ and $b \in \mathbb{Z}/2\mathbb{Z}$. And then we can compute the group operation explicitly:

$$\sigma_{c,d} \circ \sigma_{a,b}(\omega) = \sigma_{c,d}(\omega^{2^b}) = (\sigma^{2^d})^{2^b} = \sigma^{2^{b+d}}$$

and

$$\sigma_{c,d} \circ \sigma_{a,b}(\alpha) = \sigma_{c,d}(\omega^a \alpha) = (\omega^{2^d})^a \omega^c \alpha.$$

In other words,

$$\sigma_{c,d} \circ \sigma_{a,b} = \sigma_{c+2^d a, b+d}.$$

This gives an explicit isomorphism between Gal$(E/\mathbb{Q})$ and a certain semidirect product of $\mathbb{Z}/3\mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z}$. Indeed, since the group is not abelian, we have Gal$(E/\mathbb{Q}) \cong S_3$.

Now the subgroups of Gal(E/F) (other than the group itself, and the trivial subgroup) have order either 2 or 3, and so must be cyclic. We simply need to identify the elements of Gal(E/F) of order 2 or 3. One checks that $\sigma_{a,0} \circ \sigma b, 0 = \sigma_{a+b,0}$, and so the elements $\sigma_{1,0}$ and $\sigma_{2,0}$ generate the same subgroup of order 3. Also note that $\sigma_{0,1}^2 = \sigma_{1,1}^2 = \sigma_{2,1}^2 = id$, so the remaining three elements of this group of order 6 each have order 2. Now, $E^{\langle \sigma_{1,0} \rangle} \subset E$ should satisfy $[E : E^{\langle \sigma_{1,0} \rangle}] = 3$. Note that $\sigma_{1,0}(\omega) = \omega$, and $[E : \mathbb{Q}(\omega)] = 3$, so we must have $E^{\langle \sigma_{1,0} \rangle} = \mathbb{Q}(\omega)$. Similarly, $[E : E^{\langle \sigma_{0,1} \rangle}] = 2$, and $\sigma_{0,1}(\alpha) = \alpha$, so we must have $E^{\langle \sigma_{0,1} \rangle} = \mathbb{Q}(\alpha)$. Finally, a bit of trial-and-error shows that $\sigma_{1,1}(\omega^2 \alpha) = \omega^2 \alpha$, and $\sigma_{2,1}(\omega\alpha) = \omega\alpha$, and so comparing degrees gives $E^{\langle \sigma_{1,1} \rangle} = \mathbb{Q}(\omega^2 \alpha)$ and $E^{\langle \sigma_{2,1} \rangle} = \mathbb{Q}(\omega\alpha)$.

The one thing that remains is to decide which of these is a Galois extension of $\mathbb{Q}$. Let's cheat here: the only non-trivial proper normal subgroup of S_3 is A_3, so as we already see that $\mathbb{Q}(\omega)$ (being quadratic) is, while the other three are not.

Example 4.11.9. This example is an exercise from Isaacs's Algebra. Let $p_1, \cdots, p_n$ be distinct primes. Consider $E = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$. Since $\mathbb{Q}$ is perfect, $E/\mathbb{Q}$ is separable. E being the splitting field of $(x^2 - p_1) \cdots (x^2 - p_n) \in \mathbb{Q}[x]$ over $\mathbb{Q}$ is also normal. Therefore, $E/\mathbb{Q}$ is Galois. We need two lemmas to see $[E : \mathbb{Q}] = 2^n$,

Lemma 4.11.10. *Let a, b be in K and char$(K) \neq 2$. Then $[K(\sqrt{a}, \sqrt{b}) : K] = 4$ if and only if none of $\sqrt{a}, \sqrt{b}, \sqrt{ab}$ lies in K.*

Proof. Only-if part is clear.

Let $L = K(\sqrt{b})$. Then $[L : K] = 2$ since $\sqrt{b} \notin K$ and char$(K) \neq 2$. It suffices to show that $[L(\sqrt{a}) : L] = 2$. This fails only if $\sqrt{a} \in L = K(\sqrt{b})$. Then we have $\sqrt{a} = r + s\sqrt{b}$ for some $r, s \in K$. Squaring it, we get

$$a = r^2 + bs^2 + 2rs\sqrt{b}.$$

If $rs \neq 0$, then we get $\sqrt{b} \in K$, a contradiction. If $s = 0$, then $\sqrt{a} = r$, a contradiction. If $r = 0$, then $\sqrt{ab} \in K$, a contradiction. □

Lemma 4.11.11. *Let Q be a field with char$(Q) \neq 2$, and $L = Q(S)$ be an extension of Q generated by n square roots $S = \{\sqrt{a}, \sqrt{b}, \cdots\}$ of $a, b \cdot \in Q$. If every nonempty subset of S has a product not in Q, then each successive adjunction $Q(\sqrt{a}), Q(\sqrt{a}, \sqrt{b}), \cdots$ double degree over Q and so $[L : Q] = 2^n$.*

Proof. We induct on the height $n =$ number of root adjunctions.

Base case: $n = 1$. $L = Q(\sqrt{a})$ so $[L : Q] = 2$ since $\sqrt{a} \notin Q$ by hypothesis.

Induction step: $n > 1$. Let $L = K(\sqrt{a}, \sqrt{b})$, and K of height $n - 2$. By induction hypothesis, $[K : Q] = 2^{n-2}$. Again by induction hypothesis, $[K(r) : K] = 2$ where $K(r)$ is of hight $n - 1$ and r is any one of $\sqrt{a}, \sqrt{b}, \sqrt{ab}$. By the lemma above, $[L : K] = 4$ since none of $\sqrt{a}, \sqrt{b}, \sqrt{ab}$ is in K. □

From the lemma above, we immediately get $[E : \mathbb{Q}] = 2^n$. Writing $C_2 = \{-1, 1\}$, we define a map

$$\text{Gal}(E/\mathbb{Q}) \to \{-1, 1\}^n, \sigma \mapsto (\frac{\sigma(\sqrt{p_1})}{\sqrt{p_1}}, \cdots, \frac{\sigma(\sqrt{p_n})}{\sqrt{p_n}}).$$

This is a well-defined map, indeed a group homomorphism, since $\sigma(\sqrt{p_i}) = \pm\sqrt{p_i}$ for $i = 1, \cdot, n$. Moreover, each $\sigma \in \text{Gal}(E/\mathbb{Q})$ is uniquely determined by its action on $\sqrt{p_i}$. The map is also injection and by counting elements we conclude that $\text{Gal}(E/\mathbb{Q}) \cong \{-1, 1\}^n$. Now consider the element $\alpha = \sqrt{p_1} + \cdots + \sqrt{p_n}$. It is fixed by the identity element only and so by the fundamental theorem $\text{Gal}(E/\mathbb{Q}(\alpha)) = \{id\}$. It follows that

$$\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_n}).$$

Week 5

We have already seen one broad class of Galois extensions, namely the quadratic extensions (of a field of characteristic other than 2). In this part of the notes, we'll see some more families of examples.

5.12 Cyclotomic Extensions

Cyclotomic extensions are extensions generated by roots of unity. Recall that we have Equation 2.2.

Definition 5.12.1. If d is a positive integer, then the d-th cyclotomic polynomial is defined by

$$\Phi_d(x) = \prod(x - \zeta),$$

where ζ ranges over all the primitive d-th roots of unity.

Theorem 5.12.2. *Let n be a positive integer and regard $x^n - 1 \in \mathbb{Z}[x]$. Then*

1. $$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

   where d ranges over all the positive divisors d of n (in particular, $\Phi_1(x) = x - 1$ and $\Phi_n(x)$ occur).

2. *$\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ and $\deg(\Phi_n) = \phi(n)$, the Euler ϕ-function.*

3. *For every integer $n \geq 1$, we have $n = \sum_{d|n} \phi(d)$.*

4. *Each $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Actually, part (3) is a classical result in number theory.

1. For each divisor d of n, collect all terms in the equation $x^n - 1 = \prod(x - \zeta)$ with ζ a primitive d-th root of unity, since every n-th root of unity is a primitive d-th root of unity for some divisor d of n.

2. We prove that $\Phi_n(x) \in \mathbb{Z}[x]$ by induction on $n \geq 1$. The base step is true, for $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. For the inductive step, let $f(x) = \prod_{d|n, d<n} \Phi_d(x)$, so that

   $$x^n - 1 = f(x)\Phi_n(x).$$

   By induction, each $\Phi_d(x)$ is a monic polynomial in $\mathbb{Z}[x]$, and so f is a monic polynomial in $\mathbb{Z}[x]$. Now f divides $x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$, where ζ_n is a primitive n-th root, hence also divides it in $\mathbb{Q}[x]$ by the division algorithm. Gauss' Lemma that the quotient $\Phi_n(x) = (x^n - 1)/f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ indeed.

3. Immediately from (1) and (2):

$$n = \deg(x^n - 1) = \deg(\prod_{d|n} \Phi_n(x)) = \sum_{d|n} \deg(\Phi_n(x)) = \sum_{d|n} \phi(d).$$

4. The case when $n = p$ is a prime is easy to prove by Eisenstein's Criterion. The general case is highly non-trivial. Suppose that $\Phi_n(x) = f(x)g(x)$ in $\mathbb{Q}[x]$ with f of positive degree. With Gauss' lemma, we can suppose that both f and g are monic and are in $\mathbb{Z}[x]$. Let $x - \zeta$ be a linear factor of $f(x)$ in $k[x]$ for an extension field k of $\mathbb{Q}$. We wish to show that $x - \zeta^a$ is also a linear factor of f for every $a \in (\mathbb{Z}/n\mathbb{Z})^*$, and thus that

$$\deg f = \phi(n) = \deg(\Phi_n)$$

concluding that $f = \Phi_n$.

Since each $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is a product of primes p not dividing n, it suffices to show that $x - \zeta^p$ is a linear factor of $f(x)$ for all primes p not dividing n, and the iterating the results $x - \zeta^a$ is also a root. If not, then $x - \zeta^p$ is necessarily a linear factor of $g(x)$, by unique factorization in $k[x]$. That is, ζ is a root of $g(x^p) = 0$ in $k[x]$, so $x - \zeta$ divides $g(x^p)$ in $k[x]$. Thus, in $\mathbb{Q}[x]$ the $\gcd$ of $f(x)$ and $g'(x) = g(x^p)$ is not 1 — they are both divisible by the minimal polynomial of ζ in $\mathbb{Q}[x]$. Let's say

$$f(x) = a(x)d(x) \text{ and } g(x^p) = b(x)d(x),$$

where $a(x), b(x), d(x)$ are all monic in $\mathbb{Z}[x]$.

Mapping everything to $\mathbb{F}_p[x]$, where $g(x^p) = g(x)^p$, we have $g(x)^p = b(x)d(x)$ in $\mathbb{F}_p[x]$. Let $\delta(x) \in \mathbb{F}_p[x]$ be an irreducible dividing $d(x)$ in $\mathbb{F}_p[x]$. Then since $\delta(x)$ divides $g(x)^p$ in $\mathbb{F}_p[x]$, it divides $g(x)$. Also $\delta(x)$ divides $f(x)$ in $\mathbb{F}_p[x]$, so $\delta(x)^2$ apparently divides $\Phi_n(x) = f(x)g(x)$ in $\mathbb{F}_p[x]$. But p does not divide n, $\gcd(x^n - 1, nx^{n-1} - 1) = 1$ and so $x^n - 1$ and thus $\Phi_n(x)$ has no repeated root in $\mathbb{F}_p[x]$, contradiction. Thus, it could not have been that $\Phi_n(x)$ factored properly in $\mathbb{Q}[x]$.

□

We can calculate the cyclotomic polynomials based on this theorem without going into complex analysis. Here is a list of first few ones:

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
&\cdots
\end{aligned}$$

Theorem 5.12.3. *Let $N \geq 1$, and let ζ be a root of Φ_N. Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension of degree $\phi(N)$, with*

$$\textit{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times.$$

An extension of the above sort is called a *cyclotomic extension*.

Proof. Since $\Phi_N(x)$ is irreducible over $\mathbb{Q}$, we have

$$[E : \mathbb{Q}] = \deg(\Phi_N) = \phi(N).$$

Also, note that if $\Phi_N(\zeta) = 0$, then the roots of $\Phi_N(x)$ in $\mathbb{C}$ are precisely the numbers of the form ζ^a for $\gcd(a, N) = 1$, all of which are in $E = \mathbb{Q}(\zeta)$. So $E/\mathbb{Q}$ is a normal extension, and hence Galois. Now, any $\sigma \in \text{Gal}(E/\mathbb{Q})$ is entirely determined by what it does to ζ, and $\sigma(\zeta)$ must be ζ^a for some $\gcd(a, N) = 1$. Since there are precisely $\phi(N)$ such values of $a \pmod N$, and since $|\text{Gal}(E/\mathbb{Q}) = \phi(N)$, we must have an automorphism $\sigma_a \in \text{Gal}(E/\mathbb{Q})$ defined by $\sigma_a(\zeta) = \zeta^a$ for each $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. But the group operation is

$$\sigma_a \circ \sigma_b = \sigma_{ab},$$

and so the bijection $a \mapsto \sigma_a$ is actually an isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \to \text{Gal}(E/\mathbb{Q})$. □

Note that $\phi(N)$ is even for $N \geq 3$, which you can see either by developing the formula for $\phi(N)$ in terms of the prime factorization of N:

$$\phi(p_1^{e_1} \cdots p_n^{e_n}) = (p_1 - 1)p_1^{e_1 - 1} \cdots (p_n - 1)p_n^{e_n - 1},$$

or by noting the non-triviality of the automorphism $x \mapsto -x$ of the unit group in $\mathbb{Z}/N\mathbb{Z}$. In particular, there is an element of order 2 in $\text{Gal}(E/\mathbb{Q})$, and hence a field of which E is a quadratic extension. It turns out to be relatively easy to describe this field. The automorphism $x \mapsto -x$ of $(\mathbb{Z}/N\mathbb{Z})^\times$ corresponds to the element $\sigma_{-1} \in \text{Gal}(E/\mathbb{Q})$. This element is exactly the complex conjugation by observing

$$e^{-2k\pi i/N} = \overline{e^{2k\pi i/N}}.$$

In other words, the fixed field of σ_{-1} is exactly $K = E \cap \mathbb{R}$, and E is a quadratic extension of this. We can actually describe this field quite nicely. Clearly $\zeta + \zeta^{-1} \in K$, since it is fixed by $\zeta \mapsto \zeta^{-1}$, and so $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K$. We could use an argument about symmetric polynomials to conclude that everything fixed by σ_{-1} is actually a polynomial in $\zeta + \zeta^{-1}$, but there is a more direct proof that in fact $K = \mathbb{Q}(\zeta + \zeta^{-1})$. To see this, note that

$$\zeta^2 - (\zeta + \zeta^{-1})\zeta + 1 = 0,$$

and so ζ satisfies a quadratic polynomial over $\mathbb{Q}(\zeta + \zeta^{-1})$. Thus,

$$\mathbb{Q}(\zeta + \zeta^{-1}) \subset K \subset E,$$

with $[E : K] = 2$, and $[E : \mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$. It follows that $K = \mathbb{Q}(\zeta + \zeta^{-1})$.

Perhaps the most amazing fact about cyclotomic extensions is that, at least over $\mathbb{Q}$, they completely explain abelian extensions.

Theorem 5.12.4 (Kronecker-Weber)**.** *Let $E/\mathbb{Q}$ be a finite Galois extension such that Gal$(E/\mathbb{Q})$ is abelian. Then there is a root of unity ζ such that $E \subset \mathbb{Q}(\zeta)$.*

In particular, every quadratic extension over $\mathbb{Q}$ is contained in some cyclotomic extension. This theorem is one of the earliest known results in class field theory. We shall prove it. But the proof requires sophisticated tools like ramification theory and so let's push on at this stage.

Let us see some examples before ending this section.

Example 5.12.5. Let $K = \mathbb{Q}(\zeta_7)$ and then $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$, which is a cyclic group 6. Write $\text{Gal}(K/\mathbb{Q}) = \{\sigma_i : i = 1, \cdots, 6\}$, where $\sigma(\zeta_7) = \zeta_7^i$. Then $\sigma_1 = id$ and σ_3 is a generator. Moreover, $\sigma_i \circ \sigma_j = \sigma_{ij}$. The nontrivial proper subgroups are $\langle\sigma_3^3\rangle, \langle\sigma_3^2\rangle$. Let $L = K^{\langle\sigma_3^3\rangle} = K^{\sigma_3^3} = K^{\sigma_6}$. Then $[K : L] = |\langle\sigma_3^3\rangle| = 2$. The unique intermediate extension is discussed above $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(\cos(2\pi/7))$. Now let $M = K^{\langle\sigma_3^2\rangle} = K^{\sigma_3^2} = K^{\sigma_2}$. Note $\sigma_2^3 = id$ and then

$$\alpha = \zeta_7 + \sigma_2(\zeta_7) + \sigma_2^2(\zeta_7) = \zeta_7 + \zeta_7^2 + \zeta_7^4$$

is easy to be checked to be fixed by σ_2. Since $[M : \mathbb{Q}] = 2$, it is enough to show $\alpha \notin \mathbb{Q}$. If yes, then we reach a contradiaction that ζ_7 satisfies a polynomial $x^4 + x^2 + x - \alpha \in \mathbb{Q}[x]$ of degree 4.

5.13 Cubic Extensions

We've seen that, at least if $\text{char}(F) \neq 2$, every extension of degree 2 is Galois. We know that this is not true for extensions of degree 3, since $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a Galois extension. Rather than address the problem of which degree-three extensions of a field are Galois, we'll instead ask what the splitting field of a cubic polynomial looks like (which ultimately answers the other question).

Let F be a field with $\text{char}(F) \neq 2$ or 3, let $f(x) = x^3 + ax + b$ be an irreducible cubic polynomial. (We may assume F to be perfect. But we will see it is really not necessary. We will see more about separable extensions later.) Note we can always complete the cube to write $f(x)$ in this way by replacing x with $x - p/3$ and we do need $\text{char}(F) \neq 3$. Let $f(\alpha) = 0$. If E/F is the splitting field of $f(x)$ over F, then since $f(x)$ has a linear factor over $F(\alpha)$, we have $[E : F(\alpha)] \leq 2$, and so $[E : F] = 3$ or 6. $f(x)$ factors into three linear terms or a product of a linear term and a quadratic in $F(\alpha)[x]$. Since $\text{char}(F) \neq 2$, the quadratic is separable and so is $f(x)$. Note that $\text{Gal}(E/F)$ is a subgroup of S_3, the symmetric group on the three roots of $f(x)$, and so the question of whether or not $E = F(\alpha)$ comes down to whether or not $\text{Gal}(E/F)$ contains an element of order 2; if it does, it is the full group S_3, and if it doesn't it's the alternating group A_3.

Let $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ in $E[x]$, and let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3).$$

Then clearly $\sigma(\delta) = \pm\delta$ for each $\sigma \in \text{Gal}(E/F)$. It is easy to check that an arbitrary transposition of two elements in $\{\alpha_1, \alpha_2, \alpha_3\}$ changes the sign of δ, and so for $\sigma \in \text{Gal}(E/F) \subset S_3$ a permutation of the α_i, we have

$$\sigma(\delta) = (-1)^{\text{sgn}(\sigma)}\delta.$$

In other words, if $\text{Gal}(E/F) = A_3$, then $\sigma(\delta) = \delta$ for all $\sigma \in \text{Gal}(E/F)$, and so $\delta \in F$. If $\text{Gal}(E/F) = S_3$, then $\text{Gal}(E/F)$ contains an odd element which doesn't fix δ, and hence $\delta \notin F$. But $\delta^2 \in F$, since $\sigma(\delta^2) = (\pm\delta)^2 = \delta^2$ for all $\sigma \in \text{Gal}(E/F)$. Note that, in the case that $\text{Gal}(E/F) \cong S_3$, so that $\delta \notin F$, there must be a quadratic extension of F corresponding to the subgroup $A_3 \subset \text{Gal}(E/F)$. But clearly $\delta \in E$, and $\delta^2 \in F$, so $F(\delta)$ is precisely this quadratic extension. A simple calculation shows that

$$\Delta = \delta^2 = -(4a^3 + 27b^2).$$

Theorem 5.13.1. *Let F be a field with $\text{char}(F) \neq 2$ or 3, let $f(x) = x^3 + ax + b \in F[x]$ be irreducible, let E be the splitting field of $f(x)$ over F. Then if $\Delta = -(4a^3 + 27b^2)$ is the square of an element in F, then $\text{Gal}(E/F) \cong A_3$. Otherwise, if Δ is not a square, then $\text{Gal}(E/F) \cong S_3$.*

Example 5.13.2. We can check that $x^3 - x - 1$ has no roots in $\mathbb{Q}$, and hence (being cubic) is irreducible. We can also calculate the discriminant:

$$\Delta(x^3 - x - 1) = -(4(-1)^3 + 27(-1)^2) = -23.$$

This is not a square in $\mathbb{Q}$, and so if E is the splitting field of $x^3 - x - 1$, we have $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. The unique quadratic extension corresponding to $A_3 \subset S_3$ is $\mathbb{Q}(\sqrt{-23})$.

Example 5.13.3. We can check that $x^3 - 3x + 1$ is irreducible over $\mathbb{Q}$, and

$$\Delta(x^3 - 3x + 1) = 9^2.$$

Thus if $\alpha^3 - 3\alpha + 1 = 0$, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois.

Example 5.13.4. The polynomial $x^3 - x - 1$ has no roots in $\mathbb{F}_{73}$, and so (being cubic) is irreducible. We know that $\Delta(x^3 - x - 1) = -23$, but

$$14^2 + 23 = 3 \cdot 73,$$

and so -23 is a perfect square in $\mathbb{F}_{73}$. In other words, if $E/\mathbb{F}_{73}$ is the splitting field of $x^3 - x - 1$, then $\mathrm{Gal}(E/F) \cong A_3$. Note that, since $[E : \mathbb{F}_{73}] = 3$, we must have $E \cong \mathbb{F}_{73^3}$.

5.14 Quartic Functions of Special Type

Let K be a field and $f \in K[x]$ a separable polynomial. Let L be a splitting field of f over K. Then L/K is a finite Galois extension. $\mathrm{Gal}(L/K)$ is also referred as the Galois group of the equation $f(x) = 0$. Then the Galois group of a polynomial is clearly isomorphic to a subgroup of the symmetric group on the roots.

Let us look at a special kind of irreducible polynomial of degree 4, more precisely, irreducible monic polynomial $f \in \mathbb{Q}[x]$ that are biquadratic in the sense that the linear and cubic terms are trivial. Such polynomials can be written as $f(x) = (x^2 - a)^2 - b$, where we further assume $b > a^2$. For instance, $x^4 - 2$ and $x^4 - 4x^2 - 6$ are of this type.

The zeros of f in $\overline{\mathbb{Q}} \subset \mathbb{C}$ are given by

$$\alpha = \sqrt{a + \sqrt{b}}, -\alpha, \beta = \sqrt{a - \sqrt{b}}, -\beta,$$

where $\sqrt{b} > |a|$. And then we have α is real and β has a non-trivial imaginary part. The splitting field of f is given by $L = \mathbb{Q}(\alpha, \beta)$. Note that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and that $\beta^2 = a - \sqrt{b} \in \mathbb{Q}(\alpha)$ implies $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq 2$. But β has a non-trivial imaginary part and so $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. We conclude $[L : \mathbb{Q}] = 8$.

