LECTURE 1

YIHANG ZHU

1. Review of Galois Theory and separability

Let K be a field. An irreducible non-constant polynomial $f(X) \in K[X]$ is called *separable* if all of its roots in an algebraic closure of K are distinct. Equivalently, $f'(X) \neq 0$ as a polynomial. We see that $f'(X) = 0$ only when the characteristic of K is positive, say p, and $f(X)$ is of the form

$$\sum a_n X^{pn}.$$

Definition 1.1. Let L/K be an algebraic extension. An element $\alpha \in L - K$ is called *separable* if its minimal polynomial is separable. The extension L/K is said to be *separable* if any $\alpha \in L - K$ is separable.

Example 1.2. Consider the field $\mathbb{F}_p(t)$ where t is an indeterminate. It has a finite extension $\mathbb{F}_p[\sqrt[p]{t}] := \mathbb{F}_p(t)[\alpha]/(\alpha^p - t)$. This extension is inseparable since the minimal polynomial of $\alpha = \sqrt[p]{t}$ is $X^p - t = (X - \alpha)^p$ is irreducible over $\mathbb{F}_p(t)$ (exercise).

In a sense this example is the only possibility for a field extension to be inseparable. To be more precise, we call a field K *perfect* if any algebraic extension of K is separable. We have

Proposition 1.3. *If* $\operatorname{char} K = 0$*, then* K *is perfect. If* $\operatorname{char} K = p > 0$*, then* K *is perfect if and only if* $K^p = K$*.*

Proof. It follows from the following observation: Any polynomial $f(X)$ over K is of the form $g(X^{p^n})$ for some $n \geq 0$ and g a separable polynomial over K. □

Example 1.4. Any finite field is perfect.

In classical number theory, the fields we consider are usually either of characteristic zero or finite fields, so the issue of separability will not occur. However, as we will see in the later stage of the course, it is important to study fields like $\mathbb{F}_p(t)$ which are not perfect. They occur as the field of rational functions on an algebraic curve over a finite field.

Recall the following definition.

Definition 1.5. Let L/K be an algebraic extension. It is called *normal* if for any $\alpha \in L - K$, the minimal polynomial of α splits in L. It is called *Galois* if K is equal to the fixed field of $\operatorname{Aut}(L/K)$. In this case, we denote $\operatorname{Gal}(L/K) = \operatorname{Aut}(L/K)$.

Recall: The splitting field of any polynomial over K is normal over K. A finite extension L/K is Galois if and only if $[L : K] = |\operatorname{Gal}(L/K)|$. (In general $\geq$).

Proposition 1.6. *Let* L/K *be an algebraic extension. TFAE*

(1) It is Galois.
(2) It is normal and separable.
(3) L is the splitting field of a set of separable polynomials over K.

Theorem 1.7 (Main Theorem of Galois Theory)**.** *Let L/K be a finite (resp. algebraic) extension. The maps $H \mapsto L^H$, $F \mapsto \mathrm{Gal}(L/F)$ give an inclusion reversing bijection between (resp. closed) subgroups of $H \subset \mathrm{Gal}(L/K)$ and sub-extensions F/K. Moreover, F/K is Galois if and only if $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/K)$, in which case we have $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.*

We can understand the structure of an inseparable extension L/K quite well. We can always find a sub-extension S/K which is separable, such that L/S is purely inseparable.

Definition 1.8. Let L/K be an algebraic extension. An element $\alpha \in L - K$ is called *purely inseparable* if its minimal polynomial has only one distinct root, i.e. of the form $(X-\alpha)^n$. The extension L/K is said to be *purely inseparable* if any $\alpha \in L - K$ is purely inseparable.

