Lecture 34

(34.0) Recall: for a field K and a polynomial $p(x) \in F[x]$ which is a (multiplicity free) product of distinct monic irreducible polynomials $f_1, \ldots, f_r \in F[x]$:

$$p(x) = f_1(x) \cdots f_r(x)$$

$p(x)$ is separable iff each f_i is. Perfect fields are those for which every irreducible polynomial is separable. We proved that if $f(x) \in K[X]$ is an irreducible, non-separable polynomial then $\mathrm{Char}(K) = p \neq 0$ and $f(x) \in K[X^p]$.

Proposition. K is imperfect if and only if $\mathrm{Char}(K) = p \neq 0$ and $\sigma_p : K \to K$, $a \mapsto a^p$ is not surjective (i.e. not an iso.) (it is automatically injective, being a morphism of fields)

Pf ($\Rightarrow$) If K is imperfect, there must exist an irreducible $g(X) \in K[X]$ s.t. $g'(X) = 0$. i.e. $g(X) \in K[X^p]$

But if σ_p is surjective, then $g(X) = f(X)^p$ (if $g(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ and $b_0, \ldots, b_{n-1} \in K$ are s.t. $b_i^p = a_i$ then $f(X) = X^{n/p} + b_{n-1}X^{\frac{n-1}{p}} + \ldots + b_0$)

contradicts irreducibility of g.

($\Leftarrow$) Assume $\sigma_p : K \to K$ is not surjective. Pick $a \in K \setminus$ Image of σ_p. We claim that $g(X) = X^p - a \in K[X]$ is irreducible This is because in the splitting extn. L of $g(X)$ over K, $L = K(b)$ where $b^p = a$, we have $(X-b)^p = X^p - a$.

This observation translates to

$$\underset{\text{is irreducible}}{g(X) = X^p - a \in K[X]} \iff a \notin \text{Image of } \sigma_p : K \to K$$

Now all the polynomials appearing above are inseparable

Thus K is imperfect $\iff$ σ_p is not surjective.

Proof of the equivalence above.

Let $g(X) = X^p - a \in K[x]$ ($a \in K$ arbitrary for now.)

Write $g(X) = g_1(X)^{n_1} \cdots g_r(X)^{n_r}$ where $g_1, \dots, g_r \in K[X]$ are distinct irred. monic polynomials.

If $i \neq j \in \{1, \dots, r\}$, $g_i \neq g_j$ hence must have different roots in any extension But in the splitting extn. of g, there is only one root.

$\Rightarrow r = 1$ and $g(X) = g_1(X)^n \Rightarrow p = n \cdot \deg(g_1)$

As p is prime, either $g(X) = g_1(X)^p$ where $g_1(X) = X - b$ for some b s.t. $b^p = a$

or $g(X) = g(X)$ is irreducible. □

(34.1) Corollary of Prop. (34.0) Every finite field is perfect.

(K : char $p \neq 0$, $\sigma_p : K \to K$ is injective. If $|K| < \infty$, it is surjective , hence K is perfect.).

(34.2) A group-theoretic lemma.

Lemma. Let G be a finite abelian group and

$$m = \max\{\mathrm{ord}(g) \mid g \in G\} \quad \text{(called exponent of } G\text{)}$$

Then $\forall\, \tau \in G$, $\tau^m = 1$. (i.e. $\mathrm{ord}(\tau)$ divides m).

This lemma can be immediately deduced from the structure theorem of finite abelian groups. We will give an independent proof below, which in turn can be used to prove the structure theorem.

Corollary of the lemma. Let K be a finite field, of $\mathrm{Char}(K) = p\ (\neq 0)$.

Then $K^\times$ is a finite abelian group. Let m = exponent of $K^\times$.

Then $a^m = 1$ $\forall\, \alpha \in K^\times$ $\Rightarrow$ There are at least $|K^\times|$ solutions of the equation $X^m - 1 = 0$. Thus $|K^\times| = m$ is cyclic.

Primitive element thm (finite)

$\Rightarrow$ $K = \mathbb{F}_p(\alpha)$ for some $\alpha \in K$.

$$\boxed{K : \text{finite field} \Rightarrow \exists\, \alpha \in K \text{ s.t. } K = \mathbb{F}_p(\alpha)}$$

(34.3) Proof of Lemma (34.2).

