LECTURE 30

(30.0) Galois extensions.– Let L/K be a field extension, and let $\Gamma = \mathsf{G}(L/K)$ be its Galois group. Recall that we say L/K is a Galois extension if $L^\Gamma = K$.

In previous lecture, we showed that an algebraic extension L/K is Galois if and only if it is *normal and separable.*

- An algebraic extension L/K is called *normal* if for every $\alpha \in L$, $\mathsf{m}_\alpha(x)$ splits into linear factors in $L[x]$.

- A polynomial $f(x) \in K[x]$ is said to be *separable* if $f(x)$ has distinct roots in $\mathcal{E}(f(x), K)$, the splitting extension of $f(x)$ over K.

- An algebraic extension L/K is said to be *separable* if for every $\alpha \in L$, the minimal polynomial $\mathsf{m}_\alpha(x)$ is separable.

We will prove that normal extensions are nothing but splitting extensions of various subsets of $K[x]$. Theorem 29.5 says that an algebraic extension is Galois if and only if it is the splitting extension of a set of separable polynomials. We will discuss how an irreducible polynomial may fail to be separable.

(30.1) Normal extensions.– Recall that a field extension L/K is normal if it is algebraic, and for every $\alpha \in L$, $\mathsf{m}_\alpha(x)$ splits into a product of (not necessarily distinct) linear factors in $L[x]$.

Theorem. *The following are equivalent, for an algebraic extension L/K.*

(1) *L/K is normal.*
(2) *There exists a set $P \subset K[x]$, such that $L = \mathcal{E}(P, K)$ is the splitting extension of P.*
(3) *For every extension E/L and $g \in \mathsf{G}(E/K)$, $g(L) = L$. Thus we have a short exact sequence:*
$$\mathbf{1} \to \mathsf{G}(E/L) \to \mathsf{G}(E/K) \to \mathsf{G}(L/K) \to \mathbf{1},$$
proving that $\mathsf{G}(E/L) \subset \mathsf{G}(E/K)$ is a normal subgroup.
(4) *Let $\overline{K}$ be the algebraic closure of K. We view $L \subset \overline{K}$ via a fixed embedding. Then, for every $g \in \mathsf{G}\left(\overline{K}/K\right)$, we have $g(L) = L$.*

Proof. (1) $\Rightarrow$ (2). It is clear that $L = \mathcal{E}(P_L, K)$, where
$$P_L(x) = \{\mathsf{m}_\alpha(x) : \alpha \in L\} \subset K[x].$$

(2) $\Rightarrow$ (3). Assume that a set $I \subset K[x]$ of irreducible, monic polynomials is given. It is not a serious restriction, since given any set $P \subset K[x]$, we may replace P by I consisting of irreducible polynomials which divide some element of P. Then $\mathcal{E}(P, K) = \mathcal{E}(I, K)$. Let $L = \mathcal{E}(I, K)$. Let E/L be an arbitrary extension and $g \in \mathsf{G}(E/K)$. To show that $g(L) = L$,

it is enough to prove that $g(\alpha) \in L$ for every $\alpha \in L$ which is a root of some $f(x) \in P$ (since L is generated over K by such elements). Now $g(\alpha)$ is another root of $f(x)$, hence is in L.

(3) $\Rightarrow$ (4) is obvious. Now we show that (4) implies (1). Let $\alpha \in L$ and $f(x) = \mathsf{m}_\alpha(x) \in K[x]$. In $\overline{K}[x]$, we have the factorization $f(x) = (x - r_1) \cdots (x - r_n)$, where $n = \deg(f)$ and $r_1, \ldots, r_n \in \overline{K}$ are not necessarily distinct. Assuming $r_1 = \alpha$, let $r_j = \beta$ be different from α (if $r_1 = \ldots = r_n = \alpha$, then $f(x) = (x - \alpha)^n$ is already in $L[x]$ as we want to prove). Then $f(x) = \mathsf{m}_\alpha(x) = \mathsf{m}_\beta(x)$ and hence (by Theorem 26.1) there exists $g \in \mathsf{G}\left(\overline{K}/K\right)$ such that $g(\alpha) = \beta$. As $g(L) \subset L$, we conclude that $\beta \in L$. We have shown that $r_1, \ldots, r_n \in L$, that is, $f(x)$ splits into a product of linear factors in $L[x]$. $\square$

(30.2) Separable polynomials.– Theorem 29.5 can now be stated as follows. An algebraic extension L/K is Galois if and only if $L = \mathcal{E}(I, K)$ where $I \subset K[x]$ is a set of irreducible, separable polynomials.

Theorem. *Let K be a field and let $f(x) \in K[x]$ be an irreducible, monic polynomial of degree $n \geq 1$. Then the following conditions are equivalent.*

1. *$f(x)$ has n distinct roots in its splitting extension (i.e, $f(x)$ is separable).*
2. *The ideal generated by f and its derivative f' in $K[x]$ is the unit ideal.*
3. *$f'(x) \neq 0$.*
4. *Either $\mathrm{Char}(K) = 0$, or $\mathrm{Char}(K) = p$ ($p \in \mathbb{Z}_{\geq 2}$ a prime number) and $f(x) \notin K[x^p] \subset K[x]$.*

Proof. We will first show that (1) and (2) are equivalent. (2) and (3) are clearly equivalent, since $f(x)$ is irreducible. (4) follows since

$$f(x) = x^n + \sum_{j=0}^{n-1} c_j x^j \qquad \Rightarrow \qquad f'(x) = nx^{n-1} + \sum_{j=1}^{n-1} jc_j x^{j-1},$$

Thus $f'(x) = 0$ if and only if $jc_j = 0$ for every $1 \leq j \leq n$ (with the assumption that $c_n = 1$). If $\mathrm{Char}(K) = 0$, this is equivalent to $c_j = 0$ for every $1 \leq j \leq n$, i.e, f is a constant. But $\deg(f) \geq 1$. In $\mathrm{Char}(K) = p$ case, we conclude that either $c_j = 0$ or $p|j$. That is, $f(x) \in K[x^p]$.

