LECTURE 33

(33.0) Fundamental theorem of Galois theory.– Recall that last time we proved the following result. For an algebraic Galois extension L/K, there is a topology on the Galois group $\mathsf{G}(L/K)$, with regards to which we have bijections:

$$\begin{tikzcd} \boxed{\begin{array}{c}\text{Subextensions}\\ \text{of } L/K\end{array}} \arrow[r, bend left, "\mathcal{G}"] & \boxed{\begin{array}{c}\text{Closed subgroups}\\ \text{of } \mathsf{G}(L/K)\end{array}} \arrow[l, bend left, "\mathcal{F}"] \end{tikzcd}$$

Here, $\mathcal{F}(H) = L^H$ and $\mathcal{G}(E) = \mathsf{G}(L/E)$.

These notes contain a description of the Galois group of the algebraic closure of a finite field, as a topological group. The main theorem is stated and proved for $\mathbb{F}_p$, though the argument is valid for any finite field (necessarily of the form $\mathbb{F}_{p^r}$, see Theorem 33.2 below). Thus, for any finite field k, the Galois group $\mathsf{G}\left(\overline{k}/k\right)$ is independent of k, and is given by $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$.

(33.1) A useful lemma.–

Lemma. *Let F be a field and $A \subset F^\times$ a finite subgroup. Then A is cyclic.*

Proof. Let $m \in \mathbb{Z}_{\geq 1}$ be such that $m\mathbb{Z} \subset \mathbb{Z}$ is the annihilator of A. That is, m is the smallest positive integer such that $a^m = 1$ for every $a \in A$. Thus, every element of A is a root of $x^m - 1$. Since a polynomial cannot have more roots than its degree, we have $|A| \leq m$. Note that $m \leq |A|$, since $a^{|A|} = 1$ for every $a \in A$, which proves that $m = |A|$. By HW 10, Problem 12, there exists $x \in A$ of order m, proving that A is cyclic. $\square$

(33.2) Finite fields.– Let us fix $p \in \mathbb{Z}_{\geq 2}$ a prime number. Let K be a finite field of characteristic p. Then $[K : \mathbb{F}_p] = r$ implies that K has $q = p^r$ elements.

Theorem. *For each $r \in \mathbb{Z}_{\geq 1}$, there exists a unique (up to isomorphism) field with $q = p^r$ elements, denoted by $\mathbb{F}_q$. This field K is determined by the following equivalent properties.*

1. *K is the splitting extension of $x^q - x \in \mathbb{F}_p[x]$.*
2. *Let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$, and let σ_p be the Frobenius endomorphism of $\overline{\mathbb{F}_p}$. Then $K = \{\alpha \in \overline{\mathbb{F}_p} : \sigma_p^r(\alpha) = \alpha\}$.*

Moreover, there exists $a \in K$ such that $K = \mathbb{F}_p(a)$.

Proof. Since $|K| = q$, $K^\times$ is a finite abelian group of order $q-1$, proving that $a^{q-1} = 1$ for every $a \in K^\times$. This implies that every element of K is a solution of $x^q - x = 0$. Hence K consists of all (distinct) roots of $x^q - x \in \mathbb{F}_p[x]$. By definition, K is the splitting extension of this polynomial, proving its uniqueness and (1) above. (2) is merely a reformulation of (1), since $\sigma_p^r(\alpha) = \alpha$ is same as saying that α is a root of $x^{p^r} - x$.

Note that $K^\times$ is a cyclic group, by Lemma 33.1 above. Let $a \in K^\times$ be its generator. Then $K = \mathbb{F}_p(a)$. $\square$

(33.3) Galois group of $\overline{\mathbb{F}_p}/\mathbb{F}_p$.– Again we fix a prime number $p \in \mathbb{Z}_{\geq 2}$. For any field K of characteristic p, we will denote by σ_p the Frobenius endomorphism of K.

Let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. As a corollary of Theorem 33.2, we have the following description of finite subextensions of $\overline{\mathbb{F}_p}$.

Corollary.

(1) *Every finite subextension $K/\mathbb{F}_p$ of $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is Galois.*

(2) *We have a bijection between the set of finite (Galois) subextensions of $\overline{\mathbb{F}_p}/\mathbb{F}_p$ and $\mathbb{Z}_{\geq 1}$:*

$$r \in \mathbb{Z}_{\geq 1} \rightsquigarrow K_r = \mathbb{F}_{p^r}$$

(3) $\mathsf{G}\left(\mathbb{F}_{p^r}/\mathbb{F}_p\right) \cong \mathbb{Z}/r\mathbb{Z}$ *is generated by the Frobenius automorphism σ_p.*

Hence, we have:

$$\boxed{\mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \cong \varprojlim_{r \in \mathbb{Z}_{\geq 1}} \mathbb{Z}/r\mathbb{Z}}$$

Note that the inverse system appearing above is based on the partially ordered set $\mathbb{Z}_{\geq 1}$, where the partial order is via divisibility. That is, we have a group homomorphism $\rho_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, sending $\overline{1}$ to $\overline{1}$, assuming that m divides n.