G : a finite group. (written additively below). $\quad m = \max\{\operatorname{ord}(g) \mid g \in G\}$

Pick $\sigma \in G$ s.t. $\operatorname{ord}(\sigma) = m$. We want to show that $\forall\, \tau \in G$, $\operatorname{ord}(\tau)$ divides m. By defn. of m, $\operatorname{ord}(\tau) \leq m$.

So let $H = \langle \sigma, \tau \rangle \subset G$. Let k be smallest s.t. $k\tau^* \in \langle \sigma \rangle$ (assuming $\tau \notin \langle \sigma \rangle$, $k \in \{2, \dots, \operatorname{ord}(\tau)\}$, i.e. $2 \leq k \leq \operatorname{ord}(\tau) \leq m$).

$k\tau = j \cdot \sigma$. Exercise. – up to changing the generator $\tau \to \tau + \alpha\sigma$ we may assume that $0 \leq j \leq k-1$.

[Hint:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/m\mathbb{Z} \arrow[r] & H \arrow[r] & \mathbb{Z}/k\mathbb{Z} \arrow[r] & 0 \\
 & \bar{1} \arrow[r, mapsto] & \sigma \arrow[r, mapsto] & 0 & \\
 & & \tau \arrow[r, mapsto] & \bar{1} &
\end{tikzcd}$$

is an element of

$$\operatorname{Ext}^1(\mathbb{Z}/k\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) = \frac{\mathbb{Z}/m\mathbb{Z}}{\text{Image of } \mu_k : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}} .$$]

But then $\operatorname{ord}(\tau) = k \cdot \dfrac{m}{\gcd(j, m)} \leq m \implies j = 0$, in which case $(0 \leq j \leq k-1 \leq m-1)$

$k = \operatorname{ord}(\tau)$ &

$$\operatorname{ord}(\sigma + \tau) = \text{l.c.m.}(m, k) \leq m$$

i.e. k divides m $\quad \square$

(34.4) Primitive element theorem. Let K/F be an algebraic extension such that there are only finitely many sub-F-extensions of K. Then $\exists\ \alpha \in K$ s.t. $K = F(\alpha)$. [Converse will be proved next time.]

Proof Note first that the hypothesis implies that K/F is a finite extension. This is because K, being algebraic, is the direct limit of finite sub-F-extns. of K $(F \subset E \subset K$ s.t. $(E:F) < \infty)$.

Thus, if there are only finitely many such extns., then K is necessarily one of them.

So we know $K = F(\alpha_1, \dots, \alpha_n)$ for some finite set $\alpha_1, \dots, \alpha_n$

K/F has only finitely many subextns.

Now we proceed by induction on n, to show that $K = F(\alpha)$ for some $\alpha \in K$. $n = 1$ case being trivial, and induction hypothesis reduces the problem to $n = 2$. i.e. $K = F(\alpha, \beta)$

K/F has finitely many sub-F-extns.

(T.S.)

$\Rightarrow \exists\ \gamma \in K$ s.t. $F(\gamma) = K$.

Remark. If F is finite (equivalently, K is finite since $(K:F)<\infty$) then the theorem is true because of Cor. (34.2) page 3 above.

Let us focus on the case when F is an infinite field. Then $\alpha+t\beta \in F(\alpha,\beta)$ $(t \in F)$ are infinitely many elements of $F(\alpha,\beta)$

So there must be $\alpha+s\beta \in F(\alpha+t\beta)$ $(s \neq t)$, as there are only finitely many $F \subset E \subset F(\alpha,\beta)$. But then $\begin{matrix}\alpha+s\beta\\ \alpha+t\beta\end{matrix} \in F(\alpha+t\beta)$

$\Rightarrow \alpha, \beta \in F(\alpha+t\beta)$. Hence, for $\gamma=\alpha+t\beta$,

$F(\alpha,\beta) = F(\gamma)$. □

(34.5) ~~Special case. K/F is a finite Galois extn. That is, $K = F(\alpha_1,\dots,\alpha_n)$ where $\alpha_1,\dots,\alpha_n \in K$ are distinct roots of a monic polynomial $p(x) \in F[x]$. We may as well assume that $p(x)$ is irreducible and separable. Let N = degree of K/F $(=(K:F))$~~

(recall: N divides $n!$)

FOR LATER.