Now let us determine the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. We already G is a subgroup of the group permutations S on $\{\alpha, -\alpha, \beta, -\beta\}$ and $|G| = 8$. Moreover, every $\sigma \in G$ shall have $\sigma(-\alpha) = -\sigma(\alpha), \sigma(-\beta) = -\sigma(bb)$. Now the combinations of

$$\sigma(\alpha) \in \{\alpha, -\alpha\}, \quad \sigma(\beta) \in \{\beta, -\beta\}$$

will give you 4 possibilities. The rest elements in G shall have $\sigma(\alpha) = \pm\beta$, say $\sigma(\alpha) = \pm\beta$. Since σ is injective, we must have then $\sigma(\beta) = \pm\alpha$. This gives you another 4 possibilities:

$$\sigma(\alpha) \in \{\beta, -\beta\}, \quad \sigma(\beta) \in \{\alpha, -\alpha\}.$$

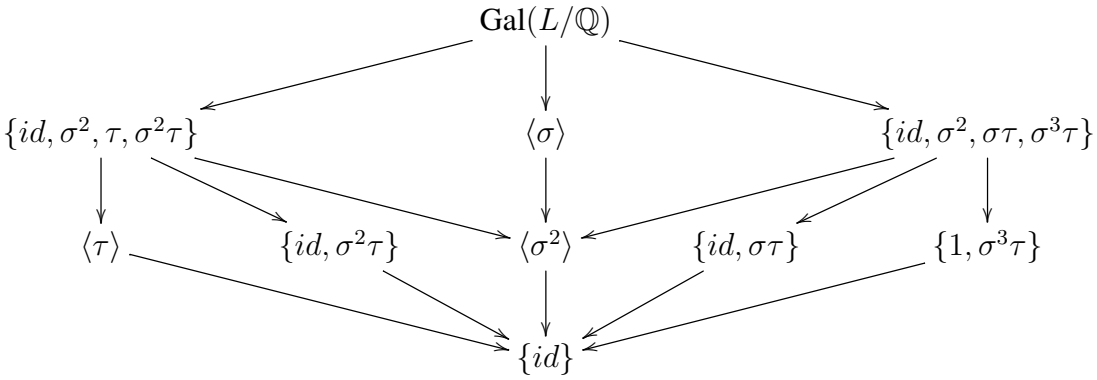
Consider two elements $\sigma, \tau \in G$ given by

$$\sigma : \alpha \mapsto \beta, \beta \mapsto -\alpha; \quad \tau : \alpha \mapsto -\alpha, \beta \mapsto \beta.$$

Now $\sigma^2(\alpha) = \sigma(\beta) = -\alpha$ and $\sigma^2(\beta) = \sigma(-\alpha) = -\beta$. Hence σ is of order 4 and clearly τ is of order 2. Since $\tau \notin \langle\sigma\rangle$, $G = \langle\tau, \sigma\rangle$. Now by checking the ration $\tau\sigma\tau = \sigma^{-1}$, we see that

$$G = \langle \tau, \sigma | \tau^2, \sigma^4, \tau\sigma\tau = \sigma^{-1} \rangle \cong D_4.$$

We can list all the subgroups of G by the following diagram:



And the intermediate fields can be determine accordingly. We will do it in lecture.

As a counterexample to the preceding type of biquadratic polynomials, let us consider $f(x) = \Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{Q}[x]$. Now if we write $f(x) = (x^2 - a)^2 - b$, then we have $a = 1/2$ and $b = -3/4$, not satisfying the above condition. And then the Galois group is isomorphic to $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 9\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.15 Inverse Galois Problems for S_p and Abelian Groups

In this section, we construct a field extension E over the rationals $\mathbb{Q}$ such that its Galois group Gal$(E/\mathbb{Q})$ is isomorphic to S_p, p prime, or Gal$(E/\mathbb{Q})$ is an arbitrary finite abelian group. If it is the latter case, the extension E is so constructed that it is a subfield of some cyclotomic extension.

Through all this section, ζ_n is a primitive n-th root and $\Phi_n(x)$ is the n-th cyclotomic polynomial, where n is a positive integer.

Lemma 5.15.1. *Let p be a prime. If a subgroup G of the symmetric group S_p contains a transposition and a p-cycle, then G is the whole group S_p.*

Proof. After renaming elements, we can assume the transposition $\sigma = (1\ 2)$. We can write a p-cycle τ as $\tau = (1\ i_2\ \cdots\ i_p)$ after rotations on τ, if necessary. Now $i_j = 2$ for some $2 \leq j \leq p$, and then $\tau^{j-1} = (1\ 2\ \cdots)$ is also a p-cycle. After renaming elements, we get $\sigma = (1\ 2), \tau = (1\ 2 \cdots\ p)$ and then σ, τ generate S_p. □

Theorem 5.15.2. *Let $f \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree p, p prime. If f has precisely two complex roots and $p - 2$ real roots, then the Galois group of f is isomorphic to the symmetric group S_p.*

Proof. Fix an algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$. Let E be the splitting field of f over $\mathbb{Q}$ and α one of the roots. Note that $E/\mathbb{Q}$ is a Galois extension and $\mathrm{Gal}(E/\mathbb{Q})$ is (isomorphic to) a subgroup of S_p. Since f is irreducible, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ and so $p \mid [E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})|$. By Cauchy's theorem (or Sylow's theorem), $\mathrm{Gal}(E/\mathbb{Q})$ contains an element of order p. But the only elements in S_p of order p are p-cycles. Hence $\mathrm{Gal}(E/\mathbb{Q})$ contains a p-cycle. Note the complex conjugation exchanges the two complex roots of f and fixes reals, so it is also an element in $\mathrm{Gal}(E/\mathbb{Q})$ and is a transposition indeed. Since $\mathrm{Gal}(E/\mathbb{Q})$ contains a transposition and a p-cycle, $\mathrm{Gal}(E/qq)$ is the whole group S_p by the lemma above. □

Example 5.15.3. Probably the simplest example of a polynomial over $\mathbb{Q}$ with Galois group S_n, where n is a positive integer, is $x^n - x - 1$. This is proved in a paper by H. Osada in J. Number Theory, 25(1987), 230–238.

Example 5.15.4. Let $p \geq 5$ be a prime. Define $f(x), g(x) \in \mathbb{Q}[x]$ as

$$g(x) = (x^4 + 4)(x - 2)(x - 4) \cdots (x - 2(p - 2)),\ f(x) = g(x) - 2.$$

If we draw f, g on the plane, we see that $g(x)$ interests x-axis at $2, 4, \ldots, 2(p-2)$ and that $g(x) > 2$ for $x = 3, 5, 7, \ldots, 2p - 1$. The graph of f is obtained by shifting down 2 units of that of g. Therefore, f has precisely $p - 2$ real roots. Write $f(x)$ as

$$f(x) = x^p + d_{p-1}x^{p-1} + \cdots + d_0.$$

Then $d_0 = 4k - 2$ for some nonzero integer k and hence $2^2 \nmid d_0$ while it is easily seen that $2 \mid d_j$ for $j = 0, \ldots, d - 1$. By Eisenstein's criterion, f is irreducible. And Theorem 5.15.2 says the Galois group of f over $\mathbb{Q}$ is S_p.

Now we move the the case where we want the Galois group be finite abelian. Recall from the classification on finite abelian groups, we can write a finite abelian group G as

$$G \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_r^{e_r},$$

where p_i are primes not necessarily distinct and e_r are positive integers. And for two rings R_1 and R_2, we have

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

The following theorem is a special case of Dirichlet's theorem about primes in aritheoremetic progression. To be self-contained, we prove it using cyclotomic polynomials

Theorem 5.15.5. *Let $n > 1$ be a positive integer. Then there are infinitely many primes p such that $p \equiv 1 \pmod{n}$.*

Proof. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. We first note that $\Phi_1(0) = -1$ and $\Phi_n(0) = 1$ for $n \geq 2$. This can be easily done by induction on $n \geq 2$. Hence the constant term for $\Phi_n(x)$ is 1 when $n > 1$.

Claim: Let p be a prime. If $p \mid \Phi_n(x_0)$ for some integer x_0, then $p \mid n$ or $p \equiv 1 \pmod{n}$.

Proof of Claim: Note that $p \mid \Phi_n(x_0) \mid x_0^n - 1$. We must have $p \nmid x_0$. Let k be the order of x_0 in $(\mathbb{Z}/p)^*$. Since $|(\mathbb{Z}/p)^*| = p - 1$, we have $k \mid (p - 1)$ and so $p \equiv 1 \pmod{k}$. Since $x_0^n \equiv 1 \pmod{p}$, we have $k \mid n$. If $k = n$, then $p \equiv 1 \pmod{n}$ and we are done. If $k < n$, then $p \mid x_0^k - 1$ implies $p \mid \Phi_d(x_0)$ for some $d \leq k < n$. Since p also divides $\Phi_n(x_0)$, x_0 is a double root of $x^n - 1$ when we regard it as a polynomial in $\mathbb{F}_p[x]$. This can only happen if p divides n.

Assume that there are only finitely many primes $p \equiv 1 \pmod{n}$. We define

$$N = n \prod_{p \text{ prime},\, p \equiv 1 \pmod{n}} p.$$

Then $N > n > 1$ is well-defined. Consider the monic polynomial $\Phi_n(x)$. We have $\Phi_n(N^k) > 1$ for some large enough integer k. Let p be a prime divisor of $\Phi_n(N^k)$. Note the constant term of $\Phi_n(x)$ is 1 and then $\Phi_n(N^k) - 1$ is a multiply of N. But $p \mid \Phi_n(N^k)$ implies $p \nmid \Phi_n(N^k) - 1$ and $p \nmid N$ and $p \nmid n$. It follows from the claim that $p \equiv 1 \pmod{n}$. On the other hand $p \nmid N$ means p is not any of the primes in the definition of N. Contradiction. □

We need one lemma more before going to construct abelian extensions.

Lemma 5.15.6. *Let G be a finite abelian group. Then there is a surjective homomorphism*

$$\phi : (\mathbb{Z}/n)^* \to G$$

for some positive integer n.

Proof. By the classification of finite abelian groups, we can write

$$G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r,$$

where $\mathbb{Z}/n_i$ is a cyclic group of order n_i.

Since there are infinitely many primes $p \equiv 1 \pmod{n_i}$, we can choose distinct primes p_i such that $p_i = n_i m_i + 1$ for some positive integer m_i for $i = 1, \ldots, r$. Now $(\mathbb{Z}/p_i)^*$ is a cyclic group of order $n_i m_i$ and hence there is a surjection $\phi_i : (\mathbb{Z}/p_i)^* \to \mathbb{Z}/n_i$. Collecting all the surjections, we can define a surjective homomorphism

$$\phi : (\mathbb{Z}/p_1)^* \times \cdots \times (\mathbb{Z}/p_r)^* \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r,\ (a_1, \ldots, a_r) \mapsto (\phi_1(a_1), \ldots, \phi_r(a_r)).$$

Note that $(\mathbb{Z}/p_1)^* \times \cdots \times (\mathbb{Z}/p_r)^* = (\mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_r)^*$ and that by Chinese Remainder Theorem $\mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_r \cong \mathbb{Z}/(p_1 \ldots p_r)$. We get a surjection $\phi' : (\mathbb{Z}/(p_1 \ldots p_r))^* \to G$. □

Theorem 5.15.7. *Let G be a finite abelian group. Then there is a subfield E of $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root for some positive integer n, such that E is Galois over $\mathbb{Q}$ and Gal$(E/\mathbb{Q}) \cong G$.*

Proof. By the lemma above, we can find a positive integer n such that there is a surjection

$$\phi : (\mathbb{Z}/n)^* \to G.$$

Then the kernel $H = \ker(\phi)$ is a normal subgroup.

Now let $E = \mathbb{Q}(\zeta_n)^H$ be the fixed subfield of H. Since H is normal, by the fundamental theorem about Galois theory, $E/\mathbb{Q}$ is Galois and

$$\text{Gal}(E/\mathbb{Q}) \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\text{Gal}(\mathbb{Q}(\zeta_n)/E) \cong (\mathbb{Z}/n)^*/H \cong G.$$

□

Note the difference between this theorem and Kronecker-Weber theorem. Kronecker-Weber theorem says *every* abelian extension over the rationals can be embedded into a cyclotomic extension, while we we constructed *some* extension with Galois group a finite abelian group G that happens to embed into a cyclotomic extension.

Theorem 5.15.8 (Kronecker-Weber)**.** *Let $E/\mathbb{Q}$ be a finite Galois extension such that $Gal(E/\mathbb{Q})$ is abelian. Then there is a root of unity ζ such that $E \subset \mathbb{Q}(\zeta)$.*

And we will prove a special case of Kronecker-Weber theorem.

Theorem 5.15.9. *Let $p > 2$ be a prime. Then the only quadratic subfield over $\mathbb{Q}$ of $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p-th root, is $M = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$ and $M = \mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$.*

Note this theorem leads immediately a corollary about quadratic extensions.

Corollary 5.15.10. *Let E be a quadratic Galois extension over $\mathbb{Q}$. Then E embeds into some cyclotomic extension.*

Proof. Note that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and $i \in \mathbb{Q}(\zeta_4)$. We fix an algebraic closure $\mathbb{Q} \subset E \subset \overline{\mathbb{Q}} \subset \mathbb{C}$. A quadratic extension E over $\mathbb{Q}$ looks like $E = \mathbb{Q}(\sqrt{d})$ from some square-free integer d. We can do inductions on the prime factors of

$$d = \pm \prod_{p_i | n} p_i,$$

with the observation that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ if $m \mid n$. □

We need a technical lemma before proving Theorem 5.15.9.

Lemma 5.15.11. *Let $p > 2$ be a prime and g a generator of $\mathbb{F}_p^*$. Then the number of solutions of the equation $x^2 + gy^2 = r$ over $\mathbb{F}_p$ for some $r \in \mathbb{F}_p$ is given as*

$$|\{(x, y) \in \mathbb{F}_p^2 | x^2 + gy^2 = r\}| = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ and } r = 0, \\ p + 1 & \text{if } p \equiv 1 \pmod 4 \text{ and } r \neq 0, \\ 2p - 1 & \text{if } p \equiv 3 \pmod 4 \text{ and } r = 0, \\ p - 1 & \text{if } p \equiv 3 \pmod 4 \text{ and } r \neq 0. \end{cases}$$

Proof. Consider the case $p \equiv 1 \pmod 4$. The equation $x^2 + gy^2 = 0$ has the trivial solutions only. If not, say $y \neq 0$, then $g = -(x^2/y^2) = -(x/y)^2$ but this says $g^{(p-1)/2} = (x/y)^{p-1} = 1$ contradicting to the assumption that g is a generator of $\mathbb{F}_p^*$. Therefore, the quadratic polynomial $T^2 + g \in \mathbb{F}_p[T]$ has no solution in $\mathbb{F}_p$. Let $\alpha = \sqrt{-g}$ be one of its roots. Then $\mathbb{F}_p[\alpha]/\mathbb{F}_p$ is a Galois extension of degree 2. The norm of an element $a + b\alpha \in \mathbb{F}_p[\alpha]$ is given as $\mathrm{N}(a + b\alpha) = a^2 + b^2 g$. The norm mapping $\mathrm{N} : \mathbb{F}_p[\alpha]^\times \to \mathbb{F}_p^\times$ is a group homomorphism. The map is surjective since $\mathrm{N}(\alpha) = g$ and the kernel is of size $|\mathbb{F}_p[\alpha]^\times|/|\mathbb{F}_p^\times| = (p^2 - 1)/(p - 1) = p + 1$. Namely, for each $r \in \mathbb{F}_p^*$ we will get $p + 1$ solutions $x + y\alpha$ with $\mathrm{N}(x + y\alpha) = x^2 + y^2\alpha = r$.

The case $p \equiv 3 \pmod 4$ can be argued in a similar manner and left as an exercise. □

Proof of Theorem 5.15.9. Note that $(\mathbb{Z}/p)^* = \mathbb{F}_p^*$ is of order $p - 1 = 2m$ for some positive integer m. Let g be a generator of $\mathbb{F}_p^*$ and ζ a primitive p-th root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p)^*$ and is generated by σ who is defined by $\sigma(\zeta) = \zeta^g$. Hence $\langle \sigma^2 \rangle$ is a subgroup of index 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. The fixed subfield $E = \mathbb{Q}(\zeta)^{\langle \sigma^2 \rangle}$ is then a quadratic extension over $\mathbb{Q}$. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian and every subgroup is normal. Therefore, $E/\mathbb{Q}$ is Galois.

Note that elements

$$\alpha = \sigma^2(\zeta) + \cdots + \sigma^{p-1}(\zeta) = \zeta^{g^2} + \zeta^{g^4} + \cdots + \zeta^{g^{p-1}} = \sum_{i=1}^{\frac{p-1}{2}} \zeta^{g^{2i}} = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}}$$

$$\beta = \sigma(\alpha) = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i+1}}$$

are invariant under σ^2. Because the terms ζ^j in α, β run out all possibilities of the form ζ^j for some $0 < j < p$ as g is a generator, we see either $\alpha \notin \mathbb{Q}$ or $\beta \notin \mathbb{Q}$, otherwise, ζ would satisfy a polynomial of degree $< p-1$ in $\mathbb{Q}[x]$. Without loss of generality, we assume $E = \mathbb{Q}(\alpha)$.

We want to construct a quadratic with α, β its roots:

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

Note that

$$\alpha + \beta = \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}} + \sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i+1}} = \sum_{i=1}^{p-1} \zeta^i = (\sum_{i=0}^{p-1} \zeta^i) - 1 = \Phi_p(\zeta) - 1 = -1.$$

Hence indeed $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. And then

$$\alpha\beta = (\sum_{i=0}^{\frac{p-3}{2}} \zeta^{g^{2i}})(\sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2j+1}}) = \sum_{i=0}^{\frac{p-3}{2}} \sum_{j=0}^{\frac{p-3}{2}} \zeta^{g^{2i}+g^{2j+1}} = \sum \zeta^{x^2+gy^2},$$

where $x = g^i$ and $y = g^j$ for $i, j = 0, \ldots, (p-3)/2$ and the number of such term $\zeta^{x^2+gy^2}$ is $(p-1)^2/4$. Note that

$$(g^i)^2 = g^{2i} = g^{2i+(p-1)} = (g^{i+\frac{p-1}{2}})^2.$$

Extending the range of $x = g^i$ and $y = g^j$ to $i, j = 0, \ldots, p-2$, we get

$$4\alpha\beta = \sum_{x,y \in \mathbb{F}_p^*} \zeta^{x^2+gy^2}.$$

First consider the case $p \equiv 1 \pmod 4$. By the lemma above, we can count the number of solutions of $x^2 + gy^2 = r$. But we need to exclude the case where x or y is zero. If $r = 0$, then the quadratic form $x^2 + gy^2$ is non-isotopic, which means the only solution is $x = y = 0$.Thus if $x, y \in \mathbb{F}_p^*$, then $x^2 + gy^2$ is never 0. Then in how many ways we can get $r \neq 0$, the lemma above says there are $p + 1$. But we have to exclude the case $x = 0$ or $y = 0$. If r is a quadratic residue, then we get two solution for x if $y = 0$ and no solution for y if $x = 0$. If r is not a quadratic residue, then we get no solution for x if $y = 0$ and two solution for y if $x = 0$. Either case, we get $p - 1$ solutions for $x, y \in \mathbb{F}_p^*$. And hence

$$4\alpha\beta = (p-1)\sum_{i=1}^{p-1} \zeta^i = -(p-1).$$

And the minimal polynomial of α, β is $x^2 + x - (p-1)/4$ and then

$$\pm(\alpha - \beta) = \sqrt{\Delta} = \sqrt{1^2 - 4 \cdot (-\frac{p-1}{4})} = \sqrt{p} \in E = \mathbb{Q}(\alpha).$$

Therefore, $E = \mathbb{Q}(\sqrt{p})$.

Now consider the case $p \equiv 3 \pmod 4$. In this case, the quadratic residue is isotopic, which means we get nontrivial solution for $x^2 + gy^2 = 0$. The number of solutions is then $2p-1$ by the lemma above. But we have to exclude the trivial solution $x = y = 0$. So indeed, there are $2p - 2$ solution when $x, y \in \mathbb{F}_p^*$. Exactly the same argument as last case, we get $p - 3$ solutions for $x^2 + gy^2 = r$ for each $r \neq 0$ when $x, y \in \mathbb{F}_p^*$. Therefore, we have

$$4\alpha\beta = 2p - 2 + (p-3)\sum_{i=1}^{p-1} \zeta^i = 2p - 2 - (p-3) = p + 1.$$

And the minimal polynomial of α, β is $x^2 + x + (p+1)/4$ and then

$$\pm(\alpha - \beta) = \sqrt{\Delta} = \sqrt{1^2 - 4 \cdot (\frac{p+1}{4})} = \sqrt{-p} \in E = \mathbb{Q}(\alpha).$$

Therefore, $E = \mathbb{Q}(\sqrt{-p})$. □

Week 6

6.16 Characters

In this section, we will discuss some methods from linear algebra that are of special interest for applications in Galois theory, in particular for the study of cyclic extensions in next week.

Definition 6.16.1. Let G be a group and K a field. A K-valued character of G is a group homomorphism $\chi : G \to K^*$.

For a group G and a field K, there exists always the trivial character $G \to K^*$, mapping every element $g \in G$ to the unit element $1 \in K^*$. Furthermore, the K-valued characters of G form a group, whose law of composition is induced from the multiplication on K^*. Indeed, the product of two characters $\chi_1, \chi_2 : G \to K^*$ is given by

$$\chi_1 \cdot \chi_2 : G \to K^*, g \mapsto \chi_1(g)\chi_2(g).$$

Theorem 6.16.2 (Dedekind)**.** *Distinct characters $\chi_1, \cdots, \chi_m$ on a group G with values in a field K are K-linearly independent.*

Proof. We proceed indirectly and assume that the assertion of the proposition is false. Then there is a minimal number $n \in N$ such that there exists a linearly dependent system of K-valued characters $\chi_1, \cdots, \chi_n$ on G. Of course, we must have $n \geq 2$, since every character assumes values in K^* and therefore cannot coincide with the zero map. Now we can get a linear equation

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \tag{6.3}$$

where all a_i from K are non-zero due to the minimality of n. Let $g, h \in G$ and we evaluate Equation 6.3 at gh an get

$$a_1\chi_1(gh) + \cdots + a_n\chi_n(gh) = 0.$$

We choose g in the way such that $\chi_1(g) \neq \chi_2(g)$. By run h through all elements in G, we get a new relation

$$a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n = 0. \tag{6.4}$$

Now multiplying Equation 6.3 by $\chi_1(g)$ and subtracting Equation 6.4, we get a third relation

$$a_2(\chi_1(g) - \chi_2(g))\chi_2 + \cdots + a_n(\chi_1(g) - \chi_n(g))\chi_n = 0.$$

This is a nontrivial relation of length $n-1$, since $a_2(\chi_1(g) - \chi 2(g)) \neq 0$. However, this contradicts the minimality of n, and it follows that the assertion of the proposition is true. □

The preceding proposition can be applied in various settings. For example, if L/K is an algebraic field extension, we see that the system $\mathrm{Aut}(L/K)$ of all K-automorphisms of L is linearly independent in the L-vector space of all maps $L \to L$. Indeed, we have:

Corollary 6.16.3. *Let L/K be a finite separable field extension and $x_1, \cdots, x_n$ a basis of L as a K-vector space. Furthermore, let $\sigma_1, \cdots, \sigma_n$ denote the K-homomorphisms of L to an algebraic closure $\overline{K}$ of K. Then the vectors*

$$\begin{aligned}\xi_1 &= (\sigma_1(x_1), \cdots, \sigma_1(x_n)),\\ &\cdots,\\ \xi_n &= (\sigma_n(x_1), \cdots, \sigma_n(x_n)),\end{aligned}$$

give rise to a system that is linearly independent over $\overline{K}$. Therefore, they form an L-basis of L^n if L/K is Galois.

Proof. The linear dependence of the ξ_i would imply the linear dependence of the σ_i. However, by preceding theorem, the σ_i form a linearly independent system. □

Example 6.16.4. An $\mathbb{R}$-basis of $\mathbb{C}$ is $\{1, i\}$. The corollary says $\{(1, 1), (i, -i)\}$ is a $\mathbb{C}$-basis of $\mathbb{C}^2$.

Definition 6.16.5. Let L/K be a finite Galois extension of degree n. A *K-conjugate* of an element $\alpha \in L$ is $\sigma(\alpha)$, where σ is an element in $\mathrm{Gal}(L/K)$. A *normal basis* of L/K is a basis of L consisting of K-conjugates only, namely, $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ for some $\alpha \in L$.

Example 6.16.6. The usual basis $\{1, i\}$ is not a normal basis since the terms are not related by an element in Galois group. $\{i, -i\}$ is a set of $\mathbb{R}$-conjugate, but it is linearly dependent. The set $\{1 + i, 1 - i\}$ is a normal basis.

Example 6.16.7. Consider the field extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$. The set of four conjugates of $\sqrt{2} + \sqrt{3}$ is not a normal basis, since it is not linearly independent. If $\alpha = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$, then the four conjugates of α are

$$1 + \sqrt{2} + \sqrt{3} + \sqrt{6}, 1 - \sqrt{2} + \sqrt{3} - \sqrt{6}, 1 + \sqrt{2} - \sqrt{3} - \sqrt{6}, 1 - \sqrt{2} - \sqrt{3} + \sqrt{6}.$$

They are linearly independent by checking the determinate and spans $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore, they form a normal basis.

The normal basis theorem says that every finite Galois extension admits a normal basis. Firstly, we give a proof of this theorem when the base field is infinite.

