ZAHLENTHEORIE SS 2019 - NOTE 2

Last time we saw that a problem over $\mathbb{Z}$ can be solved by working in a finite extension, such as $\mathbb{Z}[i]$. In particular, the factorization properties of $\mathbb{Z}[i]$ were especially useful and to get a hold on these we used tools such as the norm.

A central theme of the course will be the generalization of this study to other extension of $\mathbb{Z}$.

However, before considering extension of rings, we start with something easier: extension of fields. This is the subject of GALOIS THEORY, that we recall now.

1. BASICS of GALOIS THEORY

Consider an extension of fields $K \subseteq F$ (we will also write K/F).

def: ALGEBRAIC ELEMENT
An $\alpha \in F$ is called algebraic over K if it is the root of a (non trivial) polynomial over K.

Formally: $\exists\ f(x) \in K[X], f \neq 0$ s.t.
$$f(\alpha) = 0$$
The field extension is called algebraic if all elements of F are algebraic.

Examples: (1) $\sqrt{2}$ in $\mathbb{C}$ is algebraic over $\mathbb{Q}$.
(2) π is not algebraic over $\mathbb{Q}$ (HARD! LINDEMANN 1882).

def: FINITE EXTENSIONS
A field extension F/K is called finite if F has finite dimension as a K-vector space.
In this case the dimension is called the degree of the extension and it is denoted by $[F:K]$.

Every finite ext is algebraic.
If $K \subseteq F$ is a field extension and $\alpha \in F$, we denote by $K(\alpha)$ the extension of K generated by α.

Suppose that α is algebraic: then consider the homomorphism
$$ev_\alpha : K[X] \longrightarrow F$$
$$f(x) \longmapsto f(\alpha)$$
Since α is algebraic, the kernel is a nonzero prime ideal. $K[X]$ is a PID, it is generated by an irreducible

monic polynomial

$$\ker ev_\alpha = (m_\alpha(x))$$

$m_\alpha(x)$ is called the MINIMAL POLYNOMIAL of α over K. We get an isomorphism

$$K[x]/(m_\alpha(x)) \cong K[\alpha] \subseteq F$$

However, since $K[x]$ is a PID, we know that $m_\alpha(x)$ is maximal, hence $K[\alpha]$ is a field so that

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

Moreover, if $m_\alpha(x)$ has degree n, then $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a basis of $K(\alpha)$ over K, hence

$$[K(\alpha) : K] = \deg m_\alpha(x)$$

As usual in algebra it is important to consider isomorphisms and isomorphic object: for example consider a field extension $K \subseteq K(\alpha)$, how many other extensions of K are there that are isomorphic to $K(\alpha)$? We need to look at the embeddings

$$\sigma : K(\alpha) \hookrightarrow \overline{K}$$

which leave K fixed: recall that $K(\alpha) \cong K[x]/m_\alpha(x)$ so a map

$$\sigma : K[x]/ \longrightarrow \overline{K}$$

$/(m_\alpha(x))$

that is the identity on K, is the same thing as the choice of a root of $m_\alpha(x)$ inside $\overline{K}$

$\sigma : K(\alpha) \to \overline{K}$ $\quad \alpha \longmapsto \beta$ where β is a root of $m_\alpha(x)$

For example, when $m_\alpha(x)$ has all distinct roots we can count them easily: their number is precisely the degree of $m_\alpha(x)$.

This discussion introduces the notion of

Def: SEPARABLE EXTENSION

An algebraic extension $K \subseteq F$ is called separable if for every $\alpha \in F$ the minimal polynomial $m_\alpha(x)$ has distinct roots in K.

Rmk: (1) If $\mathrm{char}(K) = 0$, every extension is separable

(2) If K is a finite field, every extension is separable

(3) Let $K = \mathbb{F}_p(t)$ and let α be a root of the polynomial $x^p - t$.

We consider $K(\alpha)$: since $x^p - t$ is irreducible, this is the minimal polynomial of α.

However, in $K(\alpha)[X]$, we can write

$$X^p - t = X^p - \alpha^p = (X-\alpha)^p$$

From now on, we will consider only separable extensions, especially because we will consider char 0 mostly.

Thm: PRIMITIVE ELEMENT THEOREM

Let $K \subseteq F$ be a finite and separable extension

Then F is principal: $F = K(\alpha)$ for a certain α.

Example: (1) Let's look at two extensions of $\mathbb{R}$:

$\mathbb{R}(\sqrt{2})$ and $\mathbb{R}(\sqrt[3]{2})$

the minimal polynomials of $\sqrt{2}, \sqrt[3]{2}$ are x^2-2, x^3-2 respectively: their roots are

$$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$$

$$x^3-2 = (x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})$$

where $\omega = e^{2\pi i/3}$ is a 3rd primitive root of unity

Then let's look at the embeddings

$\sigma: \mathbb{R}(\sqrt{2}) \hookrightarrow \overline{\mathbb{R}}$ $\quad$ $\sigma: \mathbb{R}(\sqrt[3]{2}) \hookrightarrow \overline{\mathbb{R}}$

$\sqrt{2} \mapsto \pm\sqrt{2}$ $\quad$ $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$

In particular, we see that the first field remains fixed and the second not.

def: NORMAL EXTENSION, GALOIS EXTENSION
A finite extension $K \subseteq F$ is called normal if for every embedding $\sigma : F \hookrightarrow \overline{K}$ s.t. $\sigma|_K = id_K$, we have that $\sigma(F) = F$.
A finite extension is called GALOIS if it is normal and separable

Prop: Let $K \subseteq F$ be a finite separable extension. Then TFAE:

(1) F/K is Galois.
(2) F is the splitting field of a polynomial with coefficients in K.
(3) for any $\alpha \in F$, the minimal polynomial $m_\alpha(x)$ splits in F.

proof: (3) $\Rightarrow$ (2) $F = K(\alpha)$ and the min poly of α splits in F.
(2) $\Rightarrow$ (1) $F = K(\alpha)$ then for any $\sigma : K(\alpha) \hookrightarrow \overline{K}$ the image of α needs to be one of the roots of $m_\alpha(x)$, but these are all in F
(1) $\Rightarrow$ (3) Let α' be another root of $m_\alpha(x)$
Then there is an embedding $\sigma' : K(\alpha) \hookrightarrow \overline{K}$ s.t. $\sigma'(\alpha) = \alpha'$ then there is an extension

$\sigma : F \hookrightarrow \bar{K}$ and by hypothesis $\sigma(F) = F$, hence $a' \in F$. □

In particular, let $K(a) \supseteq K$ be any finite extension. Then let F be the splitting field of $m_a(x)$ over K. We have $F \supseteq K(a) \supseteq K$ and F is Galois over K. Moreover any Galois extension contains F. Hence, F is the smallest Galois extension

def: NORMAL CLOSURE
$K \subseteq F$ extension. The normal closure is the smallest Galois extension of K which contains F

Example: Let $K = \mathbb{Q}(\sqrt[3]{2})$: then this is not Galois over $\mathbb{Q}$, and indeed the Galois closure is given by $K^{nor} = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

- THE GALOIS GROUP
Let $K \subseteq F$ be a Galois extension. The Galois group is
$$Gal(F/K) = \{\sigma : F \to F \mid \sigma_{|K} = id_K\}$$
Observe that $|Gal(F/K)| = [F : K]$

For every subgroup $G < Gal(F/K)$
we define a subfield of F as

$$Fix(G) = \{ \alpha \in F \mid \sigma(\alpha) = \alpha \ \forall \sigma \in G \}$$

(check that this is a subfield)

Conversely, for subfield $K \subseteq F' \subseteq F$
we define a subgroup

$$Gal(F/F') < Gal(F/K)$$

Thm: FUNDAMENTAL THEOREM of GALOIS THEORY

(i) There is a bijection

$$\{ \text{subgroups of } Gal(F/K) \} \longleftrightarrow \{ \text{subextensions } K \subseteq F' \subseteq F \}$$

$$G \longmapsto Fix(G)$$

$$Gal(F/F') \longleftarrow F'$$

(ii) the correspondence induces a bijection

$$\{ \text{normal subgroups of } Gal \} \longleftrightarrow \{ \text{normal subextensions} \}$$

(iii) If $K \subseteq F' \subseteq F$ is a Galois subextension

$$Gal(F'/K) \cong Gal(F/K) / Gal(F/F').$$

Cor: $\mathrm{Fix}(\mathrm{Gal}(F/k)) = k$.

Examples: (1) QUADRATIC EXTENSIONS

We want to look at extensions $L/\mathbb{Q}$ of degree two: these are called quadratic extensions, and are the simplest nontrivial extensions.

An easy example are extensions $L = \mathbb{Q}(\sqrt{m})$ where $m \in \mathbb{Z}$ is squarefree: the minimal poly is $x^2 - m$, irreducible by Eisenstein, hence $[L:\mathbb{Q}] = 2$. Moreover $x^2 - m = (x - \sqrt{m})(x + \sqrt{m})$ splits completely in L, so that L is Galois with Galois group $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ gen by $\sigma : \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt{m})$

$$\sqrt{m} \longmapsto -\sqrt{m}$$

Conversely, suppose $[L:\mathbb{Q}] = 2$: then we can write $L = \mathbb{Q}(\alpha)$ with α a root of

$$x^2 + bx + c = 0 \quad (\text{min poly})$$

by the p-q formula we can write

$$-b + \sqrt{b^2 - 4c}$$

$$\alpha = \frac{b - \sqrt{b^2 - 4c}}{2}$$

hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2-4c})$. This shows that every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{\frac{a}{b}})$ for some $a, b \in \mathbb{Z}$.
We can do a bit more:

$$\mathbb{Q}\left(\sqrt{\frac{a}{b}}\right) = \mathbb{Q}\left(\sqrt{\frac{a \cdot b}{b \cdot b}}\right) = \mathbb{Q}\left(\frac{\sqrt{ab}}{b}\right)$$

$$= \mathbb{Q}(\sqrt{ab}).$$

Hence every quadratic extension is of the form $\mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$ sqfs.

(2) Cyclotomic fields

The n-th cyclotomic field is the extension $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive n-th root of unity.

This is the splitting field of $x^n - 1$, hence it is Galois. What is the Galois group?

We need to look at the conjugates of ζ_n: these are all of the form ζ_n^k for $0 \leq k < n$, since

These are the roots of $x^n - 1$. First we observe that

$$\zeta_n^k = e^{2\pi i \frac{k}{n}} = e^{\frac{2\pi i \frac{k}{(k,n)}}{\frac{n}{(k,n)}}} = e^{2\pi i \frac{k/(k,n)}{n/(k,n)}}$$

Hence ζ_n^k is a root of $x^{\frac{n}{(k,n)}} - 1$.

Claim: Conjugates of ζ_n are precisely the ζ_n^k are $(k,n) = 1$.

We will maybe prove it later. Hence

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

hence

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \quad (\text{Euler's function})$$

Now we observe that if n is odd, then

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$$

indeed $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{2n})$ and moreover

$$\varphi(n) = \varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$$

so they are the same.

Conversely

Fact: The cyclotomic fields $\mathbb{Q}(\zeta_n)$ with n even are all distinct.