LECTURE 29

(29.0) Review.– Let L/K be a field extension. Last time we defined

$$\mathsf{G}\,(L/K) = \mathrm{Aut}_{K\text{–Alg}}(L) = \{\sigma : L \xrightarrow{\sim} L \text{ field automorphism, such that } \sigma|_K = \mathrm{Id}_K\},$$

called the Galois group of the extension L/K.

For a group Γ acting on L via field automorphisms (that is, we are given a group homomorphism $\Gamma \to \mathrm{Aut}_{\text{field}}(L)$), we denote by $L^\Gamma \subset L$, the subfield of Γ–fixed elements:

$$L^\Gamma = \{z \in L \text{ such that } \sigma(z) = z,\ \forall\, \sigma \in \Gamma\}.$$

A field extension L/K is called a *Galois extension* if $L^{\mathsf{G}(L/K)} = K$.

(29.1) Linear independence of algebra homomorphisms.– Let K be a field, L/K a field extension, and A a unital (not necessarily commutative) algebra over K. Meaning, A is a unital ring together with a ring homomorphism, necessarily injective, $K \hookrightarrow A$.

Theorem. $\mathrm{Hom}_{K\text{–Alg}}(A, L) \subset \mathrm{Hom}_{K\text{–vs}}(A, L)$ *is linearly independent over* L.

Remark. For a K–vector space V, we view $\mathrm{Hom}_{K\text{–vs}}(V, L)$ as an L–vector space via the following operations. For every $\xi, \eta : V \to L$, K–linear maps, and $a, b \in L$, we set:

$$(a\xi + b\eta)(v) = a\xi(v) + b\eta(v).$$

Note that, we have the canonical L–linear map:

$$\beta : V^* \otimes_K L \to \mathrm{Hom}_{K\text{–vs}}(V, L), \qquad \beta(f \otimes z) : v \mapsto f(v)z.$$

If V is finite–dimensional, this map is an isomorphism, and we obtain:

$$\boxed{\dim_{L\text{–vs}}\left(\mathrm{Hom}_{K\text{–vs}}(V, L)\right) = \dim_{K\text{–vs}}(V^*) = \dim_{K\text{–vs}}(V)}$$

Proof. Let $\{\xi_1, \ldots, \xi_n\} \subset \mathrm{Hom}_{K\text{–Alg}}(A, L)$ be a finite set of K–algebra homomorphisms $A \to L$. We will show, by induction on n, that this set of linearly indepedent. For $n = 1$, we have $\{\xi : A \to L\}$ is linearly independent if and only if $\xi \neq 0$, which is true since $\xi(1) = 1$.

Now assume that we have a linear relation $\displaystyle\sum_{i=1}^{n} a_i \xi_i = 0$, where $a_1, \ldots, a_n \in L$. Note that for every $x, y \in A$, we get:

$$a_n \xi_n(xy) - \xi_n(x)(a_n \xi_n(y)) = 0.$$

Replacing $a_n\xi_n = -\sum_{i=1}^{n-1} a_i\xi_i$, we get:

$$\sum_{i=1}^{n-1} a_i(\xi_i(x) - \xi_n(x))\xi_i(y) = 0, \text{ for every } y \in A.$$

Thus, we obtain (by induction) that for every $1 \leq i \leq n-1$, and $x \in A$: $a_i(\xi_i(x) - \xi_n(x)) = 0$. Since $\xi_i \neq \xi_n$, there must exist some $x \in A$ such that $\xi_i(x) \neq \xi_n(x)$, implying that $a_i = 0$. Now $a_n\xi_n = -\sum_{i=1}^{n-1} a_i\xi_i = 0$, but $\xi_n \neq 0$, and we conclude that $a_n = 0$. Therefore, the set $\{\xi_1, \ldots, \xi_n\}$ is linearly independent over L. □

(29.2) Application of Theorem 29.1 I: independence of characters.– Let Γ be a group and L be a field. Let $L[\Gamma]$ be the group algebra of Γ over L. As an L–vector space, $L[\Gamma]$ has a basis $\{e(g) : g \in \Gamma\}$, relative to which multiplication is determined by $e(g) \cdot e(h) = e(gh)$. Note that

$$\mathrm{Hom}_{\mathrm{gp}}(\Gamma, L^\times) = \mathrm{Hom}_{L\text{–Alg}}(L[\Gamma], L).$$

Therefore, we obtain the following result, due to Dedekind, known as *independence of characters.* An L–valued character of a group Γ, is just a group homomorphism $\Gamma \to L^\times$.