Theorem 6.16.8 (Normal Basis Theorem)**.** *Every finite Galois extension of an infinite field admits a normal basis.*

Proof. Let L/K be a Galois extension and $[L : K] = n$ and $\mathrm{Gal}(L/K) = \{\sigma_1, \cdots, \sigma_n\}$. We aim to find an element $\alpha \in L$ such that $\sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ are linearly independent. If we have a linear dependence relation for some $\alpha \in L$:

$$\sum_{j=1}^{n} a_j \sigma_j(\alpha) = 0,$$

for some $a_1, \cdots, a_j \in K$, then we can get a new one by applying σ_i^{-1}:

$$\sum_{j=1}^{n} a_j (\sigma_i^{-1}\sigma_j)(\alpha) = 0.$$

Collecting these together for $i = 1, \cdots, n$, we get

$$\begin{pmatrix} \sigma_1^{-1}\sigma_1(\alpha) & \cdots & \sigma_1^{-1}\sigma_n(\alpha) \\ \vdots & \ddots & \vdots \\ \sigma_n^{-1}\sigma_1(\alpha) & \cdots & \sigma_n^{-1}\sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

To force a trivial solution for $a_1, \cdot, a_n$, we must have $\det((\sigma_i^{-1}\sigma_j)(\alpha)) \neq 0$. Let $\{e_1, \cdots, e_n\}$ be a K-basis of L. Then an arbitrary element $\alpha \in L$ is of the form $\sum_{k=1}^n b_k e_k$ with $b_k \in K$. And then we have

$$(\sigma_i^{-1}\sigma_j)(\alpha) = \sum_{k=1}^n b_k((\sigma_i^{-1}\sigma_j)(e_k)).$$

Consider the polynomial

$$\Delta(X_1, \cdots, X_n) = \det(\sum_{k=1}^n X_k((\sigma_i^{-1}\sigma_j)(e_k))) \in L[X_1, \cdots, X_n].$$

Let σ_1 be the identity automorphism. Corollary 6.16.3 says there are $c_1, \cdots, c_n \in L$ such that

$$\sum_{k=1}^n c_k(\sigma_1(e_k), \cdots, \sigma_n(e_k)) = (1, 0, \cdots, 0).$$

Reading this off component-wise,

$$\sum_{k=1}^n c_k e_k = 1, \quad \sum_{k=1}^n c_k \sigma(e_k) = 0 \text{ for } \sigma \neq id.$$

Thus

$$\sum_{k=1}^n c_k(\sigma_i^{-1}\sigma_j)(e_k) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore the matrix $(\sum_{k=1}^n c_k(\sigma_i^{-1}\sigma_j)(e_k))$ is the identity matrix and so $\Delta(c_1, \cdots, c_n) = 1$, which means $\Delta(X_1, \cdots, X_n)$ is not the zero polynomial.

Since K is infinite, there must be $b_1, \cdots, b_n \in K$ such that $\Delta(b_1, \cdots, b_n) \neq 0$. Then $\alpha = \sum_{k=1}^n b_k e_k$ is the desired element. □

Before proving the normal basis theorem for finite fields, let us recap a few facts which we did not quite make explicitly before.

Suppose E/F is a finite Galois extension. Then $\sigma \in \mathrm{Gal}(E/F)$ is also a F-linear transformation from E to E. There are different angles of views. One can say there is a canonical embedding $\mathrm{Gal}(E/F) \to \mathrm{GL}(E)$ or one can say E has a $F[x]$-module structure induced by $\sigma \in \mathrm{Gal}(E/F)$. Either case, it makes sense to talk about the characteristic/minimal polynomial of σ (and then also $\phi_a : E \to E, x \to ax$ as in the definition 6.17.1 of the norm and trace).

Finite extensions over finite fields are cyclic. In particular, the Galois group is generated by the Frobenius map. Suppose $E/\mathbb{F}_q$, where $q = p^r$ for some prime p and r a positive integer, is such an extension. Then the Frobenius map $\varphi : E \to E, x \mapsto x^q$ is clearly a ring homomorphism. $\varphi|_{\mathbb{F}_q} = id|_{\mathbb{F}_q}$ and $\varphi^{[E:\mathbb{F}_q]} = id|_E$.

Theorem 6.16.9 (Normal Basis Theorem)**.** *Every finite Galois extension of a finite field admits a normal basis.*

Indeed, the proof works for the Galois extensions whose Galois group is cyclic.

Proof. Please refer to Conrad's notes. □

6.17 Norm and Trace

Definition 6.17.1. Let L/K be a finite field extension. For an element $a \in L$, consider the multiplication map $\phi_a : L \to L, x \mapsto ax$, as a linear transformation of L as a K-vector space. Then

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(\phi_a), \quad \mathrm{N}_{L/K}(a) = \det(\phi_a)$$

are called the *trace* and the *norm* of a with respect to the extension L/K.

In particular, $\mathrm{Tr}_{L/K} : L \to K$ is a homomorphism of K-vector spaces, or in more precise terms, a linear functional on L viewed as a K-vector space. Likewise, $\mathrm{N}_{L/K} : L^* \to K^*$ is a group homomorphism.

Example 6.17.2. If $z = x + yi$ is the decomposition of a complex number z into its real and imaginary parts, then the multiplication by z on $\mathbb{C}$ is described relative to the $\mathbb{R}$-basis $1, i$ by the matrix

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

And then $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2\Re(z)$ and $\mathrm{N}_{\mathbb{C}/\mathbb{R}} = z\overline{z}$.

Example 6.17.3. Consider a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. For $\alpha = a + b\sqrt{d}$, the action ϕ_α on a $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$ of $\mathbb{Q}(\sqrt{d})$ is given by

$$\phi_\alpha(1) = a + b\sqrt{d}, \quad \phi_\alpha(\sqrt{d}) = db + a\sqrt{d}.$$

The matrix represetation of ϕ_α is then

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix},$$

and then $\mathrm{Tr}(\alpha) = 2a, \mathrm{N}(\alpha) = a^2 - db^2$.

Example 6.17.4. To see $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, we pass the norm on $\mathbb{Q}(\sqrt{-5})$ to $\mathbb{Z}[\sqrt{-5}]$. A unit must be of norm 1. Note that

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

We have $\mathrm{N}(2) = 4, \mathrm{N}(3) = 9$ and $\mathrm{N}(1 + \sqrt{-5}) = 6 = \mathrm{N}(1 - \sqrt{5})$, and so 2 and $\sqrt{1 \pm \sqrt{5}}$ are not associated. We have two distinct factorizations of 6.

Example 6.17.5. Here we use trace and norm to show $1 + \sqrt[3]{2}$ is not a perfect square in $F = \mathbb{Q}(\sqrt[3]{2})$. Let $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ be the $\mathbb{Q}$-basis of F. Then the action $\phi_{1+\sqrt[3]{2}}$ has the matrix representation

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Hence $\mathrm{N}_{F/\mathbb{Q}}(1 + \sqrt[3]{2}) = 3$. If $1 + \sqrt[3]{2}$ is a perfect square, then so is its norm. But 3 is not a square of any rational number.

Lemma 6.17.6. *Let L/K be a finite field extension of degree $n = [L : K]$, and consider an element $a \in L$.*

1. *If $a \in K$, then*
$$Tr_{L/K}(a) = na, \quad N_{L/K}(a) = a^n.$$
2. *If $L = K(a)$ and $X^n + c_{n-1}X^{n-1} + \cdots + c_0$ is the minimal polynomial of a over K, then*
$$Tr_{L/K} = -c_{n-1}, \quad N_{L/K}(a) = (-1)^n c_0.$$

Proof. For $a \in K$, the linear map $\phi_a : L \to L$ is described by a times the unit matrix of $K_{n\times n}$. This justifies the formulas in (i).

Furthermore, if $L = K(a)$, the minimal polynomial of a coincides with the minimal polynomial of the endomorphism ϕ_a, and hence by reasons of degree, must coincide with the characteristic polynomial of ϕ_a. Therefore, the formulas in (ii) follow from the description of $\mathrm{Tr}(\phi_a)$ and $\det(\phi_a)$ in terms of the coefficients of the characteristic polynomial of ϕ_a. □

Now we can extend the lemma above to compute the norm and the trace of elements when one is dealing with arbitrary field extensions.

Lemma 6.17.7. *Consider an element $a \in L$ of a finite field extension L/K, and let $s = [L : K(a)]$. Then*
$$Tr_{L/K}(a) = sTr_{K(a)/K}(a), \quad N_{L/K}(a) = (N_{K(a)/K}(a))^s.$$

Proof. Choose a K-basis $x_1, \cdots, x_r$ of $K(a)$, as well as a $K(a)$-basis $y_1, \cdots, y_s$ of L. Then the products $x_i y_j$ form a K-basis of L. Let $A \in K_{r\times r}$ be the matrix describing the multiplication by a on $K(a)$ relative to the basis $x_1, \cdots, x_r$. It follows that, relative to the basis consisting of the $x_i y_j$, the multiplication by a on L is given by the matrix
$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}.$$
□

Theorem 6.17.8. *Let L/K be a finite field extension of degree $[L : K] = n = qr$, where $r = [L : K]_s$ is the separable degree of L/K. If $\sigma_1, \cdots, \sigma_r$ are the K-homomorphisms of L into an algebraic closure $\overline{K}$ of K, the following formulas hold for elements $a \in L$:*
$$Tr_{L/K}(a) = q\sum_{i=1}^{r} \sigma_i(a), \quad N_{L/K}(a) = (\prod_{i=1}^{r} \sigma_i(a))^q.$$
In particular, if L/K is not separable, then $Tr_{L/K}$ is the zero map.

Proof. Let
$$g(x) = (\prod_{j=1}^{r}(x - \sigma_j(a)))^q \in \overline{K}[x].$$
The degree of g is exactly $qr = [L : K]$.

Claim: $g(x)$ is in $K[x]$ and has precisely the same root as the minimal polynomial $p(x) = \mathrm{irr}(a, K)$ of a over K.

Let's postpone the proof of claim. It follows that p divides g immediately since all roots of g are roots of p. And then the only irreducible factor of g is p and so $g(x) = p(x)^{n/m}$, where m is the degree

of p. The characteristic polynomial $\chi(x)$ of ϕ_a is also divisible by the minimal polynomial of ϕ_a, which is $p(x)$. By arguing over the degrees of polynomials, we have $\chi(x) = g(x)$. Multiplying $g(x)$ out and looking at the constant term and the coefficient of x^{n-1}, we have

$$\mathrm{Tr}_{L/K}(a) = q\sum_{i=1}^{r}\sigma_i(a), \quad \mathrm{N}_{L/K}(a) = (\prod_{i=1}^{r}\sigma_i(a))^q.$$

Now it remains to prove the claim.

Proof of Claim. To see that g, p have the same roots, we note that each $\sigma_j(a)$ is a root of p since σ_j fixed K. If $a' \in \overline{K}$ is a root of $p(x)$, then by the extension theorem, we have a K-map $\tau : \overline{K} \to \overline{K}$ with $\tau(a) = a'$. Since $\tau|_K$ is one of σ_j, say $\tau|_K = \sigma_i$, then $a' = \tau(a) = \sigma_i(a)$. So a' is also a root of g. This proves g, p have the same roots.

To see that $g(x)$ is in $K[x]$, we aim to show that $g = p^{n/m}$. We have $[L : K(a)]_s[K(a) : K]_s = [L : K]_s$ by Theorem 3.8.3. In lieu of the proof of Theorem 3.8.3, we have

$$\mathrm{Hom}_K(L, \overline{K}) \cong \mathrm{Hom}_{K(a)}(L, \overline{K}) \times \mathrm{Hom}_K(K(a), \overline{K}).$$

In other words, an element σ in $\mathrm{Hom}_K(L, \overline{K})$ can be unqiuely written as $\sigma = \overline{\rho} \circ \tau$, where $\tau \in \mathrm{Hom}_K(K(a), \overline{K})$ and $\rho \in \mathrm{Hom}_{K(a)}(L, \overline{K})$ and $\sigma|_{K(a)} = \tau$. Write $\mathrm{Hom}_K(K(a), \overline{K}) = \{\tau_1, \cdots, \tau_s\}$ and then we have

$$p(x) = (\prod_{i=1}^{s}(x - \tau_s(a)))^{m/s},$$
$$g(x) = (\prod_{j=1}^{r}(x - \sigma_j(a)))^q = ((\prod_{i=1}^{s}(x - \tau_i(a)))^{r/s})^q = p(x)^{n/m},$$

by counting the multiplicity. Then g is in $K[x]$ as well. □

For the "in particular" part, if a is inseparable, then the characteristic of K must be a prime l. And then the trace of a is the coefficient of x^{n-1} term in $g(x) = p(x)^{n/m}$, which is a multiply of l and hence is 0. In particular, $\mathrm{Tr}_{L/K}(a) = [L : K]a = 0$ for $a \in K$ since $[L : k] = l^u v$ is zero in a characteristic l field. □

Theorem 6.17.9. *Let M/L and L/K be finite field extensions. Then*

$$Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}, \quad N_{M/K} = N_{L/K} \circ N_{M/L}.$$

Proof. Note that

$$[L : K] = q_1[L : K]_s, \quad [M : L] = q_2[M : L]_s, \quad [M : K] = q_1q_2[M : K]_s.$$

Write

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i : i \in I\}, \quad \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j : j \in J\},$$

then

$$\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma_i} \circ \tau_j; i \in I, j \in J\}.$$

And then a straightforward calculation by the formula above shows

$$\begin{aligned}\mathrm{Tr}_{M/K}(a) &= q_1 q_2 \sum_{i,j} \overline{\sigma_i} \circ \tau_j(a) \\ &= q_1 \sum_i \overline{\sigma_i}(q_2 \sum_j \tau_j(a)) \\ &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(a)),\end{aligned}$$

as well as a similar chain equalities of norm. □

Corollary 6.17.10. *If K/F is Galois with Galois group G, then for all $a \in K$ we have*

$$Tr_{K/F}(a) = \sum_{\sigma \in G} \sigma(a), \quad N_{K/F} = \prod_{\sigma \in G} \sigma(a).$$

Theorem 6.17.11. *A finite extension L/K is separable if and only if the K-linear map $Tr_{L/K} : L \to K$ is nontrivial and hence surjective. If L/K is separable, the symmetric bilinear map*

$$Tr : L \times L \to K, \quad (x, y) \mapsto Tr_{L/K}(xy)$$

is nondegenerate. In other words, Tr induces an isomorphism

$$L \to \hat{L}, \quad x \mapsto Tr(x, \cdot)$$

of L into its dual $\hat{L}$.

Proof. The "in particular" part of Theorem 6.17.8 says one direction. For the other direction, assume L/K is separable. If $\sigma_1, \cdots, \sigma_r$ are all the K-map $L \to \overline{K}$, where $\overline{K}$ is an algebraic closure of K (and L), then we have

$$\mathrm{Tr}_{L/K} = \sigma_1 + \cdots + \sigma_r.$$

Dedekind's Theorem says characters are linearly independent hence the sum is not the zero map.

Now consider an element x of the kernel of $L \to \hat{L}$. Then we get $\mathrm{Tr}_{L/K}(xL) = 0$ which says $x = 0$. Otherwise, $xL = L$ and then $\mathrm{Tr}_{L/K}$ vanished on L. Contradiction. And an injection homomorphism between finite dimensional vector spaces is necessarily an isomorphism. □

Week 7

7.18 Cyclic Extensions

Definition 7.18.1. A Galois extension L/K is said to be *cyclic* (resp. *abelian*) if the Galois group is *cyclic* (resp. *abelian*).

Example 7.18.2. Quadratic extensions are cyclic.

Example 7.18.3. Let ζ_n be a primitive n-th root. Then the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is abelian. Moreover, when $n = 1, 2, 4, p^k, 2p^k$, where p is an odd prime, $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic and in this case $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a cyclic extension.

Example 7.18.4. Let ω be a primitive 5-th root of unity (in $\mathbb{C}$) and let $F = \mathbb{Q}(\omega)$ and $K = F(\sqrt[5]{2})$. Then K is the splitting field of $x^5 - 2$ over F, so K/F is Galois. Also, $[F : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$. The degree of $[K : \mathbb{Q}]$ is divisible by 4 and 5, hence by 20. On the other side, $[K : F] \leq 5$, so $[K : \mathbb{Q}] \leq 20$. Therefore, $[K : \mathbb{Q}] = 20$ and $[K : F] = 5$. The roots of $x^5 - 2$ are precisely $\sqrt[5]{2}, \omega\sqrt[5]{2}, \omega^2\sqrt[5]{2}, \omega^3\sqrt[5]{2}$ and $\omega^4\sqrt[5]{2}$. By isomorphism extension theorem, there is a $\sigma \in \text{Gal}(K/F)$ with $\sigma(\sqrt[5]{2}) = \omega\sqrt[5]{2}$. Then $\sigma^5 = id$ and $\text{Gal}(K/F) = \langle\sigma\rangle$.

There is no simple description of the cyclic extension of degree n of a field F that does not contain a primitive n-th root of unity, unless $n = p = \text{char}(F)$. Let us discuss the case when F does contain a primitive n-th root of unity first.

The following lemma will be used in Theorem 7.18.6. The standard way to prove it is to use Hilbert Theorem 90. We will discuss Hilbert 90 in details later and use a linear algebra argument here.

Lemma 7.18.5. *Let F be a field containing a primitive n-th root ω, let K/F be a cyclic extension of degree n, and let σ be a generator of Gal(K/F). Then there is an $a \in K$ with $\omega = \sigma(a)/a$.*

Proof. The automorphism σ is also a F-linear transformation of K. We wish to find an $a \in K$ with $\sigma(a) = \omega a$, that is, we want to show that ω is an eigenvalue of σ. To do this, we show that ω is a root of the characteristic polynomial of σ. Now since ω has order n, we have $\sigma^n = id$. Therefore, σ satisfies the polynomial $x^n - 1$. Moreover, if there is a polynomial $g(x) \in F[x]$ of degree $m < n$ satisfied by σ, then the automorphisms $id, \sigma, \cdots, \sigma^m$ are linearly dependent over F, a contradiction to the Dedekind independence lemma. Thus, $x^n - 1$ is the minimal polynomial of σ over F. However, the characteristic polynomial of σ has degree $n = [K : F]$ and is divisible by $x^n - 1$, so indeed $x^n - 1$ is the characteristic polynomial of σ. Since ω is a root of this polynomial, it is an eigenvalue for σ. Thus, there is an $a \in K$ such that $\sigma(a) = \omega a$. □

Theorem 7.18.6. *Let F be a field of characteristic not dividing n, containing a primitive n-th root of unity, and let K/F by a cyclic Galois extension of degree n. Then there is an $a \in K$ such that $K = F(a)$ and $a^n = b \in F$, that is, $K = F(\sqrt[n]{b})$.*

Proof. By the lemma above, there is an a with $\sigma(a) = \omega a$. Therefore, $\sigma^i(a) = \omega^i a$, so a is fixed by σ^i only when $n \mid i$. Since the order of σ is n, we see that a is fixed by id only, in other words, $\text{Gal}(K/F(a)) = \{id\}$. Thus $K = F(a)$ by the fundamental theorem. Further more, we see that $\sigma(a^n) = (\omega a)^n = a^n$, so a^n is fixed by σ and hence by $\text{Gal}(K/F)$. We have some $b = a^n \in F$ and $K = F(\sqrt[n]{b})$. □

We also have a converse of this theorem.

Theorem 7.18.7. *Let F be a field of characteristic not dividing n, containing a primitive n-th root of unity, and let E/F be an extension of the form $E = F(\sqrt[n]{a})$, where $a \in F$. Then if r is the order of a in the group $(F^*)/(F^*)^n$, then we have E/F is Galois and Gal$(E/F) \cong \mathbb{Z}/r\mathbb{Z}$.*

Proof. If a has order r in $(F^*)/(F^*)^n$, then $a^r = b^n$ for some $b \in F^*$, and there is no smaller $r > 0$ for which this is true. First, note that $E = F(\sqrt[n]{a}) = F(\sqrt[r]{b})$. Also note that $r \mid n$ and that $(\sqrt[n]{a})^k = (\sqrt[r]{b})^k \notin F$ for $0 < k < r$ (or this will contradict the minimality of r).

Claim: $f(x) = x^r - b$ is irreducible over F.

Proof of Claim: If not, assume $f = gh$ and g is an irreducible factor of degree ≥ 2. Note that

$$f(x) = \prod_{i=0}^{r-1}(x - \zeta_r^i \sqrt[r]{b}),$$

where ζ_r is a primitive r-th root. Then we can find a subset $I \subset \{0, 1, \cdots, r-1\}$ such that

$$g(x) = \prod_{i \in I}(x - \zeta_r^i \sqrt[r]{b}).$$

The constant term of g is $\pm \prod_{i \in I}(\sigma_r^i \sqrt[r]{b}) = \pm \zeta'(\sqrt[r]{b})^{|I|}$, where ζ' is a r-th root of unity. Then we get $(\sqrt[r]{b})^{|I|} \in F$, which reaches a contradiction unless $|I| = 0$ or r.

Now since $\text{char}(F) \nmid n$, we also have $\text{char}(F) \nmid r$ and so E/F is separable. On the other hand, E/F is the splitting field of $x^r - b$, since all the roots of it are just $\zeta_r^i \sqrt[r]{b}$ for $i = 0, 1, \cdots, r-1$. Finally, note that any $\sigma \in \text{Gal}(E/F)$ is entirely determined by its action on $\sqrt[r]{b}$, where $\sigma(\sqrt[r]{b}) = \zeta_r^i \sqrt[r]{b}$ for some $i \in \mathbb{Z}/r\mathbb{Z}$. But $|\text{Gal}(E/F)| = r$, we indeed have a bijection between $\mathbb{Z}/r\mathbb{Z}$ and $\text{Gal}(E/F)$. It remains to check that it is indeed a group isomorphism, but that is straightforward. □

Now let's go to the case where $[E : F] = \text{char}(F) = p$. Define $\wp : F \to F, a \mapsto a^p - a$. When F is treated as an additive abelian group, $\wp$ is a group homomorphism with kernel $\mathbb{F}_p$, as we have

$$\wp(a + b) = (a + b)^p - (a + b) = (a^p - a) + (b^p - b) = \wp(a) + \wp(b).$$

So if $\wp(a) = b$, then $\wp^{-1}(b) = \{a + i : i \in \mathbb{F}_p\}$. Therefore, if K is an extension of F such that there is an $a \in K$ with $\wp(a) = b \in F$, then $F(a) = F(\wp^{-1}(b))$.

Again, the usual proof of the following lemma uses Hilbert 90, but as with Lemma 7.18.5, we give a linear algebraic proof.

Theorem 7.18.8. *Let char$(F) = p$, and let K/F be a cyclic Galois extension of degree p. Then $K = F(\alpha)$ with $\alpha^p - \alpha - a = 0$ for some $a \in F$, namely, $K = F(\wp^{-1}(a))$.*

Proof. Let σ be a generator of $\text{Gal}(K/F)$, and let T be the linear transformation $T = \sigma - id$. Note that the kernel of T is

$$\ker(T) = \{b \in K : \sigma(b) = b\} = F.$$

Also we have $T^p = (\sigma - id)^p = \sigma^p - id = 0$, since the order of σ is p and $\text{char}(F) = p$. Thus $\text{im}(T^{p-1}) \subset \ker(T) = F$. We also have $\text{im}(T^{p-1})$ is nontrivial, otherwise, $\{id, \sigma, \cdots, \sigma^{p-1}\}$ is linear dependent and that contradicts the Dedekind independence lemma. So $\text{im}(T^{p-1}) = F$ and we can find $c \in K$ such that $T^{p-1}(c) = 1$. Let $\alpha = T^{p-2}(c)$. Then $T(\alpha) = 1$ and so $\sigma(\alpha) = \alpha + 1$. Since α is not fixed by σ, we see that $\alpha \notin F$ and $F(\alpha) = K$. Moreover,

$$\begin{aligned}\sigma(\alpha^p - \alpha) &= \sigma(\alpha)^p - \sigma(\alpha) \\ &= (\alpha + 1)^p - (\alpha + 1) \\ &= \alpha^p - \alpha.\end{aligned}$$

So $\alpha^p - \alpha$ is fixed by σ and hence $\alpha^p - \alpha = a \in F$, in other words, $\alpha^p - \alpha - a = 0$. □

The converse of this theorem is also true.