Lemma 1.9. *Let K be a field of characteristic $p > 0$. If α is an algebraic element over K, then α is purely inseparable if and only if $\alpha^{p^n} \in K$ for some $n \geq 0$. When this happens the minimal polynomial of α is $(X-\alpha)^{p^n}$ for the smallest n. Let L/K be a purely inseparable extension. Then L/K is normal and $\mathrm{Gal}(L/K) = 1$. When L/K is finite its degree is a p power.*

Proposition 1.10. *Let L/K be an algebraic extension. Define*

$$S = \{\alpha \in L \text{ separable } /K\}$$

$$I = \{\alpha \in L \text{ purely inseparable } /K\}.$$

Then S and I are fields, calleds the separable/ purely inseparable closures of K in L. The extension S/K is separable, and L/S, I/K are purely inseparable.

When L/K is finite, let S be the separable closure of K in S. We define the separable degree to be $[L : K]_s := [S : K]$ and the inseparable degree to be $[L : K]_i := [L : S]$. Thus $[L : K]_s[L : K]_i = [L : K]$ and $[L : K]_i$ is a p power.

Corollary 1.11. *If L/K is a finite extension whose degree is prime to $p = \mathrm{char}\, K$, then it is separable.*

These concepts will be useful when we study algebraic curves over characteristic p fields.

2. Review of finite fields

Recall that if a field $\mathbb{F}$ is finite, then $|\mathbb{F}| = p^f$ for some $f \geq 1$ where $p = \mathrm{char}\, \mathbb{F}$. For any p power q, there is essentially only one finite field of q elements, denoted by $\mathbb{F}_q$, which is the splitting field of $X^q - X$ over $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Any finite extension of $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^n}/\mathbb{F}_q$. It is normal, hence Galois, and

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z},$$

where a generator is given by the q-Frobenius

$$\mathrm{Frob}_q = \mathrm{Frob}_p^f : \alpha \mapsto \alpha^q.$$

In a slightly fancier language, the absolute Galois group of $\mathbb{F}_q$ is isomorphic to the profinite completion of $\mathbb{Z}$, where a topological generator is given by Frob_q.

When we study number theory problems, usually the first attack is to try to solve the problem modulo p. This is how finite fields arise. We have seen that the absolute Galois group of a finite field is very easy to understand. When we try to understand $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, in some sense we would like to understand it in terms of the Frobenii Frob_p for all the prime numbers p. This point will be made clearer when we talk about class field theory. Anyhow there is a deep and miraculous relation between the Frob_p for different p's, called the Artin reciprocity law, which makes number theory more beautiful than general abstract algebra. An incarnation of the Artin reciprocity is the famous quadratic reciprocity. We briefly recall it.

Recall that $\mathbb{F}_p^\times$ (resp. $\mathbb{F}_q^\times$)is a cyclic group of order $p-1$ (resp. $q-1$). For $a \in \mathbb{F}_p$, define

$$(\frac{a}{p}) = \begin{cases} 0, & a = 0 \\ 1, & a \in (\mathbb{F}_p^\times)^2 \\ -1, & \text{otherwise.} \end{cases}$$

The map $a \mapsto (\frac{a}{p}) = a^{\frac{p-1}{2}}$ is a group homomorphism $\mathbb{F}_p^\times \to \{\pm 1\}$.

Theorem 2.1. *Let p, l be odd primes. Then $(\frac{p}{l}) = (-1)^{\frac{(p-1)(l-1)}{2}}(\frac{l}{p})$. Moreover $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}, (\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.*

As Professor Kato once put it, $(\frac{l}{p})$ is about the girl in the boy's eyes, and $(\frac{p}{l})$ is about the boy in the girl's eyes, and in real life they are not related to each other, while in number theory they are!

Proof. The assertion for $(\frac{-1}{p})$ is trivial. The case $(\frac{2}{p})$ is left as an exercise. We prove the assertion for l, p odd. Let $p^* := (-1)^{\frac{p-1}{2}}p$. Then

$$(\frac{p^*}{l}) = (\frac{-1}{l})^{\frac{p-1}{2}}(\frac{p}{l}) = (-1)^{\frac{(p-1)(l-1)}{2}}(\frac{l}{p}).$$

