MATH 416, Modern Algebra II

Volodymyr Nekrashevych

2020, April 7

Primitive Element Theorem

Theorem 1

Let E be a finite separable extension of a field F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.

Proof: If F is finite, then E is also finite. We know that then the multiplicative group $E^* = E \setminus \{0\}$ is cyclic. Let $\alpha \in E$ be its generator. Then every element of E^* is of the form α^n, so $E = F(\alpha)$.

Suppose now that F is infinite. It is enough to prove that for any extension $F(\beta, \gamma)$ there exists $\alpha \in F(\beta, \gamma)$ such that $F(\beta, \gamma) = F(\alpha)$, and then use induction. Let $\beta = \beta_1, \beta_2, \ldots, \beta_n$ be the roots of the irreducible polynomial $f(x) \in F[x]$ with root β. Let $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_m$ be the roots of the irreducible polynomial $g(x) \in F[x]$ with root γ. (All are considered to be elements of $\overline{F}$.)

Since F is infinite, we can find $a \in F$ such that $a \neq (\beta_i - \beta)/(\gamma - \gamma_j)$ for any i, j with $j \neq 1$. Denote $\alpha = \beta + a\gamma$. We have then $\alpha = \beta + a\gamma \neq \beta_i + a\gamma_j$, so $\alpha - a\gamma_j \neq \beta_i$. Consider $h(x) = f(\alpha - ax) \in F(\alpha)[x]$. Then $h(\gamma) = f(\beta) = 0$. However, $h(\gamma_j) \neq 0$ for $j \neq 1$, since β_i are the only roots of $f(x)$, so $\alpha - a\beta_i$ are the only roots of $h(x)$. The irreducible polynomial $r(x) \in F(\alpha)[x]$ with the root γ must divide $h(x)$ and $g(x)$, since both of them have γ as a root. But the only common root in $\overline{F}$ of $g(x)$ and $h(x)$ is γ. Consequently, $r(x) = x - \gamma$, i.e., $\gamma \in F(\alpha)$. It follows that also $\beta = \alpha - a\gamma \in F(\alpha)$, so that $F(\beta, \gamma) = F(\alpha)$.

Example

Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. It must be simple, since $\mathbb{Q}$ is perfect. We can check that, for example, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. We have $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, so $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Then $\sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, therefore $2\sqrt{3} + 3\sqrt{2} - 2(\sqrt{2} + \sqrt{3}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and then $\sqrt{2} + \sqrt{3} - \sqrt{2} = \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Normal Extensions

Definition 1

A finite extension $F \subseteq E$ is a *finite normal extension* if it is separable and splitting.

Theorem 2

Consider a chain of extensions $F \subseteq E \subseteq K$. Suppose that $F \subseteq K$ is a finite normal extension. Then $E \subseteq K$ is a finite normal extension. The group $G(K/E)$ coincides with the subgroup of those elements σ of $G(K/F)$ that fix every element of E. Two elements $\sigma, \tau \in G(K/F)$ induce the same isomorphism $E \mapsto \sigma(E) = \tau(E)$ if and only if they are in the same coset of $G(K/E)$ in $G(K/F)$.

Proof: The field K is generated by F and all the roots of some set $P \subset F[x]$. Hence it is generated by $E \supseteq F$ and all the roots of the same set $P \subset F[x] \subseteq E[x]$. If every element of K is a root of a polynomial $f(x) \in F[x]$ with no multiple roots, then it is a root of $f(x) \in F[x] \subseteq E[x]$ with no multiple roots. It follows that $E \subseteq K$ is a normal extension. The group $G(K/E)$ is a subgroup of $G(K/F)$ because any automorphism fixing every element of E fixes every element of $F \subseteq E$. Two elements $\sigma, \tau \in G(K/F)$ define the same isomorphism from E if and only if $\sigma^{-1} \circ \tau$ is the identity automorphism of E, i.e., belongs to $G(K/E)$. But $\sigma^{-1}\tau \in G(K/E)$ is equivalent to $\tau G(K/E) = \sigma G(K/E)$.