Theorem 7.18.9. *Let F be a field of characteristic p, and let $a \in F \setminus \wp^{-1}(F)$. Then $f(x) = x^p - x - a$ is irreducibility over F and the splitting field of f is a cyclic Galois extension of degree p.*

Proof. Let K be the splitting field of f over F. If α is a root of f, then it is easy to check that $\alpha + 1$ is also a root. Hence, the p roots of f are $\alpha, \alpha+1, \cdots, \alpha+p-1$ and α is separable. Therefore, $K = F(\alpha)$. The assumption on a assures $\alpha \notin F$.

Claim: $f(x)$ is irreducible.

Under the claim, $[K : F] = p$ and there is a $\sigma \in \text{Gal}(K/F)$ with $\sigma(\alpha) = \alpha + 1$. The order of σ is p and so $\text{Gal}(K/F) = \langle\sigma\rangle$. The statement of this theorem follows.

Proof of Claim: Assume not. Then $f = gh$ in $F[x]$ where g is an irreducible factor with degree ≥ 2. Since $f(x) = \prod_{i=0}^{p-1}(x - (\alpha + i))$, we can find a subset $I \subset \{0, 1, \cdots, p-1\}$ such that

$$g(x) = \prod_{i \in I}(x - (\alpha + i)).$$

The coefficient of the second highest term of g is then $-|I|\alpha - \sum_{i \in I} i$. But this implies $\alpha \in F$, which is a contradiction, unless $|I| = 0$ or p. □

Example 7.18.10. Let $F = \mathbb{F}_p(t)$ the rational function field in one variable over $\mathbb{F}_p$. We claim that $t \notin \wp^{-1}(F)$, so the extension $F(\wp^{-1}(t))$ is a cyclic extension of F of degree p.

To prove the claim, suppose instead $t \in \wp^{-1}(F)$, so $t = a^p - a$ for some $a \in F$, say, $a = f/g$ with $f, g \in \mathbb{F}_p[t]$ coprime. Then $t = f^p/g^p - f/g$ or $g^p x = f^p - fg^{p-1}$ or $f^p = g^{p-1}(gt - f)$, so g divides f^p. This is impossible.

Combining Theorem 7.18.8 and Theorem 7.18.9, we get the Artin-Schreier Theorem.

Theorem 7.18.11 (Artin-Schreier)**.** *Let E/F be a finite extension with $\text{char}(F) = p > 0$. Then E/F is a cyclic extension of degree p if and only if there is some $a \in F$ not of the form $b^p - b$ for any $b \in F$, namely, $a \in F \setminus \wp^{-1}(F)$, such that E/F is the splitting field of $f(x) = x^p - x - a$.*

Recall that for algebraic closures, we have $[\mathbb{C} : \mathbb{R}] = 2, [\overline{\mathbb{Q}} : \mathbb{Q}] = \infty, [\overline{\mathbb{F}_p} : \mathbb{F}_p] = \infty$. We use Artin-Schreier Theorem to prove the following theorem.

Theorem 7.18.12. *Suppose that E/F is a finite field extension and $F \subsetneq E$ is algebraically closed. Then $\text{char}(F) = 0$ and $E = F(\sqrt{-1})$ and so $[E : F] = 2$.*

Proof. See supplement notes from Conrad. □

7.19 Hilbert Theorem 90 and Noether's Lemma

The statement about Hilbert 90 and Noether's lemma is about the cohomology of the Galois group. We have a brief discussion about the group cohomology here.

Let G be a group and M an abelian group. We say M is a G-module if there is a function $G \times M \to M$, where the image of (σ, m) is written as σm, such that

$$\begin{aligned} 1m &= m, \\ \sigma(\tau m) &= (\sigma\tau)m, \\ \sigma(m+n) &= \sigma m + \sigma n, \end{aligned}$$

for all $\sigma, \tau \in G$ and $m, n \in M$. It is equivalent to say that M is a left module over the group ring $\mathbb{Z}[G]$. For example, if K is a Galois extension of a field F and $G = \mathrm{Gal}(K/F)$, then K^* is G-module by defining $\sigma a = \sigma(a)$. Similarly, the additive group $(K, +)$ is a G-module.

Suppose that M is a Let $C^n(G, M)$ be the set of all functions from the Cartesian product $G \times G \times \cdots \times G$ (n copies) to M. The elements of $C^n(G, M)$ are called *n-cochains*. If $n = 0$, we define $C^0(G, M) = M$. The set $C^n(G, M)$ can be made into a group by adding functions component-wise. Namely, define $f + g$ by

$$(f+g)(\sigma_1, \cdots, \sigma_n) = f(\sigma_1, \cdots, \sigma_n) + g(\sigma_1, \cdots, \sigma_n).$$

Define a map $\delta_n : C^n(G, M) \to C^{n+1}(G, M)$ by

$$\begin{aligned} \delta_n(f)(\sigma_1, \cdots, \sigma_{n+1}) = {} & \sigma_1 f(\sigma_2, \cdots, \sigma_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \cdots, \sigma_i\sigma_{i+1}, \cdots, \sigma_{n+1}) \\ & + (-1)^{n+1} f(\sigma_1, \cdots, \sigma_n). \end{aligned}$$

If $n = 0$, then the map $\delta_0 : M = C^0(G, M) \to C^1(G, M)$ is defined by $\delta_0(m)(\sigma) = \sigma m - m$. The definition is compatible with the general formal above. A straightforward but tedious calculation shows that δ_n is a homomorphism and that $\delta_{n+1} \circ \delta_n$ is the zero map. The maps δ_n are called boundary maps.

Let $Z^n(G, M) = \ker(\delta_n)$. The elements of $Z^n(G, M)$ are called *n-cocycles*. Let $B^n(G, M) = \mathrm{im}(\delta_{n-1})$ if $n > 1$, and $B^0(G, M) = 0$. The elements of $B^n(G, M)$ are called *n-cobundaries*. Since $\delta_n \circ \delta_{n-1} = 0$, $B^n(G, M)$ is a subgroup of $C^n(G, M)$. Finally, the n-th *cohomology group* $H^n(G, M)$ is defined to be

$$H^n(G, M) = Z^n(G, M)/B^n(G, M).$$

Two cocycles in $Z^n(G, M)$ are said to be *cohomologous* if they represent the same element in $H^n(G, M)$.

Let's look at the cohomology group of small n. The kernel of δ_0 consists of all elements $m \in M$ such that $\sigma m = m$ for all $\sigma \in G$. Therefore,

$$H^0(G, M) = M^G = \{m \in M : \sigma m = m \text{ for all } \sigma \in G\}.$$

If $n = 1$, then $f : G \to M$ is 1-cocycle if $\delta_1(f) = 0$, namely

$$\sigma f(\tau) - f(\sigma\tau) + f(\sigma) = 0,$$

for all $\sigma, \tau \in G$. If g is a 1-coboundary, then $g \in \mathrm{im}(\delta_0)$, namely, we can find an element $m \in M$ such that

$$g(\sigma) = \sigma m - m.$$

If the group M is written multiplicatively, for example $M = F^\times$, then the above is translated into

$$f(\sigma\tau) = f(\sigma)\tau f(\sigma), \quad g(\sigma) = \frac{\sigma m}{m}.$$

The following theorem is in fact a lemma of Noether's work.

Theorem 7.19.1 (Noether's Lemma)**.** *Let E/F be a finite Galois extension and $G = Gal(E/F)$. Then both $H^1(G, E)$ and $H^1(G, E^\times)$ are trivial.*

We divide the proof into multiplicative case and additive case.

Definition 7.19.2. Let E/F be a finite Galois extension and $G = \text{Gal}(E/F)$. Let

$$f : G \to E^\times$$

be a function. Then f is a *multiplicative cocycle* if

$$f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$$

for all $\tau, \sigma \in G$. f is a *multiplicative coboundary* if and only if there is a $\beta \in E^\times$ such that

$$f(\sigma) = \frac{\sigma(\beta)}{\beta}$$

for all $\sigma \in G$.

Let

$$g : G \to E$$

be another function. Then g is a *additive cocycle* if

$$g(\sigma\tau) = g(\sigma) + \sigma(g(\tau))$$

for all $\tau, \sigma \in G$. g is a *additive coboundary* if and only if there is a $\alpha \in E^\times$ such that

$$g(\sigma) = \sigma(\alpha) - \alpha$$

for all $\sigma \in G$.

Proposition 7.19.3. *Let E/F be a finite Galois extension with Gal$(E/F) = G$. Then $f : G \to E^\times$ is a (multiplicative) cocycle if and ony if it is a (multiplicative) coboundary.*

Proof. One direction is easy. Assume f is a coboundary corresponding to $\alpha \in E^\times$, then

$$f(\sigma)\sigma(f(\tau)) = \frac{\sigma(\alpha)}{\alpha}\sigma(\frac{\tau(\alpha)}{\alpha}) = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma \circ \tau(\alpha)}{\sigma(\alpha)} = f(\sigma\tau).$$

In the other direction, suppose f is a cocycle. Define a function

$$S : E \to E, x \mapsto \sum_{\sigma \in G} f(\sigma)\sigma(x).$$

Dedekind independence lemma says S is not identically 0. Choose $\alpha \in E^\times$ with $\alpha = S(x) \neq 0$ for some $x \in E$. Then we have

$$\sigma(\alpha) = \sigma(\sum_{\tau \in G} f(\tau)\tau(x)) = \sum_{\tau \in G} \sigma(f(\tau))\sigma \circ \tau(x).$$

By the cocycle condition, we can turn this into

$$\begin{aligned}\sigma(\alpha) &= \frac{1}{f(\sigma)}\sum_{\tau\in G} f(\sigma)\sigma(f(\tau))\sigma\circ\tau(x)\\ &= \frac{1}{f(\sigma)}\sum_{\tau\in G} f(\sigma\tau)\sigma\circ\tau(x)\\ &= \frac{\alpha}{f(\sigma)},\end{aligned}$$

namely, we have $f(\sigma) = \alpha/\sigma(\alpha)$ for any $\sigma \in G$. And we may take $\beta = \alpha^{-1}$. □

Proposition 7.19.4. *Let E/F be a finite Galois extension with Gal$(E/F) = G$. Then $g : G \to E$ is a (additive) cocycle if and ony if it is a (additive) coboundary.*

Proof. The proof is exactly an analogy of the above one.

One direction is straightforward. Assume g is a coboundary corresponding to $\beta \in E$. Then

$$g(\sigma\tau) = \sigma\tau(\beta) - \beta = (\sigma(\tau(\beta)) - \sigma(\beta)) + (\sigma(\beta) - \beta) = \sigma(g(\tau)) + f(\sigma).$$

We now prove the other direction. Since E/F is separable, $\mathrm{Tr}_{E/F}$ is not the zero map. Then we can find an element $c \in E$ such that $\mathrm{Tr}_{E/F}(c) = 1$ by rescaling if necessary as $\mathrm{Tr}_{E/F}$ is F-linear. Recall that $\mathrm{Tr}_{E/F}(x) = \sum_{\sigma\in G}\sigma(x)$ for all $x \in E$. Write $\beta = \sum_{\sigma\in G} g(\sigma)\sigma(c)$. Then we have

$$\tau(\beta) = \sum_{\sigma\in G}\tau(g(\sigma))(\tau\sigma)(c).$$

By the cocycle condition, we can turn this into

$$\begin{aligned}\tau(\beta) &= \sum_{\sigma\in G}\tau(g(\sigma))(\tau\sigma)(c)\\ &= \sum_{\sigma\in G}(g(\tau\sigma) - g(\tau))(\tau\sigma)(c)\\ &= \sum_{\sigma\in G} g(\tau\sigma)(\tau\sigma)(c) - \sum_{\sigma\in G} g(\tau)(\tau\sigma)(c)\\ &= \beta - g(\tau)\sum_{\sigma\in G}(\tau\sigma)(c)\\ &= \beta - g(\tau),\end{aligned}$$

namely, $g(\tau) = \beta - \tau(\beta)$. And we may take $\alpha = -\beta$. □

Now we shall move to Hilbert 90, which in fact is equivalent to Noether's lemma.

Theorem 7.19.5 (Hilbert 90, Multiplicative Form)**.** *Let K/F be a cyclic Galois extension of degree n with σ a generator of Gal(K/F). If $u \in K$, then $N_{K/F}(u) = 1$ if and only if $u = \sigma(a)/a$ for some $a \in K$.*

Proof. One direction is easy. If $u = \sigma(a)/a$, then $\mathrm{N}_{K/F}(\sigma(a)) = \mathrm{N}_{K/F}(a)$, so $\mathrm{N}_{K/F}(u) = 1$.

Conversely, if $\mathrm{N}_{K/F}(u) = 1$, we define $f : G \to K^*$ by $f(id) = 1, f(\sigma) = u$ and $f(\sigma^i) = u\sigma(u)\cdots\sigma^{i-1}(u)$ for $1 \leq i \leq n$. We want to show f is a (multiplicative) cocycle. If $i + j < n$, then

$$\begin{aligned} f(\sigma^i\sigma^j) = f(\sigma^{i+j}) &= u\sigma(u)\cdots\sigma^{i+k-1}(u) \\ &= (u\sigma(u)\cdots\sigma^{i-1}(u))\cdot\sigma^i(u\sigma(u)\cdots\sigma^{j-1}(u)) \\ &= f(\sigma^i)\sigma^i(f(\sigma^j)). \end{aligned}$$

If $i + j \geq n$, then $0 \leq i + j - n < n$ and so

$$\begin{aligned} f(\sigma^i\sigma^j) = f(\sigma^{i+j}) = f(\sigma^{i+j-n}) &= u\sigma(u)\cdots\sigma^{i+j-n-1}(u) \\ f(\sigma^i)\sigma^i(f(\sigma^j)) &= (u\sigma(u)\cdots\sigma^{i-1}(u))\cdot\sigma^i(u\sigma(u)\cdots\sigma^{j-1}(u)) \\ &= (u\sigma(u)\cdots\sigma^{i+j-n-1}(u))\cdot\sigma^{i+j-n}(u\sigma(u)\cdots\sigma^{j-1}(u)) \\ &= f(\sigma^i\sigma^j)\sigma^{i+j-n}(\mathrm{N}_{K/F}(u)) \\ &= f(\sigma^i\sigma^j). \end{aligned}$$

So f is a cocycle. By Noether's lemma, f is also a coboundary and we can find $\alpha \in K$ with $f(\sigma^i) = \sigma^i(\alpha)/\alpha$. Therefore, $u = f(\sigma) = \sigma(\alpha)/\alpha$. □

Lemma 7.18.5 follows quickly from this theorem. If K/F is a cyclic extension of degree n and σ is a generator of $\mathrm{Gal}(K/F)$, and if F contains a primitive n-th root ω, then $\mathrm{N}_{K/F}(\omega) = \omega^n = 1$. Therefore, we can find some $a \in K$ such that $\omega = \sigma(a)/a$.

Theorem 7.19.6 (Hilbert 90, Additive Form)**.** *Let K/F be a cyclic Galois extension of degree n with σ a generator of $Gal(K/F)$. If $u \in K$, then $Tr_{K/F}(u) = 0$ if and only if $u = \sigma(a) - a$ for some $a \in K$.*

Proof. If $u = \sigma(a) - a$, then clearly $\mathrm{Tr}_{K/F}(u) = 0$. Conversely, suppose $\mathrm{Tr}_{K/F}(u) = 0$. Define $g : G \to K$ by $g(id) = 0, g(\sigma) = u$ and for $1 \leq i < n$ by

$$g(\sigma) = u + \sigma(u) + \cdots + \sigma^{i-1}(u).$$

Since $\mathrm{Tr}_{K/F}(u) = 0 = \sum_{i=1}^{n}\sigma^i(u) = 0$, for $0 \leq i, j < n$, we always have

$$\begin{aligned} g(\sigma^i\sigma^j) &= u + \sigma(u) + \cdots + \sigma^{i+j-1}(u) \\ &= (u + \sigma(u) + \cdots + \sigma^{i-1}(u)) + \sigma^i(u + \sigma(u) + \cdots + \sigma^{j-1}(u)) \\ &= g(\sigma^i) + \sigma^i(g(\sigma^j)) \end{aligned}$$

And so g is a (additive) cocycle. By Noether's lemma, g is also a coboundary, namely, we can find $a \in K$ such that $g(\sigma^i) = \sigma^i(a) - a$. Therefore, $u = g(\sigma) = \sigma(a) - a$. □

Theorem 7.18.8 then goes as follows. If K/F is a cyclic Galois extension of degree p with $\mathrm{char}(F) = p$ and σ is a generator of $\mathrm{Gal}(K/F)$, then $\mathrm{Tr}_{K/F}(1) = p = 0$. So by the theorem above, we can find $a \in K$ such that $1 = \sigma(a) - a$. And we can continue the last part of the proof of Theorem 7.18.8.

Week 8

8.20 Kummer Theory

We have descriptions on cyclic Galois extensions if the ambient field contains sufficient root of unity. Now we want to do the same for abelian extension.

Definition 8.20.1. A group G has *exponent dividing* n if $g^n = id$ for all $g \in G$. The *exponent* of G is the least such n.

Definition 8.20.2. Let F be a field of character not dividing n and contain a n-th primitive unity. A finite Galois extension K/F is said to be an *n-Kummer extension* if the Galois group $\mathrm{Gal}(K/F)$ is abelian and has exponent dividing n. If K is an n-Kummer extension of F for some n, then it is said to be a *Kummer extension* of F.

Example 8.20.3. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $K/\mathbb{Q}$ is Galois and it is a 2-Kummer extension since the Galois group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

The classification of finite abelian groups say any abelian group is a direct product of cyclic groups. Together this fact with the fundamental theorem of Galois theory and the characterization of cyclic extensions, we obtain the following theorem.

Theorem 8.20.4. *Let F be a field containing a primitive n-th root of unity and K/F a finite extension. Then K/F is an n-Kummer extension if and only if $K = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ for some $a_i \in F$.*

Proof. Suppose that $K = F(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i^n = a_i \in F$. Let ω be a primitive n-th root of unity in F. Then the distinct elements are $\alpha_i, \omega\alpha_i, \ldots, \omega^{n-1}\alpha_i$ are all the roots of $x^n - a_i \in F[x]$. Since $\mathrm{char}(F) \nmid n$, $x^n - a_i$ is also separable. Hence K as a splitting field of $\prod_i (x^n - a_i)$ is Galois. If $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(\alpha_i) = \omega^j \alpha_i$ for some j since $\sigma(\alpha_i)$ must be a root of $x^n - a_i$ as well. This is true for each i and since α_i generates K over F, we see that $\sigma^n = id$. Therefore, $\mathrm{Gal}(K/F)$ has exponent dividing n. To see $\mathrm{Gal}(K/F)$ is abelian, take $\sigma, \tau \in \mathrm{Gal}(K/F)$. We only need to show $\sigma\tau(\alpha_i) = \tau\sigma(\alpha_i)$ for each i. And it is quite straightforward to verify that.

For the converse, suppose that K/F is a Galois extension with $G = \mathrm{Gal}(K/F)$ abelian and having exponent dividing n. By the classification of finite abelian groups, $G = C_1 \times \cdots \times C_r$, where each C_i is cyclic. There is a canonical homomorphism

$$G \to C_i,$$

where the kernel is $H_i = C_1 \times \cdots \times C_{i-1} \times \hat{C}_i \times C_{i+1} \times \cdots \times C_r$, namely, the product of all C_j with $j \neq i$. Note H_i is normal in G. Let $L_i = K^{H_i}$ be the fixed field of H_i. Then by the fundamental theorem of Galois theory, L_i/F is a Galois extension with Galois group

$$\mathrm{Gal}(L_i/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/L_i) = G/H_i = C_i.$$

Therefore, L_i/F is a cyclic extension. Write $m_i = [L_i : K] = |C_i|$. Then m divides n. The field F containing a primitive n-th root of unity also contains a primitive m_i-th root of unity and so by Theorem 7.18.6, $L_i = F(\alpha_i)$ for some $\alpha_i \in L_i$ with $\alpha_i^{m_i} \in F$ and so $\alpha_i^n \in F$. And the Galois correspondence says $F(\alpha_1, \ldots, \alpha_r)$ corresponds to $\cap_{i=i}^r H_i = \{id\}$. And thus $K = F(\alpha_1, \ldots, \alpha_r) = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$. $\square$

Example 8.20.5. Let $F = \mathbb{Q}(i)$ and $\overline{F} = \overline{\mathbb{Q}} \subset \mathbb{C}$. Suppose $K = \mathbb{Q}(\sqrt[4]{12}, \sqrt[4]{3})$. Since i is a 4-th primitive root of unity, K/F is a 4-Kummer extension. Note that $[K : F] = 8$ not 16, since $K = F(\sqrt{2}, \sqrt[4]{3})$ by noting that $\sqrt{2} = \sqrt[4]{12}/\sqrt[4]{3}$.

Now suppose F be a field of characteristic not dividing n containing a n-th primitive root of unity. Let $B \subset F^\times/(F^\times)^n$ be a finite subgroup. We write

$$F(B^{1/n}) = F(\sqrt[n]{b} : b(F^\times)^n \in B).$$

The definition does not depend on the choice of representation: if $b_1(F^\times)^n = b_2(F^\times)^n$, then $b_1 = b_2\gamma^n$ for some $\gamma \in F^\times$ and so $F(b_1) = F(b_2)$ and so on. The extension $F(B^{1/n})/F$ is clearly algebraic, and it is also finite if we further require B is finite. If $B \subset F^\times/(F^\times)^n$ is generated by some $\alpha \in F^\times$, then $F(B^{1/n}) = F(\alpha^{1/n}, \alpha^{2/n}, \ldots) = F(\alpha^{1/n})$. We know that if α has order r in $F^\times/(F^\times)^n$, then $\mathrm{Gal}(F(\alpha^{1/n})) \cong \mathbb{Z}/r \cong B$. In general, if B is generated by $\alpha_1, \ldots, \alpha_s$, then $F(B^{1/n})$ is just a convenient way of writing $F(\alpha_1^{1/n}, \ldots, \alpha_s^{1/n})$. The next theorem finishes the description of Kummer extensions.

Theorem 8.20.6. *Let F be a field of characteristic not dividing n and containing a primitive n-th root, and let $B \subset F^\times/(F^\times)^n$ be a finite subgroup. Then $F(B^{1/n})/F$ is Galois and*

$$\mathit{Gal}(F(B^{1/n})/F) \cong B.$$

The extension $F(B^{1/n})/F$ is Galois by Theorem 8.20.4. The question is really to confirm what the Galois group is.

Definition 8.20.7. Let A, B, C be abelian groups writing multiplicatively. A *perfect bilinear pairing* is a function $\langle \cdot, \cdot \rangle : A \times B \to C$ such that

1. $\langle a_1 a_2, b \rangle = \langle a_1, b \rangle \langle a_2, b \rangle$,
2. $\langle a, b_1 b_2 \rangle = \langle a, b_1 \rangle \langle a, b_2 \rangle$,
3. $\langle a, b \rangle = 1$ for all $b \in B$ implies $a = 1$,
4. $\langle a, b \rangle = 1$ for all $a \in A$ implies $b = 1$.

Lemma 8.20.8. *Let A, B be abelian groups and C a cyclic group of order m. Also suppose that B has exponent dividing m. If there is a perfect bilinear pairing $A \times B \to C$, then there is an embeddings $A \to B$.*

Sketch of proof. Define a function

$$\phi : A \to \mathrm{Hom}(B, C), a \mapsto \langle a, \_ \rangle.$$

The bilinearity makes it a group homomorphism. If $a \in \ker(\phi)$, then $\langle a, b \rangle = 1$ for all $b \in B$. Being a perfect bilinear pairing of $\langle \cdot, \cdot \rangle$ implies $a = 1$ and so this is a monomorphism.