We need to prove

$$(\frac{l}{p}) = (\frac{p^*}{l}).$$

Observe $(\frac{p^*}{l}) = 1$ if and only if $\sqrt{p^*} \in \mathbb{F}_l$. We try to construct $\sqrt{p^*} \in \bar{\mathbb{F}}_l$ using the Gauss sum. Let $\zeta \in \bar{\mathbb{F}}_l$ be a primitive p-th root of unity. It is well known that a candidate for $\sqrt{p^*}$ is

$$\psi := \sum_{n=0}^{p-1} (\frac{n}{p})\zeta^n.$$

In fact, we compute

$$\psi^2 = \sum_{n,k=0}^{p-1} (\frac{nk}{p})\zeta^{n+k} = \sum_{n,k=0}^{p-1} (\frac{(n-k)k}{p})\zeta^n = \sum_{n=0}^{p-1}\sum_{k=1}^{n-1} (\frac{n/k-1}{p})\zeta^n.$$

For each n, we have

$$\sum_{k=1}^{p-1} (\frac{n/k-1}{p}) = \begin{cases} \sum_{k=0}^{p-2}(\frac{k}{p}) = -(\frac{p-1}{p}) = (-1)^{\frac{p-1}{2}+1}, & n \neq 0 \\ \sum_{k=1}^{p-1}(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}(p-1), & n = 0 \end{cases}.$$

So

$$\psi^2 = (-1)^{\frac{p-1}{2}}(p-1-\sum_{n=1}^{p-1}\zeta^n) = p^*.$$

Next, $\psi \in \mathbb{F}_l$ if and only if it is fixed by the Frobenius, i.e.

$$\psi^l = \psi.$$

We compute

$$\psi^l = \sum_{n=0}^{p-1}(\frac{n}{p})\zeta^{nl} = \sum_{n=0}^{p-1}(\frac{nl^{-1}}{p})\zeta^n = (\frac{l}{p})\psi.$$

Hence

$$(\frac{l}{p}) = 1 \Leftrightarrow \psi \in \mathbb{F}_l \Leftrightarrow (\frac{p^*}{l}) = 1.$$

□

Exercise 2.2. For p an odd prime, let $\zeta \in \bar{\mathbb{F}}_p$ be a primitive 8-th root of unity. Show that $\zeta + \zeta^{-1}$ represents $\sqrt{2}$. Use this to prove $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Remark 2.3. The above calculation actually shows that for any field K whose characteristic is not p, we have $K(\sqrt{p^*}) \subset K(\zeta_p)$, where $p^* = (-1)^{\frac{p-1}{2}}p$.

3. Sum of two squares

Quadratic fields arise when studying quadratic Diophantine equations.

Question 3.1. *Let p be a prime. When is p of the form x^2+y^2 with $x, y \in \mathbb{Z}$?*

If $p = 2$ the answer is yes. If $p \equiv 3 \mod 4$, then no. We need to prove $p \equiv 1 \mod 4 \Rightarrow p = x^2 + y^2$. The equation can be rewritten as

$$p = (x+iy)(x-iy), i = \sqrt{-1}.$$

The idea is that finding a solution $(x, y) \in \mathbb{Z}^2$ is the same as finding a number $z = x + iy \in \mathbb{Z}[i]$ such that $p = z\bar{z}$. We use the following basic fact.

Fact 3.2. *The ring of Gaussian integers $\mathbb{Z}[i]$ is a UFD.*

We go on to determine the units and prime elements of $\mathbb{Z}[i]$. Define the norm map

$$N : \mathbb{Z}[i] \to \mathbb{Z}, z \mapsto z\bar{z}.$$

It is multiplicative and $Nz = N\bar{z}$. An element $u \in \mathbb{Z}[i]$ is a unit if and only if $Nu = 1$, so the group of units is $\{\pm 1, \pm i\}$. We factorize an odd rational prime p inside $\mathbb{Z}[i]$:

$$p = \prod \mathfrak{p}_i^{e_i}.$$

Then $p^2 = Np = \prod N(\mathfrak{p}_i)^{e_i}$ Which shows the factorization can only be one of the two forms

$$p = \mathfrak{p} \text{ or } p = \mathfrak{p}\bar{\mathfrak{p}}.$$