Main Theorem of Galois Theory

Theorem 3

Let $F \subseteq K$ be a finite **normal** *extension. Then we have a bijection $E \mapsto G(K/E)$ between the set of intermediate fields $\{E : F \subseteq E \subseteq K\}$ and the set of subgroups of $G(K/F)$. The inverse of this bijection is the map $H \mapsto K_H = \{x \in K : \sigma(x) = x, \forall \sigma \in H\}$. We call these bijection the* **Galois correspondence**. *It has the following properties.*

1. *The described maps are inverse to each other, i.e., $E = K_{G(K/E)}$ for every intermediate field E, and $H = G(K/K_H)$ for every subgroup $H \leq G(K/F)$.*
2. $[K : E] = |G(K/E)|$ *and* $[E : F] = [G(K/F) : G(K/E)]$.
3. *E is a normal extension of F if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$. If it is so, then $G(E/F) \cong G(K/F)/G(K/E)$.*
4. *The Galois correspondence is order-inverting: If $E_1 \subset E_2$, then $G(K/E_1) > G(K/E_2)$.*

Proof

We have $E \subseteq K_{G(K/E)}$, because every element $\sigma \in G(K/E)$ fixes every element of E, by definition. Suppose that $\alpha \in K \setminus E$. Then there is an automorphism σ of $\overline{E}$ fixing E and moving α to another conjugate element. But K is a splitting field, so every automorphism of $\overline{E}$ fixing E leaves K invariant, so $\sigma \in G(K/E)$ and $\sigma(\alpha) \neq \alpha$, so $\alpha \notin K_{G(K/E)}$. This shows that every element of $K_{G(K/E)}$ must be an element of E, i.e., that $E = K_{G(K/E)}$. We have shown $E \mapsto G(K/E) \mapsto K_{G(K/E)} = E$. This does not show yet that the Galois correspondence is a bijection, since it is possible that not all subgroups of $G(K/F)$ are of the form $G(K/E)$ for some E.

Proof

We have already proved $[K:E] = \{K:E\} = |G(K/E)|$ for normal extensions. (The first equality is separability, the second one is being a splitting extension.) We proved $[E:F] = [G(K/F):G(K/E)]$ in the previous theorem.

Let $H \leq G(K/F)$. We know that $H \leq G(K/K_H)$, by definition. Suppose that $H < G(K/K_H)$, i.e., that $|H| < |G(K/K_H)| = [K:K_H]$. By the Primitive Element Theorem, $K = K_H(\alpha)$ for some $\alpha \in K$. Consider $f(x) = \prod_{\sigma \in H}(x - \sigma(\alpha))$. Every element $\sigma \in H$ will just permute the factors, so $\sigma(f) = f$, hence $f(x) \in K_H[x]$. Its degree is $|H|$. But the degree of the irreducible polynomial $g(x) \in K_H[x]$ with root α is equal to $[K:K_H]$. We must have $g(x)|f(x)$, which is a contradiction. It follows that $H = G(K/F)$, which finishes the proof that the Galois correspondence is a bijection.

Proof

It remains to prove property (3). For every intermediate field $F \subseteq E \subseteq K$, the field E is a separable extension of F. It is normal if and only if E is splitting over F. To be splitting is equivalent to the condition that every isomorphism from E fixing F is an automorphism of E. Every such an isomorphism is an automorphism of K (since $F \subseteq K$ is splitting). Hence, $F \subseteq E$ is normal if and only if $\sigma(E) = E$ for every $\sigma \in G(E/F)$. Suppose that $F \subseteq E$ is normal. Let $\sigma \in G(K/F)$ and $\tau \in G(K/E)$. Then $\sigma^{-1}\tau\sigma$ is the identity automorphism of E, since $\sigma(E) = E$, so $\tau\sigma(\alpha) = \sigma(\alpha)$ for every $\alpha \in E$, hence $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. This shows that $\sigma^{-1}\tau\sigma \in G(K/E)$ for every $\tau \in G(K/F)$ and $\sigma \in G(K/E)$, i.e., that $G(K/E) \trianglelefteq G(K/F)$. Conversely, suppose that $G(K/E) \trianglelefteq G(K/F)$. We have to show that $\sigma(E) = E$ for every $\sigma \in G(K/F)$. Let $\alpha \in E$. Let $\tau \in G(K/E)$. Then $\tau(\sigma(\alpha)) = \sigma(\sigma^{-1}\tau\sigma(\alpha))$. But $\sigma^{-1}\tau\sigma \in G(K/E)$, so $\sigma^{-1}\tau\sigma(\alpha) = \alpha$. It follows that $\tau(\sigma(\alpha)) = \sigma(\alpha)$ for every $\tau \in G(K/E)$, i.e., that $\sigma(\alpha) \in K_{G(K/E)} = E$.

Proof

It remains to show that if $F \subseteq E$ is normal, then $G(E/F) \cong G(K/F)/G(K/E)$. ...