It now remains to show that if B has exponent dividing m and if $C \cong \mathbb{Z}/m\mathbb{Z}$ then we have $\mathrm{Hom}(B, C) \cong B$. However, this no canonical way to construct such an isomorphism. If B is cyclic, then $B \cong \mathbb{Z}/r\mathbb{Z}$ for some $r \mid m$. Then

$$\mathrm{Hom}(B, C) \cong \mathrm{Hom}(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{x \mapsto \frac{m}{r}ax : \mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} | a \in \mathbb{Z}/r\mathbb{Z}\} \cong \mathbb{Z}/r\mathbb{Z}.$$

Recall that there is precisely one subgroup of order r in $\mathbb{Z}/m\mathbb{Z}$. From the basics of module theory, we know that

$$\mathrm{Hom}(B_1 \times B_2, C) \cong \mathrm{Hom}(B_1, C) \times \mathrm{Hom}(B_2, C)$$

by regarding B_1, B_2, C as $\mathbb{Z}$-modules. Since every finite abelian group of exponent dividing m is a direct product of cyclic groups of exponent dividing m, this completes the proof. □

Proof of Theorem 8.20.6. From Theorem 8.20.4, we know $F(B^{1/n})/F$ is Galois. Now assume B is generated by $b_1, \ldots, b_k$ and write $E = F(B^{1/n})$ from simplicity. Now let μ_n be the group of n-th root of unity and define a map

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(E/F) \times B \to \mu_n, \ (\sigma, b(F^\times)^n) \mapsto \frac{\sigma(b^{1/n})}{b^{1/n}}.$$

Note this map is independent of the choice of coset representative since σ fixes $F^\times$ pointwise and is also independent of the choice of the n-th root of b since $\zeta \in F$. We write $\langle \sigma, b \rangle$ for simplicity. And the fact that the image is contained in μ_n is from that for any $\sigma \in \mathrm{Gal}(E/F)$ and $b \in B$, we have

$$(\langle \sigma, b \rangle)^n = (\frac{\sigma(b^{1/n})}{b^{1/n}})^n = \frac{\sigma(b)}{b} = 1.$$

We claim this map is a perfect bilinear pairing. The first two properties of a perfect bilinear pairing is trivial to check. For the remaining two properties, suppose that for some $b \in B$, we have $\langle \sigma, n \rangle = 1$ for all $\sigma \in \mathrm{Gal}(E/F)$, namely $\sigma(b^{1/n}) = b^{1/n}$. Then $b^{1/n}$ lies in the fixed subfield of $\mathrm{Gal}(E/F)$ which is $F = E^{\mathrm{Gal}(E/F)}$ precisely. But this means $b \in (F^\times)^n$ and so b represents the trivial coset.

Now fix $\sigma \in \mathrm{Gal}(E/F)$ and suppose that $\langle \sigma, b \rangle = 1$ for all $b \in B$. Then $\sigma(b^{1/n}) = b^{1/n}$ for all $b \in B$ and hence σ fixed $E = F(B^{1/n})$ pointwise. And so σ must be the trivial map.

Now B is abelian and obviously has exponent dividing n hence by the lemma above, we get an embedding $\mathrm{Gal}(E/F) \to B$. And by Theorem 8.20.4, $\mathrm{Gal}(E/F)$ is abelian and has exponent dividing n, so we have another embedding $B \to \mathrm{Gal}(E/F)$. But since both $\mathrm{Gal}(E/F)$ and B are finite groups, we must have $|B| = |\mathrm{Gal}(E/F)|$ and the embeddings are isomorphisms indeed.

□

Example 8.20.9. As we have discussed long ago, $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q}$ is Galois with Galois group isomorphic to C_2^n, where p_i are distinct primes.

Example 8.20.10. Again, let $p_1, \ldots, p_r$ be distinct primes. It is a consequence of unique factorizations of positive integers that $p_1, \ldots, p_r$ generates a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^n$. So we get $\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_r})/\mathbb{Q}$ is Galois with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$.

Example 8.20.11. Let $F = \mathbb{C}(x, y, z)$ be the rational function field in three variables over $\mathbb{C}$ and let $K = F(\sqrt[4]{xyz}, \sqrt[4]{y^2z}, \sqrt[4]{xz^2})$. Then K/F is a 4-Kummer extension. The set $B \subset F^\times/(F^\times)^4$ is generated by xyz, y^2z, xz^2. For simplicity, we just call them a, b, c. We claim that $B = \langle a, b, c \rangle$ has order 32, which

implies $[K : F] = 32$ by Theorem 8.20.6. The subgroup $\langle a, b\rangle$ has order 16 since the 16 elements $a^i b^j$ with $1 \leq, i, j \leq 4$ are all distinct. To see this, suppose $a^i b^j = a^k b^l$. Then there is an $h \in F^\times$ such that

$$(xyz)^i (y^2 z)^j = (xyz)^k (y^2 z)^l h^4.$$

Writing $h = g/f$ with $f, g \in \mathbb{C}[x, y, z]$ coprime, we get

$$(xyz)^i (y^2 z)^j f(x, y, z)^4 = (xyz)^k (y^2 z)^l g(x, y, z)^4.$$

By unique factorization, comparing powers of x, z on both sides we obtain

$$\begin{aligned} i &\equiv k \pmod 4, \\ i + j &\equiv k + l \pmod 4. \end{aligned}$$

This also gives $j \equiv l \pmod 4$. So the elements $a^i b^j$ are indeed distinct for $1 \leq i, h \leq 4$. Note that $abc = x^2 y^2 z^4$ and so $(abc)^2 \in (F^\times)^4$. Therefore, $c^2 = (ab)^2$ and so that $B = \langle a, b, c\rangle = \langle a, b\rangle$ or $\langle a, b\rangle$ is of index 2 in B. For the first to happen, we must have $c = a^i b^j$ for some i, j. Again, it leads to

$$xz^2 f(x, y, z)^4 = (xyz)^i (y^2 z)^j g(x, y, z)^4,$$

for some $f, g \in \mathbb{C}[x, y, z]$. Based on the unique factorization, we get

$$\begin{aligned} 1 &\equiv i \pmod 4, \\ 0 &\equiv i + 2j \pmod 4, \end{aligned}$$

by comparing the powers of x and y. However, this is impossible. And hence

$$\mathrm{Gal}(K/F) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

8.21 Ruler and Compass Constructions

In the days of the ancient Greeks, some of the major mathematical questions involved constructions with ruler and compass. In spite of the ability of many gifted mathematicians, a number of questions were left unsolved. It was not until the advent of field theory that these questions could be answered. We consider in this section the idea of constructibility by ruler and compass, and we answer the following four classical questions:

1. Is it possible to trisect any angle?
2. Is it possible to double the cube? That is, given a cube of volume V, a side of which can be constructed, is it possible to construct a line segment whose length is that of the side of a cube of volume $2V$?
3. Is it possible to square the circle? That is, given a constructible circle of area A, is it possible to construct a square of area A?
4. For which n is it possible to construct a regular n-gon?

The notion of ruler and compass construction was a theoretical one to the Greeks. A ruler was taken to be an object that could draw perfect, infinitely long lines with no thickness but with no markings to measure distance. The only way to use a ruler was to draw the line passing through two points. Similarly, a compass was taken to be a device that could draw a perfect circle, and the only way it could be used was to draw the circle centered at one point and passing through another. The compass was sometimes referred to as a "collapsible compass"; that is, after drawing a circle, the compass could not be lifted to draw a circle centered at another point with the same radius as that of the previous circle. Likewise, given two points a distance d apart, the ruler cannot be used to mark a point on another line a distance d from a given point on the line. (This is an unimportant restriction since, using a multi-step procedure, a distance can be transferred even with collapsing compass.)

The assumptions of constructibility are as follows. Two points are given and are taken to be the initial constructible points. Given any two constructible points, the line through these points can be constructed, as can the circle centered at one point passing through the other. A point is constructible if it is the intersection of constructible lilies and circles. For a more detailed review, please see the wikipedia.

Nevertheless, we shall convert the assumptions into modern algebraic languages. And we cover precisely section 6.4 of Bosch's and are not going to reproduce the materials here. Moreover, we shall answer the questions asked at the beginning of this section by applying the main theorem stated in Bosch's.

Theorem 8.21.1 (Ruler and Compass Constructibility Theorem)**.** *A real number c is constructible if and only if there is a tower of fields $\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$ such that c in K_r and $[K_{i+1} : K_i] \leq 2$ for each i. Therefore, if c is constructible, then c is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(c) : \mathbb{Q}]$ is a power of 2.*

Please go to the book to find the proof.

Theorem 8.21.2. *It is impossible to trisect a 60° angle by ruler and compass construction.*

Proof. If 60° can be trisected, then $\alpha = \cos(20^\circ)$ is constructible. From the triple angle formula $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$, we get $4\alpha^3 - 3\alpha = \cos 60^\circ = 1/2$. Thus α is algebraic over $\mathbb{Q}$. However, $8x^3 - 6x - 1$ having no real roots is then irreducible over $\mathbb{Q}$. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, so α can not be constructible. □

Theorem 8.21.3. *It is impossible to double a cube of length 1 by ruler and compass construction.*

Proof. The length of a side of a cube of volume 2 is $\sqrt[3]{2}$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2, so $\sqrt[3]{2}$ is not constructible. □

Theorem 8.21.4. *It is impossible to square a circle of radius 1.*

Proof. $\sqrt{\pi}$ is transcendental as we will see later hence not constructible. □

Theorem 8.21.5. *A regular n-gon is constructible if and only if $\phi(n)$ is a power of 2.*

Proof. This is discussed in great details in Bosch's. □

Week 9

9.22 Quartic Polynomials

Since it is asked in the assignment, it is helpful to develop the theory on quartic polynomials here. Let $f(x) = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible and separable polynomial over a field F, where char$(F) \neq 2$. We fix an algebraic closure $\overline{F}$ and the polynomial factors as

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4).$$

The key idea we use to find the roots and the Galois group of f here is to work with an associated cubic polynomial. Set

$$\begin{aligned}\beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4,\\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4,\\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_4,\end{aligned}$$

and

$$r(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3).$$

Note that β_i are distinct since α_i are distinct, for example,

$$\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \neq 0.$$

A computation shows that

$$r(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2 \in F[x].$$

The polynomial r is called the *resolvent* of f. Recall Vieta's formulas says that if we have a polynomial of degree n, say, $P(x) = a_nx^n + \cdots + a_1x + a_0,\ a_n \neq 0$, and its roots $r_1, \ldots, r_n$, then we have

$$\sum_{1\leq i_1<i_1<\cdots<i_k\leq n} (\prod_j^k r_{i_j}) = (-1)^k \frac{a_{n-k}}{a_n}.$$

And then we have

$$\begin{aligned}\sum_{i=1}^4 \alpha_i &= a,\\ &\cdots,\\ \prod_{i=1}^4 \alpha_i &= d.\end{aligned}$$

One can just substitute into the equations and verify then.

Definition 9.22.1. Let F be a field with $\text{char}(F) \neq 2$ and let $f(x) \in F[x]$. Let $a_1, \ldots, a_n$ be the roots of f in some splitting field K of f over K. The *discriminant* of f denoted by $\text{disc}(f)$ is defined to be

$$\text{disc}(f) = \Delta^2 = \prod_{i<j}(a_i - a_j)^2.$$

A direct calculation shows that f and r have the same discriminant, which we denote by D in this section. Let $K = F(\alpha_1, \ldots, \alpha_4)$ the splitting field of f over F and $L = F(\beta_1, \beta_2, \beta_3)$ the splitting field of r over F. And then L/F is Galois. Write $G = \text{Gal}(K/F)$. Instead of saying G is isomorphic to a subgroup of S_4, we just identify it to a subgroup of S_4 by abusing languages. Note that S_4 permutes $\{\beta_1, \beta_2, \beta_3\}$ transitively. The stabilizer of each β_i must be a subgroup of index 3 in S_4 and hence has order 8. For example, the stabilizer of β_2 is $\langle (1234), (13) \rangle$. Subgroups of order 8 are Sylow 2-subgroups of S_4. There are three of them, all isomorphic to D_4. Let

$$V = \{id, (12)(34), (13)(24), (14)(23)\}$$

be the subgroup of S_4 of order 4. Then by Sylow's theorem, V is contained in a Sylow 2-subgroup. But V is also normal in S_4, because S_3 is generated by $(12), (13)$ and (14) which can be easily verified to commutate with V. Hence V is contained in all three and hence fixed each β_i. Then we see that

$$L = K^{G \cap V}.$$

Moreover, since $V \cap G$ is also normal in G, we have the following lattice of fields.

$$K \xrightarrow{G \cap V} L \xrightarrow{G/(G \cap V)} F$$

Since f is irreducible, G is also transitive. By Orbit-Stabilizer Theorem, we know $|G|$ is divisible by 4. It is easy to see that if $|G| = 24$ or 12, then $G = S_4$ and A_4 respectively. If $|G| = 8$, then G can be all of the three Sylow 2-subgroups. If $|G| = 4$, then $G = V$ or G can be cyclic and generated by (1234) and can be its conjugates.

Theorem 9.22.2. *With the notation above, let $m = [L : F]$.*

1. *$G = S_4$ if and only if $r(x)$ is irreducible over F and $D \notin F^2$, if and only if $m = 6$.*
2. *$G = A_4$ if and only if $r(x)$ is irreducible over F and $D \in F^2$, if and only if $m = 3$.*
3. *$G = V$ if and only if $r(x)$ splits over F, if and only if $m = 1$.*
4. *$G \cong C_4$ if and only if $r(x)$ has a unique root $t \in F$ and $h(x) = (x^2 - tx + d)(x^2 + ax + (b - t))$ splits over L, if and only if $m = 2$ and $f(x)$ is reducible over L.*
5. *$G \cong D_4$ if and only if $r(x)$ has a unique root $t \in F$ and $h(x) = (x^2 - tx + d)(x^2 + ax + (b - t))$ does not split over L, if and only if $m = 2$ and $f(x)$ is irreducible over L.*

Proof. See Conrad's notes. □

9.23 Solvable Groups

Definition 9.23.1. A *(sub)normal series* of a group G is a sequence of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_t = \{1\},$$

where each G_{i+1} is a normal subgroup of G_i; the quotient groups G_i/G_{i+1} are called the *factor groups* of this series. The *length* of this series is the number of nontrivial factor groups.

Definition 9.23.2. A group G is *solvable* if it admits a normal series whose factor group are all abelian and then the normal series is called a *solvable* series.

Example 9.23.3. Here goes some basic examples:

1. Finite abelian groups are solvable.
2. Non-abelian simple groups are not solvable. In particular, A_n is not solvable for $n \geq 5$.
3. S_4 is solvable, because we can find a normal series,

   $$S_4 \supset A_4 \supset V \supset \{1\},$$

   where the factor groups are easily checked to be abelian.

Theorem 9.23.4. *Let G be a group and H its subgroup. We have the following:*

1. *If G is solvable, then H is also solvable.*
2. *If H is also normal and G is solvable, then G/H is solvable.*
3. *If H is also normal and both H and G/H are solvable, then G is solvable.*

Remark. Before we prove the following theorem, let us agree on the group isomorphism theorems as per Rotman's Advanced Abstract Algebra since different authors have different numbering and slightly modified statement.

- **First Isomorphism Theorem**: If $f : G \to H$ is a homomorphism between groups, then

  $$\ker(f) \triangleleft G \text{ and } G/\ker(f) \cong \text{im}(f).$$

- **Second Isomorphism Theorem**: If H and K are subgroups of a group G with $H \triangleleft G$, then HK is a subgroup, $H \cap K \triangleleft K$, and

  $$K/(H \cap K) \cong KH/H.$$

- **Third Isomorphism Theorem**: If H, K are normal subgroups of a group G with $K \subset H$, then $H/K \triangleleft G/K$ and

  $$(G/K)/(H/K) \cong G/H.$$

- **Correspondence Theorem**: Let G be a group, let $K \triangleleft G$, and let $\pi : G \to G/K$ be the natural map. Then

  $$S \mapsto \pi(S) = S/K$$

  is a bijection between $\text{Sub}(G; K)$, the family of all those subgroups S of G that contain K, and $\text{Sub}(G/K)$, the family of all the subgroups of G/K. Moreover, $T \subset S \subset G$ if and only if $T/K \subset S/K$, in which case, $[S : T] = [S/K : T/K]$, and $T \triangleleft S$ if and only if $T/K \triangleleft S/K$, in which case $S/T \cong (S/K)/(T/K)$.

Proof of Theorem 9.23.4. We shall prove piece by piece.

1. Since G is solvable, we can find a solvable series
$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$
such that G_i/G_{i+1} is abelian. Now consider the sequence
$$H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_n = \{1\}.$$
We shall verify it is a solvable series. Let $g_i \in H \cap G_i$ and $g_{i+1} \in H \cap G_{i+1}$. Then we consider $g_i g_{i+1} g_i$. Since $g_{i+1} \in H \cap G_i \subset H$ and $g_i \in H \cap G_i \subset G$, we have $g_i g_{i+1} g_i \in H$. Since $g_{i+1} \in H \cap G_i \subset G_{i+1}$ and $g_i \in H \cap G_i \subset G_i$ and G_{i+1} is normal in G_i, we have $g_i g_{i+1} g_i \in G_{i+1}$. So we have $g_i g_{i+1} g_i \in H \cap G_{i+1}$ for all $g_i \in H \cap g_i$ and $g_{i+1} \in H \cap G_{i+1}$ and then $H \cap G_{i+1}$ is normal in G_i. Moreover, by the Second Isomorphism Theorem, we have
$$(H \cap G_i)/(H \cap G_{i+1}) = (H \cap G_i)/((H \cap G_i) \cap G_{i+1}) \cong G_{i+1}(H \cap G_i)/G_{i+1}.$$
Note that $G_{i+1}(H \cap G_i)$ is a subgroup of G_i and hence $(H \cap G_i)/(H \cap G_{i+1})$ is isomorphic to a subgroup of G_i/G_{i+1} and hence is abelian. So indeed, the sequence of subgroups above is a solvable series and H is solvable.

2. Since G is solvable, we can find a solvable series
$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$
such that G_i/G_{i+1} is abelian. Write $N = H$ to emphasis that it is normal. Note that $GN = G$ and then $G/N = GN/N$. We construct the following sequence
$$G/N = GN/N = G_0N/N \supset G_1N/N \supset \cdots \supset G_nN/N = \{1\}.$$
We need to check this is a solvable series. Instead of doing directly, The trick here is to consider the following sequence:
$$G = GN = G_0N \supset G_1N \supset \cdots \supset G_nN = N.$$
By the Correspondence Theorem, $G_{i+1}N/N$ is normal in G_iN/N if and only if $G_{i+1}N$ is normal in G_iN. And if this is the case, by Third Isomorphism Theorem
$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N.$$
So the tasks to check are that $G_{i+1}N$ is normal in G_iN and that $G_iN/G_{i+1}N$ is abelian. Let $g_in \in G_iN$, where $g_i \in G_i$ and $n \in N$. Then we have
$$\begin{aligned}(g_in)G_{i+1}N(g_in)^{-1} &= g_i(nG_{i+1}Nn^{-1})g_i^{-1} \subset g_i(NG_{i+1}N)g_i^{-1} \subset g_i(G_{i+1}NG_{i+1}N)g_i^{-1} \\ &\subset g_i(G_{i+1}N)g_i^{-1} = g_iG_{i+1}g_i^{-1}N \subset G_{i+1}N.\end{aligned}$$
So $G_{i+1}N$ is a subset of G_iN. By the Second Isomorphism Theorem,
$$G_iN/G_{i+1}N = G_i(G_{i+1}N)/G_{i+1}N \cong G_i/G_i \cap (G_{i+1}N).$$
Note that $G_{i+1} \triangleleft G_i \cap G_{i+1}N \subset G_i$ and by the Correspondence Theorem and the Third Isomorphism Theorem, we have a surjection from G_i/G_{i+1} to $G_i/G_i \cap G_{i+1}N$. This implies $G_i/G_i \cap G_{i+1}N$ is abelian and so is $G_iN/G_{i+1}N$. So the series above is a solvable series and G/N is solvable.

3. Since G/H is solvable, we can find a solvable series

$$G/H = K_0^* \supset K_1^* \supset \cdots \supset K_m^* = \{1\}$$

with each K_i^*/K_{i+1}^* abelian. By the Correspondence Theorem, there are subgroups of G, namely,

$$G = G_0 = K_0 \supset K_1 \supset \cdots \supset K_m = H$$

with $K_i/H = K_i^*$ and $K_{i+1} \triangleleft K_i$. By the Third Isomorphism Theorem,

$$K_i^*/K_{i+1}^* \cong K_i/K_{i+1},$$

and so K_i/K_{i+1} is abelian for each i. Since H is solvable, there is a solvable series

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\}$$

with abelian factor groups. Concatenating these two series together, we get

$$G = K_0 \supset K_1 \supset \cdots \supset K_m = H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\},$$

which is easily seen to be a solvable series. So G is solvable.

□

Corollary 9.23.5. *If G_1, G_2 are solvable, then so is $G_1 \times G_2$.*

Corollary 9.23.6. *A finite p-group is solvable.*

Proof. Every p-group have a nontrivial center and we can prove by induction. □

Let G be a group. Recall the commutator of $x, y \in G$ is

$$[x, y] = xyx^{-1}y^{-1} = xy(yx)^{-1}.$$

Thus $[x, y] = 1$ if and only if x, y commutate and G is abelian if and only if all commutators are trivial.

For any homomorphism $\phi : G \to H$, we see that

$$\phi([x, y]) = \phi(xyx^{-1}y^{-1}) = [\phi(x), \phi(y)],$$

namely, ϕ maps commutators to commutators.

Definition 9.23.7. The subgroup $G' = G^{(1)}$ generated by all commutator in a group G is called the *commutator subgroup* or the *first derived subgroup* of G. And the n-th derived can be defined by induction $G^{(n+1)} = (G^{(n)})'$. The *derived series* is the sequence

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \ldots,$$

which is easily seen to be a normal series.

Remark. Not every element of the commutator subgroup os a group is itself a commutator, but the smallest group where this occurs has order 96.

Definition 9.23.8. A subgroup H of a group G is a *characteristic subgroup* if $\phi(H) = H$ for all group automorphism ϕ of G.

Example 9.23.9. The center $Z(G)$ of a group G is a characteristic subgroup.

Theorem 9.23.10. *The commutator subgroup G' is a characteristic subgroup of G; it is the smallest normal subgroup such that G/G' is abelian.*

Proof. An automorphism ϕ of G maps the generating set of G' into G' and hence maps G' to G'. This is true for all automorphisms of G, and so G' is characteristic.

To see G' is a normal subgroup, let $a, b, g \in G$. Then we have

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}].$$

And so the conjugation by g maps the generators of G' back to G' and so G' is normal.

Write $g \mapsto \overline{g}$ for the canonical map $g \mapsto gG' : G \to G/G'$. Then $[\overline{g}, \overline{h}] = \overline{[g,h]}$, which is 1 since $[g,h] \in G'$. Hence $[\overline{g}, \overline{h}] = 1$ for all $\overline{g}, \overline{h} \in G/G'$ and so G/G' is abelian.

Let N be another normal subgroup such that G/N is abelian. Then $[g,h] \mapsto 1$ in G/N and so $[g,h] \in N$. Since these elements generates G', we have $G' \subset N$. □

Theorem 9.23.11. *A group G is solvable if and only if its k-th derived subgroup $G^{(k)} = \{1\}$ for some k.*

Proof. If $G^{(k)} = 1$, then the derived series

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(k)} = \{1\}$$

is a solvable series.

Conversely, suppose G is solvable. We can find a solvable series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

with each factor group G_i/G_{i+1} is abelian. So we see that $(G_i)' \subset G_{i+1}$ by above theorem. Now we show by induction that $G^{(i)} \subset G_i$ for all i. The inclusion holds trivially for $i = 0$. Now suppose the inclusion is true for $0 \leq i \leq n$. Then

$$G^{(i+1)} = (G^{(n)})' \subset (G_i)' \subset G_{i+1}$$

as desired. In particular, it follows that $G^{(n)} \subset G_n = \{1\}$. □

Definition 9.23.12. A *meta-abelian group* is a group whose commutator subgroup is abelian.

Abelian and meta-abelian groups are solvable. In fact, meta-abelian groups are precisely the solvable groups of derived length at most 2.

Proposition 9.23.13. *The symmetric group S_n is solvable for $n \leq 4$, but not solvable for $n \geq 5$.*

Remark. We use the fact that A_n is simple for $n \geq 5$.

Proof. We have the following derived series of S_n for $n \leq 4$:

$$S_2 \supset \{1\},$$
$$S_3 \supset A_3 \supset \{1\},$$
$$S_4 \supset A_4 \supset V \supset \{1\},$$

where V in the last series is the Klein four group.

However, the derived series of S_n for $n \geq n$ is

$$S_n \supset A_n \supset A_n \supset \ldots,$$

which never terminates to $\{1\}$. However, by the theorem above, if a group is solvable, the derived series eventually becomes $\{1\}$. □

Theorem 9.23.14 (Feit-Thompson)**.** *Every finite group of odd degree is solvable.*

The proof is beyond the scope of this course and we omit it here.

Definition 9.23.15. A *composition series* of a group is a normal series where all the factor groups are simple and nontrivial. The list of factor groups of a composition series of G is called the list of *composition factors* of G.

A group need not have a composition; for example, $\mathbb{Z}$ does not admit a composition series although it is solvable.

