

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Lemma: Suppose that E/\mathbb{R} is a proper finite extension. Then $2 \mid [E : \mathbb{R}]$.

Proof: Suppose not. Let $\alpha \in E \setminus \mathbb{R}$, and let $f(x) = \text{Irr}(\alpha, \mathbb{R})$. Assume that $[E : \mathbb{R}]$, and hence $\deg f(x)$, is odd. But $f(x)$ being of odd degree means that it must cross the x axis by the intermediate value theorem. Hence $f(x)$ has a real root, contradicting $f(x)$ being irreducible.

Lemma: If E/\mathbb{C} is a finite extension, then $[E : \mathbb{C}] \neq 2$.

Proof: Suppose that $[E : \mathbb{C}] = 2$. Then $E = \mathbb{C}(\alpha)$ for some $\alpha \in E$. Let $f(x) = x^2 + bx + c = \text{Irr}(\alpha, \mathbb{C})$. Thus

$$\begin{aligned} 0 &= \alpha^2 + b\alpha + c = \alpha^2 + b\alpha + \frac{b^2}{4} + c - \frac{b^2}{4} \\ &= \left(\alpha + \frac{b}{2}\right)^2 - \left(\frac{b^2}{4} - c\right) \\ &= \beta^2 - d \end{aligned}$$

where $\beta = \alpha + \frac{b}{2}$ and $d = \frac{b^2}{4} - c$. Note that $\mathbb{C}(\alpha) = \mathbb{C}(\beta)$ and $\text{Irr}(\beta, \mathbb{C}) = x^2 - d$. But let $d = re^{i\theta}$ where $r \in \mathbb{R}^{\geq 0}$. Then $\sqrt{r}e^{i\theta/2}$ is a root of $x^2 - d$, a contradiction (Here we use the fact that every positive real number has a real square root).

Fundamental Theorem Of Algebra: \mathbb{C} is algebraically closed.

Proof: Let α be an algebraic element over \mathbb{C} . Hence α is algebraic over \mathbb{R} . Let $f(x) = \text{Irr}(\alpha, \mathbb{R})$. Let E be the splitting field of $f(x)(x^2 + 1)$ over \mathbb{R} . Then E/\mathbb{R} is Galois and $\mathbb{C} \subseteq E$ and $\alpha \in E$. We wish to show that $E = \mathbb{C}$. Let $G = \text{Gal}(E/\mathbb{R})$. By lemma 1, $2 \mid |G|$. Let H be a Sylow 2-subgroup of G and let $L = E_H$. Then $[L : \mathbb{R}] = [G : H]$. By lemma 1, $[L : \mathbb{R}]$ and hence $L = \mathbb{R}$ (because we have all the powers of 2 in L). Therefore $G = H$ and so $|G| = 2^n$. Let $P = \text{Gal}(E/\mathbb{C})$. Then $|P| = 2^{n-1}$, since $[E : \mathbb{C}] = \frac{[E:\mathbb{R}]}{[\mathbb{C}:\mathbb{R}]}$. If $P \neq \{1\}$, by Sylow, there exists a subgroup Q of P of order 2^{n-2} . But then $[E_Q : \mathbb{C}] = 2$, contradicting lemma 2. Hence $P = \{1\}$. Therefore, $n = 1$ and $|G| = 2$, so that $E = \mathbb{C}$.

Definition: Let $f(x) \in F[x]$ whose irreducible factors over F are separable. The Galois group of $f(x)$ over F , denoted $\text{Gal}_F(f)$ is $\text{Gal}(E/F)$ where E is the splitting field of $f(x)$ over F .

Remark: We've shown that if $\deg f = n$, then $\text{Gal}_F(f)$ is isomorphic to a subgroup of S_n . When can $\text{Gal}_F(f) \cong S_n$?

Lemma: Let p be a prime and H a subgroup of S_p which contains a transposition and a p -cycle. Then $H = S_p$. (Note that S_n is always generated by $(1\ 2)$ and $(1\ 2\ \dots\ n)$).