(33.4) $\mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right)$ is (topologically) cyclic.– By our description of the topology on the Galois group (see Lecture 32, §32.2), the following sets are open and form a fundamental system of neighbourhoods of identity:

$$U_n = \{g \in \mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) : g|_{\mathbb{F}_{p^n}} = \mathrm{Id}\}.$$

Note that $U_n = \mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_{p^n}\right)$.

Proposition. $\mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right)$ *is topologically generated by the Frobenius automorphism σ_p. The subgroup generated by σ_p is isomorphic to $\mathbb{Z}$ and is dense on* $\mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right)$.

Proof. This follows easily from the fundamental theorem, since if $H = \langle \sigma_p \rangle$, then:

$$\left(\overline{\mathbb{F}_p}\right)^H = \mathbb{F}_p = \left(\overline{\mathbb{F}_p}\right)^G ,$$

implying that $\overline{H} = G$.

Let us try to prove it directly. That is, given $g \in G$, and $n \in \mathbb{Z}_{\geq 1}$, we have to prove that $gU_n \cap H \neq \emptyset$. In other words, $g|_{\mathbb{F}_{p^n}} = \sigma_p^k|_{\mathbb{F}_{p^n}}$ for some k. This is obviously true, since $\mathsf{G}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ is cyclic and generated by σ_p.

It remains to show that $H \cong \mathbb{Z}$. If not, then there exists N such that $\sigma_p^N = \mathrm{Id}$ on $\overline{\mathbb{F}_p}$. But that would mean that $\overline{\mathbb{F}_p} = \mathbb{F}_{p^N}$ is finite, contradicting the fact that algebraically closed fields are necessarily infinite. $\square$

(33.5) ℓ**–adic integers.–** Let Z denote the set $\mathbb{Z}_{\geq 1}$, with partial order given by divisibility[1].

$$m, n \in \mathrm{Z}, \qquad m \leq n \iff m \text{ divides } n.$$

Let P denote the set of prime numbers and for $\ell \in \mathrm{P}$, consider the totally ordered subset $\mathrm{Z}(\ell) \subset \mathrm{Z}$ given by

$$\mathrm{Z}(\ell) = \{\ell^r : r \in \mathbb{Z}_{\geq 0}\}.$$

We have the following inverse limits:

$$\widehat{\mathbb{Z}} := \lim_{n \in \mathrm{Z}} \mathbb{Z}/n\mathbb{Z}, \qquad \mathbb{Z}_\ell := \lim_{\ell^r \in \mathrm{Z}(\ell)} \mathbb{Z}/\ell^r\mathbb{Z}.$$

Remark. For each prime number ℓ, $\mathbb{Z}_\ell$ is a topological ring, called the ring of ℓ–adic integers. $\widehat{\mathbb{Z}}$ also has a ring structure, though in the statement $\mathsf{G}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \cong \widehat{\mathbb{Z}}$, we are only claiming isomorphism of topological *groups*.

$\mathbb{Z}_\ell$ is known to be uncountable. For instance, for $\ell = 2$, $\mathbb{Z}_2$ is homeomorphic to the Cantor set (the one obtained by repeatedly removing the middle third from an interval) - left as an interesting exercise.

Proposition.

$$\boxed{\widehat{\mathbb{Z}} \cong \prod_{\ell \in \mathrm{P}} \mathbb{Z}_\ell}$$

Idea of the proof. It is an interesting exercise to work out the details of this isomorphism. The underlying idea is the *chinese remainder theorem.*

A typical element of $\widehat{\mathbb{Z}}$ is a sequence of numbers $(a_n)_{n \geq 1}$ such that

- $a_n \in \{0, \ldots, n-1\}$.
- For each $n, k \in \mathbb{Z}_{\geq 1}$, $a_n = a_{kn}$ modulo n.

We claim that such a sequence of numbers is completely determined by its coordinates placed at powers of primes. That is, if $\underline{a}$ and $\underline{b}$ are two elements of $\widehat{\mathbb{Z}}$ such that for every prime number ℓ, and non–negative integer r, we have $a_{\ell^r} = b_{\ell^r}$, then $\underline{a} = \underline{b}$.

To see why this is true, let n be an arbitrary positive integer, and let $n = \ell_1^{r_1} \cdots \ell_k^{r_k}$ be its prime factorization. By Chinese remainder theorem:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\ell_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell_k^{r_k}\mathbb{Z} \ ,$$

where the map sends x to its respective residue class modulo powers of primes on the right hand side. Thus, if we know that $a_{\ell_j^{r_j}} = b_{\ell_j^{r_j}}$ for every j, then $a_n = b_n$.

[1] I am using a different notation Z, so as not to confuse its partial order with the usual total order on integers.