(1) $\iff$ (2). Let L/K be the splitting extension of $f(x)$. Write $f(x) = \displaystyle\prod_{i=1}^{n}(x - r_i)$. Then:

$$f'(x) = \sum_{j=1}^{n} \prod_{i \neq j} (x - r_i).$$

Thus, for each $1 \leq j \leq n$, $f'(r_j) = \prod_{i \neq j}(r_j - r_i)$. Therefore, $f(x) \in K[x]$ has a repeated root $r \in L$ if and only if $f'(r) = 0$. Now, if $(f, f') = (1)$ in $K[x]$, then there exist $a(x), b(x) \in K[x]$ such that $a(x)f(x) + b(x)f'(x) = 1$. Setting $x = r$ gives $0 = 1$ which is absurd.

Conversely, assume that $(f, f') = (d(x))$. Since $d(x)$ divides $f(x)$, it has a root $\gamma \in L$. Since $d(x)$ divides $f'(x)$, $f'(\gamma) = 0$. So f has a repeated root. $\square$

(30.3) Perfect fields.–

Definition. A field K is said to be *perfect* if every irreducible polynomial $f(x) \in K[x]$ is separable. Thus, every field of characteristic zero is perfect (by Theorem 30.2). Every algebraically closed field is perfect.

Lemma. *Let $p \in \mathbb{Z}_{\geq 2}$ be a prime number. Let K be a field of characteristic p. Then $\sigma_p : K \to K$ given by $\sigma_p(x) = x^p$ is a homomorphism (known as Frobenius endomorphism). K is perfect if and only if σ_p is an isomorphism.*

Proof. It is clear that $\sigma_p(xy) = \sigma_p(x)\sigma_p(y)$. Note that

$$\sigma_p(x+y) = (x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p,$$

since for every $1 \leq i \leq p-1$, the binomial coefficient:

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!}$$

is divisible by p, hence zero in K. Thus $\sigma_p : K \to K$ is a homomorphism.

Now assume that $\sigma_p : K \to K$ is an isomorphism. If K is not perfect, the there would exist $g(x) \in K[x]$ monic irreducible such that $g'(x) = 0$. But that means $g(x) \in K[x^p]$, i.e,

$$g(x) = \sum_{j=0}^{n} c_j x^{pj}, \text{ with } c_n = 1.$$

Let $a_j \in K$ be such that $a_j^p = c_j$. Then

$$g(x) = \left(\sum_{j=0}^{n} a_j x^j\right)^p \text{ is not irreducible.}$$

For the converse, we will need the following claim.
Claim. For every $a \in K$, $x^p - a \in K[x]$ is irreducible if and only if $a \notin \mathrm{Im}(\sigma_p)$.

Let us assume the claim for now. Assume that σ_p is not surjective. That is there exists $a \notin \mathrm{Im}(\sigma_p)$. By the claim, $x^p - a \in K[x]$ is irreducible, and its derivative is 0, so it is not separable. Thus, K is not perfect.

Proof of the claim. Let L/K be the splitting extension of $f(x) = x^p - a \in K[x]$, and let $b \in L$ be a root of $f(x)$. Then $f(x) = (x-b)^p$. Now if $f(x) = f_1(x)^{n_1} \cdots f_r(x)^{n_r}$ is the unique factorization of $f(x)$ into a product of monic irreducible polynomials in $K[x]$, then in L, each $f_j(x)$ can only have one root, namely b. But distinct irreducible polynomials are coprime, so they cannot share a root. This implies that $r = 1$ and $f(x) = g(x)^n$. By degree reasons, either $g(x) = f(x)$ is irreducible, or $g(x)$ is linear (hence necessarily equal to $x - b$) and $n = p$, proving that $b = a^{1/p} \in K$. ∎

(30.4) Imperfect fields and purely inseparable extensions.– According to Lemma 30.3 above, every finite field is perfect. The first non–trivial example of imperfect fields is thus $K = \mathbb{F}_p(\lambda)$. Since $\lambda \notin \mathrm{Im}(\sigma_p)$, K is imperfect. Moreover the splitting extension of $x^p - \lambda \in K[x]$ is $K_1 = \mathbb{F}_p(\lambda_1)$, where $\lambda_1^p = \lambda$. Continuing this way, we obtain a tower of field extensions:

$$K \subset K_1 \subset K_2 \subset \cdots$$

where $K_n = \mathbb{F}_p(\lambda_n)$ is the splitting extension of $x^p - \lambda_{n-1} \in K_{n-1}[x]$. In other words,

$$K_n = \text{ the splitting extension of } x^{p^n} - \lambda \in K[x].$$

Note that $\mathsf{G}\,(K_n/K) = \{\mathrm{Id}\}$, so in a very concrete sense, the Galois group cannot *separate* different K_n/K. Such extensions are thus orthogonal to Galois extensions and are defined to be purely inseparable (or p–radical) extensions.

Definition. Let K be a field of characteristic $p \in \mathbb{Z}_{\geq 2}$. Let E/K be a field extension. An element $\alpha \in E$ is said to be *purely inseparable* (or *p–radical*) if there exists n such that $\alpha^{p^n} \in K$. The smallest such n is often called *height of* α. An algebraic extension E/K is called purely inseparable if it is generated by a set of purely inseparable elements.