Proposition 9.23.16. *Ever finite group G has a composition series.*

Proof. We prove by induction on the order of G. If G is simple, then $G \supset \{0\}$ is a composition series. If G is not simple, then let H be a maximal proper normal subgroup so that G/H is simple. But $|H| < |G|$ and so that H has a composition series:

$$H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}.$$

We then get a composition series of G:

$$G \supset H = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}.$$

□

Definition 9.23.17. Two normal series of G,

$$G = G_0 \supset \cdots \supset G_m = \{1\} \text{ and } G = G'_0 \supset \cdots \supset G'_n = \{1\},$$

are *isomorphic* if $n = m$ and there is a permutation $\sigma \in S(\{0, 1, \ldots, n-1\})$ such that

$$G_{\sigma(i)}/G_{\sigma(i)+1} \cong G'_i/G'_{i+1},$$

for all $i = 0, 1, \ldots, n-1$.

Example 9.23.18. Let $G = \mathbb{Z}/30$. Consider the following two normal series:

$$G = \mathbb{Z}/30 = G_0 \supset G_1 = \langle 3 \rangle \supset G_2 = \langle 6 \rangle \supset G_3 = \{1\},$$
$$G = \mathbb{Z}/30 = G'_0 \supset G'_1 = \langle 5 \rangle \supset G'_2 = \langle 15 \rangle \supset G'_3 = \{1\}.$$

They are two composition series and isomorphic by a straightforward checking.

We aim to prove the following profound theorem which is of historical importance in the development of group theory.

Theorem 9.23.19 (Jordan-Hölder Theorem)**.** *Any two composition series of a group G are isomorphic. In particular, the length of a composition series, if exists, is an invariant of G.*

We need some technical lemmas to prove the Jordan-Hölder Theorem.

Lemma 9.23.20 (Zassenhaus Lemma, aka Butterfly Lemma)**.** *Given four subgroups $A \triangleleft A^*$ and $B \triangleleft B^*$ of a group G, then $A(A^* \cap B) \triangleleft A(A^* \cap B^*)$, $B(B^* \cap A) \triangleleft B(B^* \cap A^*)$, and there is an isomorphism*

$$A(A^* \cap B^*)/A(A^* \cap B) \cong B(B^* \cap A^*)/B(B^* \cap A).$$

Proof. We claim that $A \cap B^* \triangleleft A^* \cap B^*$. Let $c \in A \cap B^*$ and $x \in A^* \cap B^*$. Now $xcx^{-c} \in A$ since $c \in A$ and $x \in A^*$, and xcx^{-1} since $c \in B^*$ and $x \in B^*$. Therefore $xcx^{-1} \in A \cap B^*$ and this is true for all $c \in A \cap B^*$ and $x \in A^* \cap B^*$ and so $A \cap B^* \triangleleft A^* \cap B^*$. Similarly, $A^* \cap B \triangleleft A^* \cap B^*$. Write $D = (A \cap B^*)(A^* \cap B)$. Then D is a subgroup of $A^* \cap B^*$.

By symmetry, it suffices to show that there is an isomorphism

$$A(A^* \cap B^*)/A(A^* \cap B) \to A^* \cap B^*/D.$$

Define

$$\phi : A(A^* \cap B^*) \to A^* \cap B^*/D, ax \mapsto xD,$$

where $a \in A$ and $x \in A^* \cap B^*$. We need to check is well-defined: if $ax = a'x'$, where $a, a' \in A$ and $x, x' \in A^* \cap B^*$, then $(a')^{-1}a = x'x^{-1} \in A \cap (A^* \cap B^*) = A \cap B^* \subset D$; hence $xD = x'D$. Also, ϕ is a group homomorphism: write $axa'x' = a''xx'$, where $a'' = a(xa'x^{-1}) \in A$ because $A \triangleleft A^*$, and so

$$\phi(axa'x') = \phi(a''xx') = xx'D = \phi(ax)\phi(a'x').$$

Since $A^* \cap B^* \subset A(A^* \cap B^*)$, ϕ is surjective and the kernel is $\ker(\phi) = A(A^* \cap B)$. By the First Isomorphism Theorem, it completes the proof. □

Definition 9.23.21. A *refinement* of a normal series of a group G is a normal series having the original series as a subseries.

Theorem 9.23.22 (Schreier Refinement Theorem)**.** *Any twi normal series of a group G,*

$$G = G_0 \supset \cdots \supset G_n = \{1\} \text{ and } G = N_0 \supset \cdots \supset N_k = \{1\},$$

have isomorphic refinements.

Proof. We insert a copy of the second series between each pair of adjacent terms in the first series. In more details, for each $i \geq 0$, define

$$G_{ij} = G_{i+1}(G_i \cap N_j),$$

which is a subgroup since $G_{i+1} \triangleleft G_i$. Since $N_0 = G$, we have

$$G_{i0} = G_{i+1}(G_i \cap N_0) = G_{i+i}G_i = G_i.$$

Similarly, since $N_k = \{1\}$, we have

$$G_{ik} = G_{i+1}(G_i \cap N_k) = G_{i+1}.$$

Therefore, the series of G_i is a subsequence of the series of G_{ij}:

$$\cdots \supset G_i = G_{i0} \supset G_{i1} \supset \cdots \supset G_{ik} = G_{i+1} \supset \ldots.$$

Similarly, the second series of N_j is a subsequence of the series

$$N_{ji} = N_{j+1}(N_j \cap G_i).$$

Both sequences are doubly indexed and have nk terms. For each i, j, the Zassenhaus Lemma, for the four subgroups $G_{i+1} \triangleleft G_i$ and $N_{j+1} \triangleleft N_j$, says both sequences are normal series and hence are refinements, and there os an isomorphism

$$G_{i+1}(G_i \cap N_k)/G_{i+1}(G_i \cap N_{j+1}) \cong N_{j+1}(N_j \cap G_i)/N_{j+1}(N_j \cap G_{i+1}),$$

that is $G_{i,j}/G_{i,j+1} \cong N_{j,i}/N_{j,i+1}$. And we see these two refinements are isomorphic. □

Proof of Theorem 9.23.19. Any refinement of a composition is insignificant in the sense that one can insert repetitions only since all the factor groups are simple. The it follows from Schreier Refinement Theorem, any two composition series are isomorphic. □

Corollary 9.23.23. *Every integer $n \geq 2$ has a factorization into primes, which are unique up to rearrangement.*

Proof. Note that the only simple abelian groups are cyclic and of prime order and consider the composition series of $\mathbb{Z}/n\mathbb{Z}$. □

Week 10

10.24 Solvability by Radicals

Definition 10.24.1. Let E/F be a finite extension. We say E is an *extension by radicals* of F if there exist $a_1, \ldots, a_n \in E$ such that $E = F(a_1, \ldots, a_n)$ and that for all $1 \leq i \leq k$, we have $a_i^n \in F(a_1, \ldots, a_{i-1})$ for some n. We say $f(x) \in F[x]$ is *solvable by radicals* if $f(x)$ splits in some E, an extension of F by radicals, or equivalently, the splitting field of $f(x)$ is contained in some extension E of F by radicals.

Note that there is not "Galois" involved in the definition.

Example 10.24.2. For any positive integer n, the polynomial $f(x) = x^n - a \in \mathbb{Q}[x]$ is solvable by radicals. The splitting field of $f(x)$ is $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$, where ζ_n is a primitive n-th root of unity.

Example 10.24.3. For any positive integer n and $a, b \in \mathbb{Q}$, the polynomial

$$f(x) = x^{2n} + ax^n + b \in \mathbb{Q}[x]$$

is solvable by radicals. To see this, note the splitting field of $f(x)$ is contained in $\mathbb{Q}(\zeta_n, a_1, a_2, a_3)$, where ζ_n is a n-primitive root of unity, $a_1^2 = a^2 - 4b$, $a_2^n = (-a + a_1)/2$, and $a_3^n = (-a - a_1)/2$.

Definition 10.24.4. Let E/F be a finite Galois extension. E/F is said to be a *solvable* extension if the Galois group $\mathrm{Gal}(E/F)$ is a solvable group.

Proposition 10.24.5. *Let $F \subset K \subset E$ be fields such that E/F and K/F are finite Galois extensions. Then E/F is solvable if and only if both E/K and K/F are solvable.*

Proof. This is just Theorem 9.23.4 and the fundamental theorem about Galois theory. □

Theorem 10.24.6 (Galois)**.** *Let F be a field of characteristic 0 and E/F be a finite Galois extension. Then E/F is contained in an extension by radicals if and only if E/F is a solvable extension. In particular, $f(x) \in F[x]$ is solvable by radicals if and only if its Galois group is solvable.*

We need some lemmas to prove this theorem.

Lemma 10.24.7. *Let F be a field of characteristic 0 and E be a splitting field of $x^n - a \in F[x]$ for some $a \in F$. Then Gal(E/F) is solvable.*

Proof. If F contains a primitive n-th root, then we know that $E = F(\sqrt[n]{a})$ and $\mathrm{Gal}(E/F) \cong \mathbb{Z}/r\mathbb{Z}$ for some $a \in F$ and some $r \mid n$ from previous sections.

If F does not contain a primitive n-th root unity, let ζ be one such root. Now the minimal polynomial of ζ is some factor of $\Phi_n(x) \in F[x]$ and so other roots are all powers of ζ. Therefore $F(\zeta)/F$ is a Galois extension. Moreover,

$$\mathrm{Gal}(F(\zeta)/F) = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/F(\zeta)).$$

Since both $\mathrm{Gal}(E/F(\zeta))$ and $\mathrm{Gal}(F(\zeta)/F)$, being a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, are solvable, we deduce that $\mathrm{Gal}(E/F)$ is solvable. □

Theorem 10.24.8 (Natural Irrationality)**.** *Let K/F be a finite Galois extension and L/F another finite extension. Then KL is a finite Galois extension of L and Gal$(KL/L) \cong$ Gal$(K/(K \cap L))$.*

Proof. The field K, as a finite Galois extension of F, is a splitting field of some separable polynomial $f[x] \in F[x]$. Regarding $f(x)$ as a polynomial in $L[x]$, $f(x)$ is also separable and then KL as the splitting field of $f(x)$ over L is a finite Galois extension of L, since it is both separable and normal.

Define $\phi : \text{Gal}(KL/L) \to \text{Gal}(K/F)$ by $\phi(\sigma) = \sigma|_K$. This map is well defined since K is normal over F, and ϕ is obviously a group homomorphism. The kernel of ϕ is

$$\ker \phi = \{\sigma \in \text{Gal}(KL/L) : \sigma|_K = id_K\}.$$

Note that $\sigma \in \ker(\phi)$ implies $\sigma|_K = id_K$ and $\sigma|_L = id_L$ and so ϕ fixes KL and $\phi = id$. In other words, ϕ is injective. Let $E = K^{\text{im}(\phi)}$ be the subfield of K fixed by the image of Gal(KL/L). We show that $E = K \cap L$. We have $\sigma|_L = id_L$ for all $\sigma \in \text{Gal}(KL/L)$ and if $a \in K \cap L \subset L$, then $\sigma(a) = a$ and so $K \cap L \subset E$. For the reverse inclusion, let $a \in E$. Then we have $a \in K$ and $\sigma(a) = \sigma|_K(a) = a$ for all $\sigma \in \text{Gal}(KL/L)$. This means $a \in KL^{\text{Gal}(KL/L)} = L$ and so $a \in K \cap L$. So $E \subset K \cap L$ and then $E = K \cap L$. We have proved that

$$\text{Gal}(KL/L) \cong \text{im}(\phi) = \text{Gal}(K/K \cap L).$$

□

Proof of Theorem 10.24.6. Suppose E/F is contained in an extension by radicals, say, E'/F is that extension. We suppose that $E' = F(a_1, \ldots, a_k)$ such that for each i, $a_i^n \in F(a_1, \ldots, a_{i-1})$ for some n. Passing to the normal closure of E' if necessary, we can assume E'/F is Galois. If Gal(E'/F) is solvable, then by Proposition 10.24.5, Gal(E/F) is also solvable. We claim indeed Gal(E'/F) is solvable. If $k = 0$, the extension is trivial and so is the claim. Now suppose the statement is true for extensions by $k-1$ radicals. We have $a_1^n \in F$ for some n, so let K/F be the splitting field of $x^n - a_1^n \in F[x]$. Since E'/F is normal with a_1 a root of $x^n - a_1^n$, we have $K \subset E'$. Now by the lemma above, K/F is solvable. It suffices to show E'/K is solvable. But we see that $E' = K(a_2, \ldots, a_k)$ and that $a_i^n \in K(a_2, \ldots, a_{i-1})$ for some n for each $2 \leq i \leq k$. By induction hypothesis, E'/K is solvable. We finish the induction.

For the other direction, we proceed by the number of terms in the composition series of Gal(E/F). If the length is 0, then Gal(E/F) is trivial and so we are done. Now suppose the statement is true when the length of the composition series is $k-1$ and let

$$\text{Gal}(E/F) = G_0 \supset G_1 \supset \cdots \supset G_k = \{1\}$$

be the composition series of Gal(E/F). The field $K = E^{G_1}$ is then a Galois extension of F, and the composition series of Gal(E/K) is

$$\text{Gal}(E/K) = G_1 \supset \cdots \supset G_k = \{1\}.$$

By induction hypothesis, E is contained in an extension by radicals, say $K(a_1, \ldots, a_s)$. If K is contained in an extension of F by radicals, say $F(b_1, \ldots, b_m)$, then it is easily seen that $E \subset F(b_1, \ldots, b_m, a_1, \ldots, a_s)$, namely, E is contained in an extension of F by radicals. So it suffices to show that K is contained in an extension of F by radicals. By the definition of solvability,

$$\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K) = G_0/G_1$$

is a simple abelian group and hence is a cyclic abelian group of prime order p. Let $\zeta \in \overline{F}$ be a primitive p-th root. Clearly, $F(\zeta)$ is an extension of F by radicals. Now apply Natural Irrationality Theorem, $K(\zeta) = KF(\zeta)$ is a Galois extension of $F(\zeta)$ and

$$\text{Gal}(K(\zeta)/F(\zeta)) \cong \text{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z}.$$

Since $F(\zeta)$ contains a primitive p-th root of unity, we see from Theorem 7.18.6 that $K(\zeta) = F(\zeta, \sqrt[n]{a})$ for some $a \in F(\zeta)$, that is, K is contained in an extension of F by radicals. Hence so is E. □

Now from Theorem 5.15.2, we known that if $f(x) \in \mathbb{Q}[x]$ is irreducible and has exactly 3 real roots, then G_f is isomorphic to S_5, which is not solvable. Moreover, Example 5.15.2 translates into that $f(x) = (x^2+4)(x-2)(x-4)(x-6) - 2$ is not solvable by radicals.

If you accept the fact the simple of the minimal order is isomorphic to S_5, then you have the following corollary.

Corollary 10.24.9. *Let L/K be a separable field extension of degree ≤ 4. Then L/K is solvable by radicals.*

So far, we just considered the case where the characteristic of the ambient field is 0. In order to approach the theory of characteristic p, we need to modify the definitions a bit in the sprit of Artin-Schreier Theorem.

Definition 10.24.10. A finite field extension L/K is *solvable by radicals* if L admits an extension field E together with a chain of field extension

$$K = E_0 \subset E_1 \subset \cdots \subset E_m = E$$

such that in each case, E_{i+1} is obtained from E_i by adjoining an element of the following type:

1. a root of unity,
2. a zero of a polynomial of the type $x^n - a \in E_i[x]$, where $\text{char}(K) \nmid n$,
3. a zero of a polynomial of the type $x^p - x - a \in E_i[x]$ for $p = \text{char}(K) > 0$.

Then L/K is necessarily separable.

Proposition 10.24.11. *Any abelian extension is solvable by radicals.*

10.25 Generic and Symmetric Polynomials

When we say quintics are not solvable by radicals, what do we really mean? It can be said more formally that the generic equation of degree n over the rational function field $K = k(c_1, c_2, \ldots, c_n)$ is not solvable. We shall give formal definitions.

We fix a field k and consider over it the field L of rational functions in many variables (indeterminates) $T_1, \ldots, T_n$, namely,

$$L = k(T_1, \ldots, T_n) = \text{Frac}(k[T_1, \ldots, T_n]).$$

Every permutation $\pi \in S_n$ defines an automorphism of L in a canonical way:

$$k(T_1, \ldots, T_n) \to k(T_1, \ldots, T_n), \ \frac{g(T_1, \ldots, T_n)}{h(T_1, \ldots, T_n)} \mapsto \frac{g(T_{\pi(1)}, \ldots, T_{\pi(n)})}{h(T_{\pi(1)}, \ldots, T_{\pi(n)})}.$$

The corresponding fixed field $K = L^{S_n}$ is referred as the field of *symmetric rational functions* in n variables with coefficients in k. By Artin's Theorem, the extension L/K is Galois with Galois group S_n.

Now we choose a variable X and consider the polynomial

$$f(X) = \prod_{i=1}^{n}(X - T_i) = \sum_{j=0}^{n}(-1)^j s_j(T_1, \ldots, T_n)X^{n-j} \in k[T_1, \ldots, T_n][x],$$

where s_j is obtained by expanding the product of $X - T_i$ and by collecting coefficients of X^{n-j}. s_j is called bt j-th *elementary symmetric polynomial* in $T_1, \ldots, T_n$, more explicitly, they are given by

$$\begin{aligned} s_0 &= 1, \\ s_1 &= T_1 + \cdots + T_n, \\ s_2 &= \sum_{1 \le i < j \le n} T_i T_j \\ &\ldots \\ s_n &= T_1 \ldots T_n. \end{aligned}$$

Regarding f as an element in $L[X]$, we see that it is invariant under S_n and so its coefficients are also invariant. Therefore, we have $k(s_1, \ldots, s_n) \subset K$. Similarly, by treating f as a polynomial in $k(s_1, \ldots, s_n)[X]$, we see that L is the splitting field of f over $k(s_1, \ldots, s_n)$. Moreover, since the Galois group is transitive, f is irreducible.

Definition 10.25.1. Let L/K be a field extension. A system $(x_1, \ldots, x_n)$ of elements in L is called *algebraically independent* or *transcendental* over K if every equation $f(x_1, \ldots, x_n) = 0$ for a polynomial $f \in K[X_1, \ldots, X_n]$ implies $f = 0$, namely, if the evaluation map

$$K[X_1, \ldots, X_n] \to L, \quad f(X_1, \ldots, X_n) \mapsto f(x_1, \ldots, x_n)$$

is injective.

Theorem 10.25.2. *Every symmetric rational function in $k(T_1, \ldots, T_n)$ can be written uniquely as rational function over k in the elementary polynomials $s_1, \ldots, s_n$, more precisely,*

1. *$k(s_1, \ldots, s_n) = K$,*
2. *$s_1, \ldots, S_n$ are algebraically independent over k.*

Proof. Observe that $[L : K] = |S_n| = n!$. But L is the splitting field of $f = \prod(X - T_i)$ over $k(s_1, \ldots, s_n)$ hence $[L : k(s_1, \ldots, s_n)] \le n!$. With $k(s_1, \ldots, s_n) \subset K$, we indeed have $K = k(s_1, \ldots, s_n)$.

To see the elementary polynomials are algebraically independent, consider $k(S_1, \ldots, S_n)$ of all rational functions in n variables over k. With the convention $S_0 = 1$, we consider the function

$$\tilde{f}(X) = \sum_{j=0}^{n}(-1)^j S_j X^{n-j} \in k(S_1, \ldots, S_n)[X]$$

as well as its splitting field $\tilde{L}$. Let $t_1, \ldots, t_n$ be all the roots of $\tilde{f}$ in $\tilde{L}$ allowing repetitions. Then we see that

$$\tilde{L} = k(S_1, \ldots, S_n)(t_1, \ldots, t_n) = k(t_1, \ldots, t_n),$$

since $S_1, \dots, S_n$ can be written as elementary symmetric functions in $t_1, \dots, t_n$ and so they belong to $k(t_1, \dots, t_n)$. Now consider the evaluation map

$$k[T_1, \dots, T_n] \to k[t_1, \dots, t_n], f(T_1, \dots, T_n) \mapsto f(t_1, \dots, t_n).$$

It maps elementary functions in $T_1, \dots, T_n$ to elementary function in $t_1, \dots, t_n$ and thus restricts to a homomorphism

$$k[s_1, \dots, s_n] \to k[S_1, \dots, S_n], f(s_1, \dots, s_n) \to f(S_1, \dots, S_n).$$

Since $S_1, \dots, S_n$ are variables, this map is necessarily injective and therefore an isomorphism. In particular, $s_1, \dots, s_n$ may be viewed as variables and hence are algebraically independent over k. □

The idea we have just employed, namely to make use of generic polynomials, i.e., of polynomials with variables as coefficients, leads immediately to the generic equation of degree n. Indeed, fixing variables $S_1, \dots, S_n$, the polynomial

$$p(X) = X^n + S_1 X^{n-1} + \cdots + S_n \in k(S_1, \dots, S_n)[X]$$

is referred to as the *generic polynomial* (aka *general polynomial*) of degree n over k. The corresponding equation $p(x) = 0$ is called the *generic equation* (aka *general equation*) of degree n. We want to determine its Galois group by showing that we may identify $p(X)$ up to isomorphism with the polynomial $f(X)$ discussed above.

Theorem 10.25.3. *The generic polynomial $p(x) \in k(S_1, \dots, S_n)[X]$ of degree n is separable and irreducible. It admits S_n as its Galois group.*

Proof. As discussed above, let $L = k(T_1, \dots, T_n)$ and $K = L^{S_n} = k(s_1, \dots, s_n)$. Since the elementary symmetric polynomials are algebraically independent over k, we can view them as variables and therefore introduced a k-isomorphism

$$k(S_1, \dots, S_n) \to k(s_1, \dots, s_n) = K$$

via $S_j \mapsto (-1)^j s_j$. Interpreting this as an identification, $p(x)$ is then transformed into the familiar polynomial

$$f(x) = \prod_{i=1}^{n} (X - T_i) = \sum_{j=0}^{n} (-1)^j s_j X^{n-j} \in K[X].$$

Therefore, $p(x)$, just like f, is separable and irreducible and admits S_n as its Galois group. □

Now it makes more sense to say quintic, the generic polynomial of degree 5, is irreducible.

If we restrict the automorphism of $k(T_1, \dots, T_n)$ given by S_n to the subring $k[T_1, \dots, T_n]$, then just as the case of rational functions, we get the symmetric polynomial $f \in k[T_1, \dots, T_n]$, which is fixed by all permutations $\pi \in S_n$.

Theorem 10.25.4 (Fundamental Theorem on Symmetric Polynomials)**.** *For every symmetric polynomial $f \in k[T_1, \dots, T_n]$, there is a unique polynomial $g \in k[S_1, \dots, S_n]$ in n variables $S_1, \dots, S_n$ such that $f = g(s_1, \dots, s_n)$.*

Proof. Uniqueness follows directly from the algebraic independence of the polynomials $s_1, \ldots, s_n$.

Consider the lexicographic order on $\mathbb{N}^n$, where $v \preceq v'$ for $v, v' \in \mathbb{N}^n$ if there is an m such that $v_m < v'_m$ and $v_i = v'_i$ for $1 \leq i < m$. Then for any nontrivial polynomial $f = \sum_v c_v T^v \in k[T_1, \ldots, T_n]$, then set $\{v \in \mathbb{N}^n : c_v \neq 0\}$ is finite and has a largest element. Such an element is unique and called the lexicographic degree of f denoted by $\operatorname{lexdeg}(f)$. Now let $f = \sum c_v T^v$ be a symmetric polynomial with lexicographic degree $\operatorname{lexdeg}(f) = u = (u_1, \ldots, u_n)$. Then we have $u_1 \geq u_2 \geq \cdots \geq u_n$ since f is symmetric. Furthermore,

$$f_1 = c_u s_1^{u_1 - u_2} s_2^{u_2 - u_3} \ldots s_n^{u_n} \in k[s_1, \ldots, s_n]$$

is a symmetric polynomial of total degree $\sum u_i$ and has lexicographic degree u. This implies

$$\operatorname{lexdeg}(f - f_1) < \operatorname{lexdeg}(f), \quad \deg(f - f_1) \leq \deg(f).$$

If f is different from f_1, we can repeat this step once more, replacing f by $f - f_1$. Continuing this wat, we end uup with a sequence $f_1, \cdots \in k[s_1, \ldots, s_n]$ such that the lexicographic degree of the sequence

$$f, f - f_1, f - f_1 - f_2, \ldots$$

decreases step by step, while in the same time, th total degree is bounded by $\deg(f)$. Therefore, the sequence will end after finitely many steps with the zero polynomial, thereby yielding a representation of f as a polynomial in the elementary symmetric polynomials $s_1, \ldots, s_n$. □

The proof of this theorem yields a very effective principle to determine for a given symmetric polynomial f a polynomial g satisfying $f = g(s_1, \ldots, s_n)$. Note that the principle works quite generally over an arbitrary ring R instead of k as coefficient domain.