Corollary. *Elements of* $\mathrm{Hom}_{\mathrm{gp}}(\Gamma, L^\times)$ *are linearly independent over* L*.*

(29.3) Application of Theorem 29.1 II: inequalities.– Let K be a field and E/K, L/K two field extensions. By Theorem 29.1, $\mathrm{Hom}_{K\text{–Alg}}(E, L) \subset \mathrm{Hom}_{K\text{–vs}}(E, L)$ is linearly independent over L. Moreover, if $[E : K] < \infty$, $\mathrm{Hom}_{K\text{–vs}}(E, L)$ is an L–vector space of dimension $[E : K]$ (see Remark 29.1). Thus, we get:

$$\boxed{|\mathrm{Hom}_{K\text{–Alg}}(E, L)| \leq [E : K]}$$

Taking $E = L$, and viewing $\mathsf{G}(L/K) \subset \mathrm{Hom}_{K\text{–Alg}}(L, L)$, we get:

$$\boxed{|\mathsf{G}(L/K)| \leq [L : K]}$$

(29.4) Application of Theorem 29.1 III: Artin's theorem.– Now let L be a field and let $\Gamma \subset \mathrm{Aut}_{\mathrm{field}}(L)$ be a finite subgroup. Let $F = L^\Gamma \subset L$.

Theorem. *L/F is a Galois extension of degree* $|\Gamma|$*.*

Proof. Let $n = |\Gamma|$ and $m = [L : F]$. Since $\Gamma \subset \mathrm{Hom}_{F\text{–Alg}}(L, L)$, the inequalities from the previous paragraph imply that $n \leq m$. Assume that $n < m$. Let $\Gamma = \{\sigma_1, \ldots, \sigma_n\}$ and $\{x_1, \ldots, x_m\}$ be a basis of L as an F–vector space. Form an $n \times m$ matrix:

$$X = (\sigma_i(x_j))_{1 \leq i \leq n, 1 \leq j \leq m} \in \mathrm{Mat}_{n \times m}(L).$$

Since $m > n$, there exists a non–zero vector $\underline{a} \in L^m$, such that $X\underline{a} = \underline{0}$. That is, for every $1 \leq i \leq n$:

$$\sum_{j=1}^{m} a_j \sigma_i(x_j) = 0.$$

We will arrive at a contradiction as follows. Let p be the smallest positive integer such that there exists $\underline{a} \in \operatorname{Ker}(X)$ with p non–zero entries. Note that $p = 1$ is absurd since it will imply the existence of $1 \leq j \leq m$ such that $\sigma_i(x_j) = 0$ for each i. But σ_i is an automorphism and $x_j \neq 0$.

Assuming the existence of $\underline{a} \in \operatorname{Ker}(X)$ with p non–zero entries, we will produce $\underline{b} \in \operatorname{Ker}(X)$ with $p-1$ non–zero entries, thus a contradiction, proving that $\operatorname{Ker}(X) = \{0\}$.

Upon reordering elements of Γ, if necessary, we can assume that $a_1, \ldots, a_p \in L^\times$ and $a_{p+1} = \ldots = a_m = 0$. Further, we can scale $\underline{a}$ to assume that $a_p = 1$. Thus,

$$\text{For every } 1 \leq i \leq n,\ \sigma_i(x_p) = -\sum_{j=1}^{p-1} a_j \sigma_i(x_j).$$

Since Γ is a subgroup, there is i such that $\sigma_i = \mathrm{Id}_L$. We are assuming that $\{x_1, \ldots, x_m\}$ are linearly independent over F, so $x_p = -\sum_{j=1}^{p-1} a_j x_j$ implies that there must be some $1 \leq \ell \leq p-1$ so that $a_\ell \notin F$. By definition of F, this means there is $1 \leq k \leq n$, with $\sigma_k(a_\ell) \neq a_\ell$.

Apply σ_k to $\sigma_i(x_p) = -\sum_{j=1}^{p-1} a_j \sigma_i(x_j)$ to get:

$$(\sigma_k\sigma_i)(x_p) = -\sum_{j=1}^{p-1} \sigma_k(a_j)(\sigma_k\sigma_i)(x_j), \qquad \text{for every } 1 \leq i \leq n.$$

Now left multiplication by σ_k is a permutation of Γ. So we get:

$$\sigma_q(x_p) = -\sum_{j=1}^{p-1} \sigma_k(a_j)\sigma_q(x_j), \qquad \text{for every } 1 \leq q \leq n.$$

Subtracting from the original relation, we get:

$$0 = \sum_{j=1}^{p-1} (\sigma_k(a_j) - a_j)\sigma_q(x_j), \qquad \text{for every } 1 \leq q \leq n.$$

Thus we obtain a non–zero (since $\sigma_k(a_\ell) \neq a_\ell$) element of $\operatorname{Ker}(X)$ with strictly less than $p-1$ non–zero entries. □

Corollary. *Let L/K be a finite extension. Then it is a Galois extension if and only if $|\mathsf{G}(L/K)| = [L : K]$.*

(29.5) Algebraic Galois extensions.– Let L/K be an algebraic extension. The following result gives algebraic characterization for L/K to be a Galois extension.