Proof: Let $\tau \in H$ be a transposition. We can assume $\tau = (1\ 2)$. Let $\sigma \in H$ be a p -cycle. As $|\sigma^i| = p$ for any $1 \leq i \leq p-1$ and any element of order p in S_p is a p -cycle, we get that σ^i is a p -cycle for all $i \in \{1, \dots, p-1\}$. Consider $S = \{\sigma(1), \sigma^2(1), \dots, \sigma^p(1)\}$. I claim that $|S| = p$. If not, then $\sigma^i(1) = \sigma^j(1)$ for some $i > j$ and hence $\sigma^{i-j}(1) = 1$, a contradiction as σ^{i-j} is a p -cycle. As $|S| = p$, $2 \in S$, i.e. there exists an i such that $\sigma_i(1) = 2$. Replacing σ by σ_i , we can assume that $\sigma = (1\ 2\ 3\ \dots\ p)$. Note that $\sigma(1\ 2)\sigma^{-1} = (2\ 3) \in H$. In general, we have that $\sigma(i-1\ i)\sigma^{-1} = (i\ i+1)$. Hence we have that $H = S_p$.

Theorem: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p a prime and suppose f has exactly 2 real non-real roots. Then $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$.

Proof: We've shown that $G \cong \text{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_p . Let E be the splitting field of $f(x)$ and let $\sigma : E \rightarrow E$ be given by complex conjugation. Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ and say α_1, α_2 are the non-real roots. Then $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_1$, and $\sigma(\alpha_i) = \alpha_i$ for all $i \neq 1, 2$. Hence σ is a transposition. So, note that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p$ since $\deg f = p$ and f was irreducible. Therefore, $p \mid [E : \mathbb{Q}] = |G|$. Hence G has an element of order p . However, the only elements of order p in S_p are p -cycles since p is prime. Therefore, by the previous lemma, we have that $G = S_p$.

Example: Let $f(x) = x^5 - 2x^3 - 8x - 2$. Then $f(x)$ is irreducible by Eisenstein. Note that $f'(x) = (5x^2 + 4)(x^2 - 2)$ so that $f(x)$ has exactly three real roots and two complex roots. Therefore, by the above theorem, we have that $\text{Gal}_{\mathbb{Q}}(f) = S_5$.

Definition: Let K be a field and t_1, \dots, t_n be indeterminants over K . Then the general equation of degree n over K is

$$f_n(x) = x^n + t_1x^{n-1} + \dots + t_{n-1}x + t_n$$

So, what is $\text{Gal}_{K(t_1, \dots, t_n)}(f_n)$. (My guess was S_n).

Definition: Let K be a field and t_1, \dots, t_n be indeterminants over K . Let $F = K(t_1, \dots, t_n)$. For each permutation $\sigma \in S_n$, define a map

$$\begin{aligned} \tilde{\sigma} : F &\rightarrow F \\ \frac{p(t_1, \dots, t_n)}{q(t_1, \dots, t_n)} &\mapsto \frac{p(t_{\sigma(1)}, \dots, t_{\sigma(n)})}{q(t_{\sigma(1)}, \dots, t_{\sigma(n)})} \end{aligned}$$

For example, if $n = 3$ and $\sigma = (1\ 2\ 3)$, then $\tilde{\sigma} \left(\frac{2x_1^2x_2 - x_3^3}{x_2x_3 + 5x_2} \right) = \frac{2x_2^2x_3 - x_1^3}{x_3x_1 + 5x_3}$. Then $\tilde{\sigma}$ are automorphisms of F (check this!). In this way, we can think of S_n to be a group of automorphisms of F that fix K . Let $L = F_{S_n}$ be the fixed field of S_n . Things that are in L are $x_1x_2 \cdots x_n$, $x_1 + x_2 + \dots + x_n$, and generally $\sum_{i < j} x_i x_j$ (in fact, these generate L over K). L is called the **field of symmetric rational functions**. Note that by Artin's Theorem, $[F : F_{S_n}] = |S_n| = n!$. Also, F/L is Galois and $\text{Gal}(F/L) \cong S_n$.