Example 10.25.5. In three variables, treating X_1, X_2, X_3 as X, Y, Z, let $f(X, Y, Z) = X^4 + Y^4 + Z^4$. We want to write f as a polynomial in the elementary symmetric polynomials in X, Y, Z, which are

$$s_1 = X + Y + Z, s_2 = XY + XZ + YZ, s_3 = XYZ.$$

The leading term of f is X^4 with lexicographic degree $u = (4, 0, 0)$. So we subtract

$$\begin{aligned} f - s_1^4 = f - (X + Y + Z)^4 = &- 4X^3Y - 4X^3Z - 6X^2Y^2 - 12X^2YZ - 6X^2Z^2 - 4XY^3 \\ &- 12XY^2Z - 12XYZ^2 - 4XZ^3 - 6Y^3Z - 6Y^2Z^2 - 6YZ^3. \end{aligned}$$

This has leading term $-4X^3Y$ with lexicographic degree $(3, 1, 0)$. So we do the subtraction again:

$$f - s_1^4 + 4s_1^2 s_2 = 2X^2Y^2 + 8X^2YZ + 2X^2Z^2 + 8XY^2Z + 8XY^2Z + 8XYZ^2 + 2Y^2Z^2.$$

This has leading term $2X^2Y^2$ with lexicographic order $(2, 2, 0)$. We do the subtraction one more time:

$$f - s_1^4 + 4s_1^2 s_2 - 2s_2^2 = 4X^2YZ + 4XY^2Z + 4XYZ^2.$$

This had leading term $4X^2YZ$ with lexicographic order $(2, 1, 1)$. We do the subtraction one more time:

$$f - s_1^4 + 4s_1^2 s_2 - 2s_2^2 - 4s_1 s_3 = 0.$$

Thus

$$X^4 + Y^4 + Z^4 = s_1^4 - 4s_1^2 s_2 + 2s_2^2 + 4s_1 s_3.$$

Corollary 10.25.6. *Let L/K be a field extension and $f(x) \in K[x]$ factor as*

$$f(x) = (x - a_1) \ldots (x - a_n) \in L[x].$$

Then for all positive integer r, we have

$$(x - a_1^r) \ldots (x - a_n^r) \in K[x].$$

If time permits, we shall discuss about resultant. I will not bother to reproduce the materials here.

Week 11

11.26 Topological Groups

We need some preliminaries before going into infinite Galois extension.

Definition 11.26.1. A *topological group* is a group G endowed with a topology such that the multiplication, $G \times G \to G, (x, y) \mapsto xy$, and the inverse map, $G \to G, x \mapsto x^{-1}$, are continuous.

Remark. Munkres also puts the T_1-axiom in the definition.

Example 11.26.2. $\mathbb{Q}$ viewed as an additive group with usual topology is a topological group. In particular, any Lie group is a topological group.

Lemma 11.26.3. *For every $g \in G$, the left multiplication $l_g : G \to G, x \mapsto gx$ is a homeomorphism. If U is an open (resp. closed) subset, then the coset gU is also open (resp. closed) for any $g \in G$.*

Proof. Consider the composition

$$G \to G \times G \to G, x \mapsto (g, x) \mapsto gx.$$

The composition, literally l_g, is continuous as it is a composition of two continuous map. And its inverse is continuous by the same reason.

Each coset gU is open (resp. closed) because $l_{g^{-1}} : G \to G, x \mapsto g^{-1}x$ is continuous and gU is the per-image of U and so is open (resp. closed). □

Before we dig into the properties of topological groups, we see they have quite nice properties fitting one's intuitions quite well. For example, we have the following.

Proposition 11.26.4. *Let G be a topological group, and let H be a subgroup.*

1. *If H contains a nonempty open subset, then H is open.*
2. *If H is open, then H is also closed.*
3. *If H is closed and of finite index, then it is also open.*
4. *If we further require G to be compact, then H is open if and only if H is closed and of finite index.*
5. *H is also a topological group under subspace topology.*

Proof. The main idea of (2) (3) and (4) here is to note we get partition of G by the cosets of H.

1. Say U is open and contained in H, then $H = \cup_{h \in H} hU$ is open.

2. The group G is a disjoint union of (left) cosets of H, namely, $G = \sqcup_g gH$. Each coset gH is open by the lemma above. Since any union of open sets is open, $\sqcup_{g\neq e} gH$ is open and its compliment $H = G \setminus (\sqcup_{g\neq e} gH)$ is closed.

3. Any finite union of closed sets are closed. We repeat the proof as part (1). Since H is of finite index, the compliment of H is a finite union, and so $H$is open.

4. It remains to prove that if G is compact and H is open, then H is of finite index. Indeed, G is covered by the cosets of H, which are all open. By the compactness of G, it is covered by finitely many of them and so G is a finite disjoint union of cosets gH and H is of finite index.

5. H is closed under product and inverse and the statement is clear about H.

□

Indeed, the key topological feature of a topological group G is its *homogeneity*: the neighborhoods of the identity and the neighborhoods of every other element in G look the same. (This is visually clear when $G = \mathbb{R}^n$.) The reason is that left multiplication by each $g \in G$ is a continuous function $l_g : G \to G$ with a continuous inverse (namely left multiplication by g^{-1}), so l_g is a homeomorphism that sends the identity element to g. Right multiplication by g is also a homeomorphism of G taking e to g, which need not be the same as left multiplication by g when G is non-abelian. Homogeneity in a topological group often reduces arguments about neighborhoods of arbitrary points to neighborhoods of the identity. The reason is that U is a neighborhood of g if and only if $g^{-1}U$ is a neighborhood of the identity. (More generally, if $\{U_i\}$ is a fundamental system of neighborhoods of the identity in G then for each $g \in G$, $\{gU_i\}$ is a fundamental system of neighborhoods of g.)

Theorem 11.26.5. *Let H be a subgroup of a topological group G. Then its closure $\overline{H}$ is also a subgroup, and if H is normal, then so is $\overline{H}$.*

Proof. This could be proved with a direct use of the definition of closure: $g \in \overline{H}$ when every open subset of G that contains g intersects H. Instead we will give a proof using a property of closures and homogeneity:

- if a subset C is closed, then gC and Cg are closed for each $g \in G$,
- the closure $\overline{A}$ of a subset A is the smallest subset containing it: if $A \subset C$ and C is closed then $\overline{A} \subset C$.

To prove $\overline{H}$ is a subgroup we show that $\overline{H}\,\overline{H} \subset \overline{H}$ and $\overline{H}^{-1} = \overline{H}$.

Since H is a subgroup, $HH \subset H \subset \overline{H}$. Thus for each $h \in H$, $hH \subset \overline{H}$, so $H \subset h^{-1}\overline{H}$, which is closed since $\overline{H}$ is closed. And so $\overline{H} \subset h^{-1}\overline{H}$ for all $h \in H$ and then we have $H\overline{H} \subset \overline{H}$. And similarly, $\overline{H}H \subset \overline{H}$.

To get $\overline{H}\,\overline{H} \subset \overline{H}$, pick $y \in \overline{H}$ and so $Hy \subset \overline{H}$. Then $H \subset \overline{H}y^{-1}$, which is closed, and so $\overline{H} \subset \overline{H}y^{-1}$. Therefore, $\overline{H}y \subset \overline{H}$ for all $y \in \overline{H}$ and so $\overline{H}\,\overline{H} \subset \overline{H}$.

Now we consider the inverse function. We have $H \subset \overline{H}$ and then $H^{-1}\overline{H}^{-1}$ so $H \subset \overline{H}^{-1}$. Since the inverse function is a homeomorphism, $\overline{H}^{-1}$ is closed and so $\overline{H} \subset \overline{H}^{-1}$. Taking inversion once more, we get $\overline{H}^{-1} \subset \overline{H}$ and so $\overline{H}^{-1} = \overline{H}$.

Suppose that H is normal. To prove $\overline{H}$ is normal, we need to show that $g\overline{H}g^{-1} = \overline{H}$ for all $g \in G$. From basic group theory, it suffices to show$g\overline{H}g^{-1} \subset \overline{H}$ for all $g \in G$.

Since H is normal in G, $gHg^{-1} = H \subset \overline{H}$ and then $H \subset g^{-1}\overline{H}g$. But $g^{-1}\overline{H}g$ is closed and then $\overline{H} \subset g^{-1}\overline{H}g$. Thus $g\overline{H}g^{-1} \subset \overline{H}$. Since g is a arbitrary in G, $\overline{h}$ is normal. □

And due to homogeneity, some properties are only needed to be checked around the identity.

Theorem 11.26.6. *Let $f : G \to H$ be a homomorphism between two topological groups.*

1. *The map f is continuous if and only if f is continuous at $e_G \in G$: for each open set V around the identity in H, there is an open set U around the identity in G such that $f(U) \subset V$.*

2. *The map f is open if and only if f is open at the identity $e_G \in G$: for each open set U in G containing identity, $f(U)$ contains an open set around the identity in H.*

Proof. One direction is clear. We need to prove the reverse direction for both statements.

1. If f is continuous, then it is continuous at the identity of G. Conversely, suppose f is continuous at the identity in G. To prove f is continuous at each $g \in G$, pick an open set V in H around $f(g) \in H$. Then $f(g)^{-1}V$ is an open set around the identity in H, so by the continuity of f at the identity of G, there is an open set U around the identity of G such that $f(U) \subset f(g)^{-1}V$. Thus $f(gU) = f(g)f(U) \subset V$, so gU is the open set around g in G whose image lies inside V.

2. If f is open, then it is open at the identity in G. Conversely, suppose f is open at the identity in G. Pick a nonempty open set U in G and choose $g \in U$. Then $g^{-1}U$ is an open set containing the identity in G, so $f(g^{-1}U) = f(g)^{-1}f(U)$ contains an open set V around the identity in H. The set $f(g)V$ after left multiplication by $f(g)$ is then contained in $f(U)$ and $f(g) \in V$. Therefore, $f(U)$ is open.

□

Definition 11.26.7. A group homomorphism $f : G \to H$ between two topological groups is called an *isomorphism between topological groups* if it is a homeomorphism.

Example 11.26.8. The exponential function e^x is an isomorphism between the topological group $\mathbb{R}$ and $(0, \infty)$.

It's important to keep in mind the difference between an isomorphism of groups and an isomorphism of topological groups. For a function between topological groups to be an isomorphism it has to be an isomorphism both algebraically and topologically: a group isomorphism and a homeomorphism. While a bijective homomorphism between groups is a group isomorphism (that is, the inverse map is automatically a homomorphism), in topology a bijective continuous map need not be a homeomorphism: the inverse map might not be continuous. Equivalently, the original map might not be an open map.

Since a continuous bijection from a compact space to a Hausdorff space is closed, when we are dealing with compact Hausdorff topological groups, the subtlety above does not occur: a bijective continuous homomorphism $G \to H$ from a compact topological group to a Hausdorff topological group is a homeomorphism and thus is an isomorphism of topological groups.

Lemma 11.26.9. *If $\mu : X \to Y$ is a bijective continuous map with X compact and Y Hausdorff, then μ is a homeomorphism.*

Proof. It is easily seen that μ is a closed map. A bijective map is open if and only if it is closed. A bijective continuous map is a homeomorphism if and only if it is open. □

Theorem 11.26.10. *Let G be a topological group with identity e.*

1. *If $\mathcal{N}$ is a neighborhood of e, then we can find a symmetric open neighborhood U of e such that $UU^{-1} \subset \mathcal{N}$ and $U = U^{-1}$.*

2. *The topology on G is discrete if and only if $\{e\}$ is open.*

3. *The topology on G is Hausdorff if and only if $\{e\}$ is closed.*

Proof. One direction is clearly for both statements.

1. We want to show that for a neighbourhood $\mathcal{N}$ of e in G there is a "symmetric" neighbourhood U of e such that $U = U^{-1}$ and $UU \subset \mathcal{N}$. Since the multiplication $m : G \times G \to G$ is continuous, there are open sets U_1, U_2 around the identity such that $m(U_1 \times U_2) \subset \mathcal{N}$. Let $U' = U_1 \cap U_2$, which is also an open neighbourhood of e, so $m(U' \times U') \subset \mathcal{N}$. Set $U = U' \cap (U')^{-1}$ and $m(U \times U) = UU \subset U'U' \subset \mathcal{N}$.

2. Topology is discrete if and only if every singleton is open. If $\{e\}$ is open, then so is every $\{g\} = g\{e\}$.

3. If G is Hausdorff, then every singleton is closed, so in particular, $\{e\}$ is closed.

   Conversely, suppose $\{e\}$ is closed. Then so is every singleton $\{g\}$. To show that G is Hausdorff, it suffices to show that e and g can be separated by open sets for any $g \in G, g \neq e$ due to the homogeneity. Since $G \setminus \{g\}$ is an open neighbourhood of e, we can obtain an open set U containing e such that $U = U^{-1}$ and $UU \subset U \setminus \{g\}$ by part (1). Then we have $U \cap gU = \emptyset$ because if $u = gv$ for some $u, v \in U$, then $g = uv^{-1} \in UU^{-1} \subset G \setminus \{g\}$, which is a contradiction. Since $e \in U$ and $g \in gU$, U and gU separates e and g.

□

Corollary 11.26.11. *If $f : G \to H$ is a continuous group homomorphism of topological groups and H is Hausdorff, then $\ker(f)$ is a closed normal subgroup of G.*

Corollary 11.26.12. *Let G be a topological group and N a normal subgroup. The G/N with the quotient topology is discrete if and only if N is open and G/N is Hausdorff if and only if N is closed.*

Proof. The identify element in G/N is the coset H. Hence $\{H\}$ is open (resp. closed) if and only if H is open (resp. closed) from the definition of quotient map. □

Theorem 11.26.13. *In a Hausdorff topological group, every discrete subgroup is closed.*

Proof. Let H be a discrete subgroup of a Hausdorff topological group G. We show that $G \setminus H$ is open. More precisely, pick $g \notin H$, we want to find an open neighbourhood of g which is disjoint from H.

By the discreteness of H, there is an open set N of G such that $N \cap H = \{e\}$. Then there is a symmetric neighbourhood U of e such that $UU \subset N$.

Suppose gU meets H twice: $gu_1 = h_1$ and $gu_2 = h_2$. Then $h_1^{-1}h_2 = u_1^{-1}u_2 \in H \cap UU \subset H \cap N = \{e\}$ and so $h_1 = h_2$ and $u_1 = u_2$. Thus $gU \cap H$ has cardinality at most 1. If $gU \cap H = \emptyset$, then gU is the desired neighbourhood of g that is disjoint from H. If $gU \cap H \neq \emptyset$, then the intersection has size 1, say $gU \cap H = \{h\}$. Since G is Hausdorff and singletons are closed, then $gU \setminus \{h\}$ is the desired open neighbourhood of g. □

Remark. $\{1, 1/2, 1/3, \dots\}$ is discrete not closed in $\mathbb{R}$. It is not a subgroup so the theorem above does not apply.

It is true more generally that in a Hausdorff topological group every locally compact subgroup is closed.

Corollary 11.26.14. *If N is a discrete normal subgroup of a Hausdorff topological group G, then G/N is Hausdorff in the quotient topology.*

Theorem 11.26.15. *If G is a topological group and N is a normal subgroup then the quotient map $G \to G/N$ is an open map. If N is compact then $G \to G/N$ is also a closed map.*

Proof. Let U be open in G and $\pi : G \to G/N$ be the canonical quotient map. The image $\pi(U)$ is open, by definition, if $\pi^{-1}(\pi(U))$ is open. Note $\pi^{-1}(\pi(U)) = \cup_{n\in N} Un$ is open since it is union of open sets.

Now let N be compact and C be closed in G. Then $\pi^{-1}(\pi(C)) = \cap_{n\in N} Cn = CN$. We want to show CN is closed. Now let $g \notin CN$ then $C^{-1}g \cap N = \emptyset$. If we can find an open neighbourhood U of e such that $C^{-1}g \cap NU = \emptyset$, which just means $gU^{-1} \cap CN = \emptyset$, then gU^{-1} is an open neighbourhood of g disjoint from CN and so CN is closed. So our task is to find such a U. Note that $C^{-1}g$ is closed. Write $A = C^{-1}g$ be closed and $B = N$ be compact with $A \cap B = \emptyset$. Due to the closeness of A, for each $x_i \in B$ we can find an open neighbourhood V_i of e such that $x_iV_i \cap A = \emptyset$. Moreover, we can assume $V_i = V_i^{-1}$ and $V_iV_i = V_i$ by Theorem 11.26.10. Since B is covered by V_i, by the compactness of B, we can find $x_1V_1, \ldots, x_nV_n$ such that $B \subset \cup_{i=1}^n x_iV_i$. Let $V = \cap_{i=1}^n V_i$, then V is open and $V_iV = V_i$ since $V \subset V_i$ and $V_iV_i = V_i$. We then have $BV \subset (\cup_{i=1}^n x_iV_i)V = \cup_{i=1}^n x_iV_iV = \cup_{i=1}^n x_iV_i$ and hence BV is disjoint from C and we are done. □

Corollary 11.26.16. *With same assumption as the theorem above, G/N endowed with the quotient topology is a topological group.*

Proof. We take the short way by showing that $\tilde{m} : G/N \times G/N, (xN, yN) \mapsto xy^{-1}N$ is continuous. Let $U \subset G/N$ be a nonempty and open subset. By the definition of quotient map, $\pi^{-1}(U)$ is nonempty and open. Since U is nonempty, $uv^{-1}N \in U$ for some $u, v \in G$ and then $uv^{-1} \in \pi^{-1}(U)$. Hence we can find open neighbourhoods C, D of u and v respectively, such that $m(C \times D) \subset \pi^{-1}(U)$. Since π is an open map, $\pi(C) = CN$ and $\pi(D) = DN$ are open neighbourhoods of uN and vN such that $CN \tilde{\times} DN \subset U$. □

Theorem 11.26.17. *Let G be a Hausdorff topological group and H be a discrete subgroup. Let N be a normal subgroup of G contained in H. Then H/N is discrete in G/N.*

Proof. The quotient map is open. □

Theorem 11.26.18. *Let G be a Hausdorff topological group and N be a closed normal subgroup. Then G is compact if and only if N and G/N are compact.*

Proof. Since closed subspaces are continuous images of compact spaces are compact, if G is compact, then N and G/N is compact.

Conversely, assume N and G/N are compact. Since N is compact, the canonical projection $G \to G/N$ has compact fibers and by Theorem 11.26.15 the projection map is a closed map. A continuous function between topological spaces that is a closed map and has compact fibers is a proper map, which means its inverse images of compact sets are compact. □

11.27 Profinite Groups

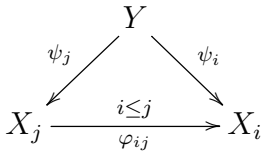
Definition 11.27.1. A *directed set* is a partially ordered set I such that for any $i, j \in I$ we can find $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 11.27.2. An *inverse system* (X_i, φ_{ij}) indexed by a directed set I consisting of a family X_i of topological spaces (resp. groups, R-modules and etc) and a family $\varphi_{ij} : X_j \to X_i$ of continuous maps (resp. homomorphisms, R-maps and etc) such that φ_{ii} is the identity map and whenever $i \leq j \leq k$ we have $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$

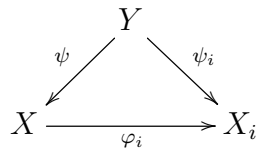
Sets for which no other topology is specified will be regarded with discrete topology.

Example 11.27.3. Let $I = \mathbb{N}$ with the usual order and let X_i be finite sets. Let $\phi_{i,i+1}$ be an arbitrary map for each i and define $\phi_{ii} = id_{X_i}$ and $\phi_{ij} = \phi_{i,i+1} \dots \phi_{j-1,j}$. Then (X_i, ϕ_{ij}) us an inverse system of finite sets.

Definition 11.27.4. Let (X_i, φ_{ij}) be an inverse system of topological spaces (resp. groups, R-modules and etc) and let Y be a topological space (resp. group, R-module and etc). A family $\psi_i : Y \to X_i$ of continuous maps (resp. homomorphisms, R-maps and etc) is *compatible* if $\varphi_{ij}\psi_j = \psi_i$ whenever $i \leq j$. In other words, the following diagram commutes whenever $i \leq j$.



An *inverse limit* (X, φ_i) of an inverse family (X_i, φ_{ij}) is a topological space (resp. groups, R-modules and etc) X together with a compatible family $\varphi_i : X \to X_i$ of continuous maps (resp. groups, R-modules and etc) with the following universal property: whenever $\psi : Y \to X_i$ is a compatible family of continuous maps resp. homomorphisms, R-maps and etc) from a topological space Y (resp. group, R-module and etc), there is a unique continuous map (resp. homomorphism, R-map and etc) $\psi : Y \to X$ such that $\varphi_i\psi = \psi_i$ for each i. In other words, the following diagram commutes.



The inverse limit is unique in the following sense.

Proposition 11.27.5. *Let (X_i, ϕ_{ij}) be an inverse system indexed by I.*

1. *If (X, ϕ_i) and (Y, ψ_i) are inverse limits of the inverse system, then there is an isomorphism $\pi : X \to Y$ such that $\psi_i = \pi\phi_i$ for each i.*
2. *Write $C = \prod_{i \in I} X_i$ and let π_i be the canonical project from C onto the i-th coordinate. Define*

$$X = \{c \in C : \phi_{ij}\pi_j(c) = \pi_i(c) \text{ for all } i, j \text{ with } j \geq i\}$$

and $\phi_i = \pi_i|_X$ for each i. Then (X, ϕ_i) is an inverse limit of (X_i, ϕ_{ij}).

3. *If (X_i, ϕ_{ij}) is an inverse system of topological groups, then X is a topological group and the maps ϕ_i are continuous homomorphisms.*

Proof. (1): The proof is similar to that of tensor product.

(2) and (3): We regard C with the product topology and X with the subspace topology. Then the map ϕ_i is certainly continuous and the definitions of (X, ϕ_i) ensures $\phi_{ij}\phi_j = \phi_i$ whenever $i \leq j$.

Now suppose (Y, ψ_i) is a compatible family. We want to show there is a unique map $\psi : Y \to X$ such that $\phi_i\psi = \psi_i$. Let $\tilde{\psi}$ be the map from Y to C taking y to $(\psi_i(y))$. Thus $\pi_i\tilde{\psi} = \psi_i$ and $\tilde{\psi}$ is continuous since the projection to each coordinate is continuous. If $i \leq j$, then

$$\pi_i\tilde{\psi} = \psi_i = \psi_{ij}\psi_j = \psi_{ij}\pi_j\tilde{\psi}_j$$

and it follows that $\tilde{\psi}$ maps Y to X. Now define $\psi : Y \to X$ by $\psi(y) = \tilde{\psi}(y)$. Thus ψ is continuous. It is a routine to check all the properties. □

With the existence and uniqueness of the inverse limit, it can be denoted as $\varprojlim(X_i, \phi_{ij})_{i\in I}$ or just $\varprojlim X_i$. It will sometimes be convenient to work with the particular inverse limit constructed above and we denote it by $s\varprojlim X_i$.

Proposition 11.27.6. *Let (X_i, ϕ_{ij}) be an inverse system indexed by I and write $X = \varprojlim X_i$.*

1. *If each X_i is Hausdorff, then so is X.*
2. *If each X_i is totally disconnected, then so is X.*
3. *If each X_i is Hausdorff and compact, then so is X.*
4. *If each X_i is Hausdorff, then X is closed in the product space $C = \prod_{i\in I} X_i$.*
5. *If each X_i is Hausdorff, compact and nonempty, then so is X.*

Proof. It suffices to prove these results for $s\varprojlim X_i$. (1), (2) and (3) follows from the fact the product space and the subspace inherit those properties.

(4): Note that if Y is Hausdorff, then the diagonal $\Delta \subset Y \times Y$ is closed. If $f, g : X \to Y$ are two continue maps then $\{x \in X : f(x) = g(x)\} = (f \times g)^{-1}(\Delta)$ is closed. Since

$$s\varprojlim X_i = \cap_{j>i}\{c \in C : \phi_{ij}\pi_j(c) = \pi_i(c)\}$$

where each X_i is Hausdorff and $\psi_i j$ and π_i, π_j are continuous, then $s\varprojlim X_i$ being an intersection of closed sets is closed.