Theorem. *An algebraic extension L/K is Galois if and only if for every $\alpha \in L$, its minimal polynomial* $\mathsf{m}_\alpha(x) \in K[x]$ *has* $\deg(\mathsf{m}_\alpha(x))$ *distinct roots in L.*

PROOF. Let $\Gamma = \mathsf{G}(L/K)$. Assume that L/K is Galois, that is, $L^\Gamma = K$. Let $\alpha \in L$ and $\mathsf{m}_\alpha(x) \in K[x]$ its minimal polynomial. Let $n = \deg(\mathsf{m}_\alpha(x))$.

Consider the Γ–orbit of α.

$$\Gamma\alpha = \{\sigma(\alpha) : \sigma \in \Gamma\} \subset L.$$

Note that for every $\sigma \in \Gamma$, $\sigma(\alpha)$ is another root of $\mathsf{m}_\alpha(x)$. Since number of roots of a polynomial $\leq$ degree of that polynomial, we conclude that $\Gamma\alpha$ is finite and has at most n elements.

Define $f(x) = \prod_{\beta \in \Gamma\alpha} (x - \beta)$. Since $f(x)$ is invariant under Γ, we have $f(x) \in K[x]$. Moreover, it divides $\mathsf{m}_\alpha(x)$ whose irreducibility implies that $\deg(f) = n$. That is $|\Gamma\alpha| = n$ consists of n distinct roots of $\mathsf{m}_\alpha(x)$.

Let us prove the converse now. Note that the assumption on L/K implies two statements.

- L is the splitting extension of the following set of (irreducible, monic) polynomials.

$$L = \mathcal{E}(P, K), \qquad \text{where, } P = \{\mathsf{m}_\alpha(x) : \alpha \in L\} \subset K[x].$$

- Every $f(x) \in P$ has distinct roots in L.

Assume $\alpha \in L \setminus K$. We will exhibit an element $\sigma \in \Gamma$ such that $\sigma(\alpha) \neq \alpha$. Note that $n = \deg(\mathsf{m}_\alpha(x)) \geq 2$, therefore there exists $\beta \neq \alpha$ also a root of $\mathsf{m}_\alpha(x)$. By Theorem 26.0, there exists an isomorphism $\overline{\sigma} : K(\alpha) \xrightarrow{\sim} K(\beta)$ uniquely determined by $\overline{\sigma}|_K = \mathrm{Id}_K$ and $\overline{\sigma}(\alpha) = \beta$. By the same theorem, part (2), $\overline{\sigma}$ extends to an element $\sigma \in \mathsf{G}(L/K)$, since L/K is a splitting extension. Thus, we have shown the existence of $\sigma \in \mathsf{G}(L/K)$ such that $\sigma(\alpha) = \beta \neq \alpha$. □

(29.6) Separable polynomials and normal extensions.– Let us record the two important properties listed in the proof of the theorem given above.

Definition. Let K be a field and $f(x) \in K[x]$ be a polynomial. We say $f(x)$ is *separable* if all its roots (in its splitting extension, for instance) are distinct.

An extension L/K is called *separable* if it is algebraic and for every $\alpha \in L$, its minimal polynomial $\mathsf{m}_\alpha(x)$ is separable.

An extension L/K is called *normal* if it is algebraic and for every $\alpha \in L$, its minimal polynomial $\mathsf{m}_\alpha(x)$ splits as a product of linear terms in $L[x]$. That is, L is the splitting extension of $\{\mathsf{m}_\alpha(x) : \alpha \in L\}$.

Theorem 29.5 is often phrased as *Galois if and only if separable and normal.* Note that there exist fields F over which irreducible polynomials are not necessarily separable. We will discuss such F (called *imperfect fields*) next time.

(29.7) Example.– Recall that last time we defined $\mathbb{Q}(\mu_n) \subset \mathbb{C}$, where

$$\mu_n = \left\{ e^{\frac{2\pi k\iota}{n}} : 0 \le k \le n-1 \right\}.$$

We saw that $|\mathsf{G}\left(\mathbb{Q}(\mu_n)/\mathbb{Q}\right)| = \phi(n)$, where

$$\phi(n) = \left|\{1 \le k \le n-1 : \gcd(k,n) = 1\}\right|, \quad \text{Euler's } \phi \text{ function.}$$

It is immediate that $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is Galois. By Corollary 29.4, we have:

$$[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \phi(n).$$