To investigate the elements of L , let $f(x) = \prod_{i=1}^n (x - t_i) \in F[x]$. For $\sigma \in S_n$, $f_{\sigma}(x) = \prod_{i=1}^n (x - t_{\sigma(i)}) = f(x)$. Hence $f(x) \in L[x]$. Writing out what $f(x)$ is, we have

$$f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \dots + (-1)^n s_n$$

where $s_1 = t_1 + \dots + t_n$, $s_2 = \sum_{i < j} t_i t_j$, etc. s_i is called the **i th elementary symmetric polynomial** and $s_i \in L$.

Theorem: $L = K(s_1, \dots, s_n)$.

Proof: Note that we have the diagram:

$$\begin{array}{c} F \\ \left| \vphantom{F} \right. \\ n! \\ L \\ \left| \vphantom{L} \right. \\ K(s_1, \dots, s_n) \end{array}$$

So, it is enough to show that $[F : K(s_1, \dots, s_n)] \leq n!$. Note that F is the splitting field for $f(x)$ over $K(s_1, \dots, s_n)$. Hence, as $f(x)$ has degree n , the splitting field has degree at most $n!$ over $K(s_1, \dots, s_n)$, as desired.

Corollary: Let $F = K(t_1, \dots, t_n)$, where the t_i are indeterminants over K . Let s_i be the i th elementary symmetric polynomial in the t s. Then $F/K(s_1, \dots, s_n)$ is Galois and $\text{Gal}(F/K(s_1, \dots, s_n)) \cong S_n$.

Theorem: Let $F = K(t_1, \dots, t_n)$ where t_i are indeterminants over K and let $f(x) = x^n + t_1x^{n-1} + \dots + t_{n-1}x + t_n$ be the general equation of degree n . Then $\text{Gal}_F(f) \cong S_n$.

Proof: Let E be the splitting field for $f(x)$ over F , and let y_1, \dots, y_n be the roots of $f(x)$ in E . So, $E = F(y_1, \dots, y_n)$, and $f(x) = \prod_{i=1}^n (x - y_i) \in E[x]$. Note that $t_i = (-1)^i s_i(y_1, \dots, y_n)$. Consider the following diagram (where the x_i are indeterminants over K , and the s_i are the elementary symmetric polynomials in the x 's, notation is our worst enemy on this problem):

$$\begin{array}{ccc} K[x_1, \dots, x_n] & \xrightarrow{\tau} & K[y_1, \dots, y_n] \\ \left| \right. & & \left| \right. \\ K[s_1, \dots, s_n] & \xleftarrow{\pi} & K[t_1, \dots, t_n] \end{array}$$

Where π sends t_i to $(-1)^i s_i$ and τ sends y_1 to x_i . Let $p(\underline{t}) \in K[\underline{t}]$. Then we have that $\tau\pi(p(\underline{t})) = \tau(p(-s_1(\underline{x}), \dots, (-1)^n s_n(\underline{x}))) = p(-s_1(\underline{y}), \dots, (-1)^n s_n(\underline{y})) = p(\underline{t})$. Hence, $\tau\pi = \text{Id}_{K[t_1, \dots, t_n]}$, and therefore π is 1-1 hence an isomorphism (as it is clearly surjective). Therefore, the induced map on quotient fields (say $\tilde{\pi}$) is also an isomorphism. Recall that $E = K(y_1, \dots, y_n) = F(y_1, \dots, y_n)$ is the splitting field for $f(x)$ over $K(t_1, \dots, t_n)$. But $K(x_1, \dots, x_n)$ is the splitting field for $f^{\tilde{\pi}}(x)$, as the x_i were the roots of the symmetric polynomial. In summary, we have the picture

$$\begin{array}{ccc} K(x_1, \dots, x_n) & \xrightarrow{\tau} & K(y_1, \dots, y_n) \\ \left| \right. & & \left| \right. \\ K(s_1, \dots, s_n) & \xleftarrow{\tilde{\pi}} & K(t_1, \dots, t_n) \end{array}$$

Where the vertical containments are splitting fields of the aforementioned polynomials. So, by the uniqueness of splitting fields, there exists the isomorphism τ as above. Therefore, we have that $\text{Gal}_F(f(x)) = \text{Gal}(K(y_1, \dots, y_n)/K(t_1, \dots, t_n)) \cong \text{Gal}(K(x_1, \dots, x_n)/K(s_1, \dots, s_n)) \cong S_n$ where the last isomorphism is given by the previous theorem.