(5): For $i < j$, the set $D_{ij} = \{c \in C : \phi_{ij}\pi_j(c) = \pi_i(c)\}$ is closed. Since C is compact, if $s\varprojlim X_i = \emptyset$, then $\cap_{r=1}^n D_{i_r j_r} = \emptyset$ for some integer n and elements $i_r, j_r \in I$, otherwise, it will violate the finite intersection property. Since I is directed, we can find $k \in I$ such that $j_r \leq k$ for all j_r. Choose $x_k \in X_k$, define $x_l = \phi_{lk}(x_k)$ for $l \leq k$, and define x_l arbitrarily for other l. Clearly, the element (x_i) is an element in $\cap_{r=1}^n D_{i_r j_r} = \emptyset$ and hence it cannot be empty. □

Proposition 11.27.7. *Let $X = \varprojlim X_i$ be an inverse limit of an inverse system (X_i, ϕ_{ij}) where each X_i is nonempty, compact and Hausdorff. Then we have*

1. *$\phi_i(X) = \cap_{i\leq j}\phi_{ij}(X_j)$.*
2. *The sets $\phi_i^{-1}(U)$ with $i \in I$ and U open in X_i form a basis fot the topology on X.*

3. *If $Y \subset X$ satisfies $\phi_i(Y) = X_i$ for each i, then Y is dense in X.*

4. *If $\theta : Y \to X$, then θ is continuous if and only if each $\phi_i\theta$ is continuous.*

5. *If $f : X \to A$ is a continuous map to a discrete space A, then f factors through X_i for some i in the sense that $g : X_i \to A$ with $f = g\phi_i$.*

Proof. Again, it suffices to prove the statement for $s\varprojlim X_i$ and $\phi_i = \pi_i|_X$.

1. We have $\phi_i(X) = \phi_{ij}\phi_j(X) \subset \phi_{ij}(X_j)$ for all $i \leq j$ and therefore $\phi_i(X) \subset \cap_{i\leq j}\phi_{ij}(X_j)$. Now let us fix i, fix $a \in \cap_{i\leq j}\phi_{ij}(X_j)$ and for $i \leq j$ set $Y_j = \{y \in X_j : \phi_{ij}(y) = a\}$. Thus Y_j being the inverse image of a closed set is closed in X_j and hence is compact. If $i \leq j \leq k$ and $y_k \in Y_k$, then $\phi_{ij}\phi_{jk}(y_k) = \phi_{ik}(y_k) = a$ and so $\phi_{jk}(y_k) \in Y_j$. Therefore, Y_j with $j \geq i$ is an inverse system of nonempty compact Hausdorff spaces and so there is an element $b \in s\varprojlim_{j\geq i} Y_j$. And we have $\phi_{jk}(b_k) = b_j$ for $i \leq j \leq k$ and $b_i = a$ for the coordinates of b. Now if $l \in I$ and $i \not\leq l$, then we can find $j \in I$ such that $i \leq j$ and $l \leq j$ and define $b_l = \phi_{lj}(b_j)$. b_l is well-defined in the sense that if there is another $j' \in I$ with $i \leq j'$ and $j \leq j'$, then we can find $k \in I$ such that $j, j' \leq k$ and then $b_l = \phi_{lk}(b_k) = \phi_{lj}\phi_{jk}(b_k) = \phi_{lj'}\phi_{j'k}(b_k)$. And hence we have find an element $b = (b_j)_{j\in I} \in s\varprojlim X_i$ with $\phi_i(b) = a$.

2. The basis of X can be pulled from C and is of the form

$$P = X \cap (\cap_{r=1}^{n}\pi_{i_r}^{-1}(U_r)) = X \cap (\prod_{i\neq i_1,\ldots,i_n} X_i \times U_1 \times \cdots \times U_n)$$

for some integer n and $i_1, \ldots, i_n \in I$ and U_r is open in X_{i_r}. The result will follow if we can prove that for all $a \in P$ there is a set $\phi_k^{-1}(U)$ with U open in X_k such that $a \in \phi_k^{-1}(U) \subset P$. Write $a = (a_i)$. Choose $k \in I$ such that $k \geq i_r$ for all i_r. The set $\phi_{i_rk}^{-1}(U_r)$ is open in X_k since ϕ_{i_rk} is continuous. Write $U = \cap_{r=1}^{n}\phi_{i_rk}^{-1}(U_r)$. This is an open neighbourhood of a_k in X_k and so $\phi_k^{-1}(U)$ is an open neighbourhood of a in X. Moreover, if $b = (b_i) \in \phi_k^{-1}(U)$ then $b_k \in U$ and so that $b_{i_r} = \phi_{i_rk}(b_k) \in U_r$. It follows that $\phi_k^{-1}(U) \subset P$.

3. For each $i \in I$ and each nonempty open set U in X_i we clearly have $\phi_i(Y) \cap U = X_i \cap U \neq \emptyset$ and hence $Y \cap \phi_i^{-1}(U) \neq \emptyset$. It follows from (2) that Y is dense in X.

4. If θ is continuous, then $\phi_i\theta$ is continuous. Conversely, if each $\phi_i\theta$ is continuous, then for each i and each open set U in X_i, the set $\theta^{-1}(\phi_i^{-1}(U)) = (\phi_i\theta)^{-1}(U)$ is open. It follows from (2) that θ is continuous.

5. The image $\mathrm{im}(f)$ is compact and discrete and so finite. For each $a \in \mathrm{im}(f)$ the set $Y_a = f^{-1}(a)$ is compact and open and so it is, by the compactness, a finite union of basis element $Y_a = \cup_{j\in J}\phi_j^{-1}(U_j)$ with J a finite subset of I and U_j open in X_j. Choose $k \in I$ such that $j \leq k$ for all $j \in J$. We have $\phi_j^{-1}(U_j) = \phi_k^{-1}(\phi_{jk}^{-1}(U_j))$ for each j and so for each $a \in \mathrm{im}(f)$ we can write $Y_a = \phi_k^{-1}(V_a)$ where V_a is open in X_k. Write $D = X_k \setminus (\cup_{a\in\mathrm{im}(f)}V_a)$. Then $D \cap \phi_k(X) = \emptyset$. By (1), we have $D \cap (\cap_{k\leq l}\phi_{kl}(X_l)) = \emptyset$. Since X_k is compact and D and each $\phi_{kl}(X_l)$ are closed, we can find $l_1, l_2, \ldots, l_s$ such that $D \cap \phi_{kl_1}(X_{l_1}) \cap \cdots \cap \phi_{kl_s}(X_{l_s}) = \emptyset$ by the finite intersection property. Choose $t \in I$ such that $t \geq l_i$ for each l_i. For $k \leq l \leq t$, we have $\phi_{kt}(X_t) = \phi_{kl}(\phi_{lt}(X_t)) \subset \phi_{kl}(X_l)$, and we can conclude that $D \cap \phi_{kt}(X_t) = \emptyset$ and $\phi_{kt}(X_t) \subset \cap_{a\in\mathrm{im}(f)}V_a$. Write $W_a = \phi_{kt}^{-1}(V_a)$ for each $a \in \mathrm{im}(f)$ then $W_{a_1} \cap W_{a_1}$ of $a_1 \neq a_2$. Let

$x \in X_t$. Then $\phi_{kt}(x) \in V_a$ for some a and then $x \in \phi_{kt}^{-1}(V_a) = W_a$. Therefore, $X_t = \cup_{a \in \mathrm{im}(f)} W_a$ and each set W_a is also closed. It follows that the map $g : X_i \to A$ which takes W_a to a for each $a \in \mathrm{im}(f)$ is continuous and $f = g\phi_t$ as required.

□

Proposition 11.27.8. *Let X be a compact Hausdorff totally disconnected space. Then X is the inverse limit of its discrete quotient spaces.*

Remark. As the quotient space of a compact space is also compact, discreteness implies finiteness.

Proof. Let I be the set of all partitions of X into finitely many clopen subsets. For each $i \in I$, let X_i be the corresponding quotient space (whose elements are clopen subsets of the partition i) and let $q_i : X \to X_i$ be the quotient map. Thus the sets X_i are precisely the quotient spaces of X which are discrete.

We write $i \leq j$ if and only if there is a map $q_{ij} : X_j \to X_i$ satisfying $q_{ij}q_j = q_i$. The map q_{ij} is then uniquely determined because q_j is surjective. Clearly, I is a partially ordered set by inclusion. It is also directed: if

$$i = \{U_r : 1 \leq r \leq m\}, \quad j = \{V_s : 1 \leq s \leq n\}$$

are elements of I, then

$$k = \{U_r \cap V_s : 1 \leq r \leq m, 1 \leq s \leq n\}$$

is an element in I and $i, j \leq k$. It follows that (X_i, q_{ij}) is an inverse system and that (X, q_i) is a compatible family. Let $Y = \varprojlim X_i$ and ϕ_i be the canonical map. The universal property of inverse limit gives us a continuous map $\mu : X \to Y$ such that $\phi_i\mu = q_i$. If $x_1, x_2 \in X$ such that $\mu(x_1) = \mu(x_2)$, then $q_i(x_1) = q_i(x_2)$ for each i, so that no clopen set contains just one of x_1, x_2 and since X is totally disconnected, we must have $x_1 = x_2$. Therefore, μ is injective. Since $\phi_i(\mu(X)) = q_i(X) = X_i$, it follows from Proposition 11.27.6 above that $\mu(X)$ is dense in Y. Since μ is continuous and X is compact and Y is Hausdorff, $\mu(X)$ is also closed and $\mu(X) = Y$ and μ is surjective. Since μ is a bijective continuous map with X compact and Y Hausdorff, μ is a homeomorphism by Lemma 11.26.9. □

Let $\mathcal{C}$ be a class of finite groups. We can a group F a $\mathcal{C}$-group if $F \in \mathcal{C}$ and we call G a pro-$\mathcal{C}$ group if it an inverse limit of $\mathcal{C}$ groups. We say $\mathcal{C}$ is *closed* for subgroups (resp. quotients, direct product and etc) if every subgroup (resp. quotient, direct product and etc) of a $\mathcal{C}$-group is a $\mathcal{C}$-group. Some importance classes are the class of all finite groups, the class of finite p-groups and the class of all finite cyclic groups. Similarly, we have the profinite (topological) spaces. We are now able to "classify" profinite spaces and profinite groups.

Lemma 11.27.9. *Let X be a compact Hausdorff space and $x \in X$ a point. Then the connected component of x is the intersection of all clopen sets containing x.*

Proof. Let $U = \cap_{i \in I} U_i$ where each U_i is a clopen set containing x. Write C the connected component containing x. Then $C \subset U_i$ as otherwise C cannot be connected, and therefore $C \subset U$. If we can prove that U is connected, we will have $C = U$ as by definition the connected component of a point is the maximal connected set containing that point. Assume $U = V \cup W$, where V and W are disjoint closed sets. We will show either V or W is empty. As X is compact and Hausdorff, it is T_4 and normal. Therefore, we can find disjoint open subsets V' and W' containing V and W respectively. Since $C \subset U$, we must have $(X \setminus (V' \cup W')) \cap (\cap_{i \in I} U_i) = \emptyset$, which is to say $(V' \cup W') \cup (\cup_{i \in I} X \setminus U_i) = X$. By the compactness of X, there is finite index set $I' \subset I$ such that $(V' \cup W') \cup (\cup_{i \in I'} X \setminus U_i) = X$, which is to

say $(X \setminus (V' \cup W')) \cap (\cap_{i \in I'} U_i) = \emptyset$. Let $A = \cap_{i \in I'} U_i$ and note that A is then a clopen neighbourhood of x since the index set I' is finite. Thus $x \in (A \cap V') \cup (A \cap W') = A$. Say, without loss of generality, $x \in A \cap V'$. We know that $A \cap V'$ is open, and it is also closed as $A \cap V' = (X \setminus A \cap W') \cap A$. Therefore $U \subset A \cap V' \subset V'$. Then $U \cap W \subset U \cap W' = \emptyset$ and thus $W = \emptyset$. Therefore we conclude U is connected and that $C = U$. □

Definition 11.27.10. A space X is *zero-dimensional* if each point $x \in X$ has a neighbourhood system consisting of clopen sets. Equivalently, X is 0-dimensional if and only if for each point $x \in X$ and a closed set A not containing x, there is a clopen set containing x and not intersecting A.

Theorem 11.27.11. *Let X be a topological space. Then the following conditions are equivalent:*

1. *X is a profinite space;*
2. *X is compact, Hausdorff and totally disconnected;*
3. *X is compact, Hausdorff and zero-dimensional.*

Proof. The equivalence of (1) and (2) are shown in Proposition 11.27.6 and Proposition 11.27.8.

(2) $\implies$ (3): We want to show for any open set $U \subset X$, there is a clopen set C such that $x \in C \subset U$ for all $x \in U$. Now let U be an arbitrary nonempty open set and $x \in U$. Let $C = \cap_{t \in T} C_t$ be the intersection of all clopen neighbourhoods of x. By Lemma 11.27.9, it follows that $C = \{x\}$ since X is totally disconnected. As $X \setminus U$ is closed and disjoint from C, it follows by the compactness of X that there exists finite subset $T' \subset T$ such that $(X \setminus U) \cap (\cap_{t \in T'} C_t) = \emptyset$ by the finite intersection properties and $(X \setminus U) \cap C = \emptyset$. Thus $\cap_{t \in T'} C_t$ is a clopen set containing x also contained in U.

(3) $\implies$ (2): A zero-dimensional Hausdorff space is clearly totally disconnected from the definitions directly. □

Let G be a topological group. For the rest of this section, we write $H \leq G$ to mean H is a closed subgroup of G and $N \ll G$ to mean N is an open normal subgroup of G. We call a family of normal subgroups of G a *filter base* if for all $K_1, K_2 \in I$ there is a subgroup $K_3 \in I$ such that $K_3 \subset K_1 \cap K_2$.

We have two technical results.

Proposition 11.27.12. *Let (G, ϕ_i) be an inverse limit of an inverse system (G_i, ϕ_{ij}) of compact Hausdorff topological groups and let $L \ll G$. Then $\ker(\phi_i) \leq L$ for some i. Consequently, G/L is isomorphic to a quotient group of a subgroup of some G_i and if in addition each map ϕ_i is surjective then G/L is isomorphic to a quotient of some G_i.*

Proof. Since L is open and contains 1, we have $\phi_i^{-1}(U) \subset L$ for some i and some open subset U of G_i containing 1 by Proposition 11.27.7 as $\phi_i^{-1}(U)$ form a basis. Therefore, $\ker(\phi_i) \leq L$ for that i and we have $G/L \cong (G/\ker(\phi_i))/(L/\ker(\phi_i))$ and so since $G/\ker(\phi_i) \cong \text{im}(\phi_i)$, it follows that G/L is isomorphic to a quotient group of some G_i. □

Proposition 11.27.13. *Let G be a topological group and I be a filter base of closed normal subgroups. For $K, L \in I$, define $K \leq L$ if and only if $L \subset K$. Thus I is a directed with respect to $\leq$ and define $q_{KL} : G/L \to G/K$ for $K \leq L$. This makes G/K into an inverse system. Let $\tilde{G} = \varprojlim G/K$. There is a continuous homomorphism $\theta : G \to \tilde{G}$ with kernel $\cap_{K \in I} K$. If G is compact, then θ is surjective; if G is compact and $\cap_{K \in I} K = \{1\}$, then θ is an isomorphism of topological groups.*

Proof. The proof of Proposition 11.27.7 implies $(G/K, q_{LK})$ is an inverse system directed by I. We take $\tilde{G} = s\varprojlim G/K$. It is easy to see that the image of $\tilde{\theta} : G \to \prod_{K\in I} G/K, g \to (gK)_{K\in I}$ lies in $\tilde{G}$. Define θ to be the induce map $\theta : G \to \tilde{G}, g \mapsto \tilde{\theta}(g)$. Since the product of $\tilde{\theta}$ with the projection maps are quotient maps and so continuous, it follows that $\tilde{\theta}$ and θ are continuous. Note $g \in \ker(\theta)$ if and only if $gK = K$ for each K and so $\ker(\theta) = \cap_{K\in I} K$. For each $K \in I$, we have $\phi_K(\theta(G)) = G/K$ and so by Proposition 11.27.7, $\mathrm{im}(\theta)$ is dense in $\tilde{G}$.

By Corollary 11.26.12, each group G/K is Hausdorff. Now suppose G is compact. Then $\theta(G)$ is compact hence closed as $\tilde{G}$ is Hausdorff by Proposition 11.27.6. Since $\theta(G)$ is also dense, $\theta(G) = \tilde{G}$. If in addition $\cap_{K\in I} K = \{1\}$, then θ is a continuous bijection. Since G is compact and $\tilde{G}$ is Hausdorff, θ is a homeomorphism by Lemma 11.26.9. □

Lemma 11.27.14. *Let $G = \varprojlim G_i$ be a profinite group, and let $\phi_i : G \to G_i$ be the canonical projection. Then $\mathcal{S} = \{\ker(\phi_i) | \phi_i : G \to G_i\}$ forms a fundamental system of neighbourhoods of the identity in G.*

Proof. Form Proposition 11.27.7 (2) we know that G has a basis of the form

$$\{\phi_i^{-1}(U) : U \text{ open in } G_i \text{ for some } i\}.$$

But G_i are finite sets with discrete topology and so say $U = \{g_1, \dots, g_n\}$ then $\phi_i^{-1}(U)$ is just a union of translations of $\ker(\phi_i)$, which are all open. So it is sufficient to say $\mathcal{S}$ is a basis.

If you are not happy, here is a more detail copy-and-paste. Let $\mathcal{C}$ be the collection of elements of the form

$$(\prod_{i\neq i_0,\dots,i_n} G_i) \times \{1\}_{i_0} \times \cdots \times \{1\}_{i_n}$$

where $i_0, \dots, i_n \in I$ are arbitrary and $i_0 \geq i_1, \dots, i_n$. We will now prove that this is a fundamental system of neighbourhoods around 1 in $X = \prod_{i\in I} G_i$. Let $V \subset X$ be an open neighbourhood of 1. Then V contains an open set of the form $(\prod_{i\neq j_1,\dots,j_n} G_i) \times U_{j_1} \times \cdots \times U_{j_n}$. Now let $U = (\prod_{i\neq j_0,\dots,j_n} G_i) \times \{1\}_{j_0} \times \cdots \times \{1\}_{j_n}$ with $j_0 \geq j_1, \dots, j_n$. Then $U \subset V$ and $U \in \mathcal{C}$. Thus $\mathcal{C}$ is a fundamental system of open neighbourhoods of 1. Now we let $\mathcal{D} = \{G \cap C : C \in \mathcal{C}\}$. Then $\mathcal{D}$ is a fundamental system of neighbourhoods around 1 of G with the subspace topology. We further note that elements in $\mathcal{D}$ has the form

$$G \cap (\prod_{i\neq i_0} G_i \times \{1\}_{i_0})$$

as

$$G \cap ((\prod_{i\neq i_0,\dots,i_n} G_i) \times \{1\}_{i_0} \times \cdots \times \{1\}_{i_n}) = G \cap (\prod_{i\neq i_0} G_i \times \{1\}_{i_0}) = \ker(\phi_i).$$

□

Lemma 11.27.15. *Let G be a compact topological group and H be a open subgroup. Then the normal core of H, defined as $\mathrm{core}(H) = \cap_{g\in G} gHg^{-1}$, is an open subgroup.*

Proof. By Proposition 11.26.4, H is also closed and of finite index. The number of conjugacy class of H is $[G : N(H)]$, where $N(H) \supset H$ is the normalizer of H, hence is finite. Hence $\mathrm{core}(H)$ is a finite intersection of open sets and hence open. □

Theorem 11.27.16. *Let G be a topological group. Then the followings are equivalent:*

1. *G is a profinite group.*

2. *G is compact, Hausdorff and totally disconnected.*

3. *G is compact, Hausdorff and the identity element 1 admits a fundamental system $\mathcal{S}$ of open subgroups U satisfying $\cap_{U\in\mathcal{S}} = \{1\}$ and $U \lll G$ with G/U finite.*

4. *The identity element 1 of G admits a fundamental system $\mathcal{S}$ of open subgroups U satisfying $\cap_{U\in\mathcal{S}} = \{1\}$ and $U \lll G$ with G/U finite, and $G = \varprojlim_{U\in\mathcal{S}} G/U$.*

Remark. You can extend this theorem to pro-$\mathcal{C}$ groups where $\mathcal{C}$ shall be assumed to be closed under subgroups and direct products (and quotients if needed).

Proof. $(1) \implies (2)$ follows directly from Theorem 11.27.11.

$(2) \implies (3)$: By Theorem 11.27.11 we know that G admits a basis $\mathcal{C}$ consisting of clopen sets. Therefore, we have a fundamental system of clopen sets around each point and especially 1. Denote the fundamental system of 1 by $\mathcal{V}$. By Lemma 11.27.9, as G is totally disconnected, $\cap_{V\in\mathcal{V}} V = \{1\}$. If we can show that each $V \in \mathcal{V}$ contains a open normal subgroups $N \lll G$, then the collection of all these open normal subgroups will form the desired fundamental system. Let $V \in \mathcal{V}$ be arbitrary. Now for each $x \in V$, we can find open neighbourhood U_x of x such that $U_x \subset V$ as V is open and a symmetric open neighbourhood V_x such that $V_x \subset U_x, V_x = V_x^{-1}$ and that $V_xV_x \subset U_x$. Since V is compact and covered by V_x, we can find $x_1, \dots, x_n$ such that $V = \cup_{i=1}^n V_{x_i} = \cup_{i=1}^n U_{x_i}$. Let $S_{x_i} = x_i^{-1}V_{x_i}$ be a open neighbourhood of 1. Write $S = \cap_{i=1}^n S_{x_i}$ and $W = S \cap S^{-1}$. Then W is a symetric open neighbourhood of 1. Then we have

$$VW \subset VS = (\cup_{i=1}^n V_{x_i})(\cap_{i=1}^n S_{x_i}) \subset \cup_{i=1}^n V_{x_i}V_{x_i} \subset \cup_{i=1}^n U_{x_i} = V$$

and the reverse inclusion is also true since $1 \in W$. In short, we have $VW = V$ and inducttively $VW^n = V$ for all positive integer n. Since V contains 1, we have $W^n \subset V$ and hence $R = \cup_{n\in\mathbb{N}} W^n \subset V$ is an open subgroup since W is open and symmetric. By the lemma above, the normal core $\mathrm{core}(R)$ is an open normal subgroup of finite index and is contained in V. Clearly, $G/\mathrm{core}(R)$ is finite.

$(3) \implies (4)$: This is Proposition 11.27.13 by noting that the fundamental system derscribed in (3) is a filter base.

$(4) \implies (1)$: This is just the definition of profinite group. □

Week 12

12.28 Infinite Galois Extensions

Recall that we have defined normal and Galois extensions for finite field extensions. We now extend to a possibly infinite ones.

Definition 12.28.1. An algebraic extension L/K is called *normal* if it satisfies one of the following conditions:

1. L is a splitting field of a family of polynomials in $K[x]$;
2. Every irreducible polynomial in $K[x]$ that admits a root in L splits completely over L into linear factors;
3. Every K-map $L \to \overline{L}$, where $\overline{L} = \overline{K}$ is the algebraic closure, is an automorphism of L in the sense that the image is also L.

Definition 12.28.2. An algebraic extension L/K is called *Galois* if it is normal and separable. Then $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ is called the *Galois group* of the extension L/K.

Note that it is equivalent to say that for each irreducible polynomial $f \in K[x]$ either has no root in L or has $\deg(f)$ distinct roots in L.

Recall we have the fundamental theorem of Galois theory when it is a finite extension.

Theorem 12.28.3 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite extension with Galois group $G = Gal(L/K)$. Then the maps*

$$\begin{aligned} \{\textit{subgroups of } G\} &\underset{\Phi}{\overset{\Psi}{\rightleftharpoons}} \{\textit{intermediate fields of } L/K\} \\ H &\longmapsto L^H, \\ Gal(L/E) &\longleftarrow\!\shortmid E, \end{aligned}$$

that assign to a subgroup $H \subset G$ the fixed filed L^H, resp. to an intermediate field E of L/K the Galois group of the Galois extension L/E, are bijective, inclusion reversing and mutually inverse.

The fixed field L^H is normal and therefore Galois over K if and only if H is a normal subgroup of G. If this is the case, the surjective group homomorphism

$$G \to Gal(L^H/K), \sigma \mapsto \sigma|_{L^H},$$

admits H as its kernel and hence induces an isomorphism $G/H \cong Gal(L^H/K)$.

Surely, we want to generalize this theorem to infinite Galois extensions and follow Bosch's book.