MATH200C, LECTURE 1

GOLSEFIDY

Galois extensions.

Lemma 1. *Suppose E/F is a finite extension and $\sigma : F \to E$ is an embedding. Let* $\mathrm{Isom}_\sigma(E,E) := \{\widehat{\sigma} : E \to E | \ \widehat{\sigma}|_F = \sigma\}$. *Then*

$$|\mathrm{Isom}_\sigma(E,E)| \le [E:F];$$

in particular $|\operatorname{Aut}(E/F)| \le [E:F]$.

Proof. We have already proved this for the case when E is a splitting field of a polynomial. The same argument gives us the above result. We proceed by the strong induction on $[E:F]$. Suppose $\alpha \in E \setminus F$; let

$$\mathrm{Embed}_\sigma(F[\alpha],E) := \{\widetilde{\sigma} : F[\alpha] \to E | \ \widetilde{\sigma}|_F = \sigma\}.$$

Then

$$|\mathrm{Embed}_\sigma(F[\alpha],E)| = \#\text{ of distinct zeros of } \sigma(m_{\alpha,F}(x)) \text{ in } E \le [F[\alpha]:F].$$

And so

$$\begin{aligned}
|\mathrm{Isom}_\sigma(E,E)| &= \sum_{\widetilde{\sigma} \in \mathrm{Embed}_\sigma(F[\alpha],E)} |\mathrm{Isom}_{\widetilde{\sigma}}(E,E)| \\
&\le \sum_{\widetilde{\sigma} \in \mathrm{Embed}_\sigma(F[\alpha],E)} [E:F[\alpha]] \qquad \text{(induction hypothesis)} \\
&\le [F[\alpha]:F][E:F[\alpha]] = [E:F]
\end{aligned}$$

□

Theorem 2. *Suppose E/F is a finite field extension; then the following statements are equivalent:*

(1) E is a splitting field of a separable polynomial over F.
(2) $|\operatorname{Aut}(E/F)| = [E:F]$.
(3) E/F is a normal separable extension.

Proof. (1) $\Rightarrow$ (2), we have already proved. (2) $\Rightarrow$ (3) Suppose $\alpha \in E$; then

$$|\mathrm{Embed}_{\mathrm{id}_F}(F[\alpha], E)| = \#\text{ of distinct zeros of } m_{\alpha,F}(x) \text{ in } E,$$

and

$$\begin{aligned} |\operatorname{Aut}(E/F)| &= \sum_{\sigma\in \mathrm{Embed}(F[\alpha],E)} |\mathrm{Isom}_\alpha(E,E)| \\ &\le \sum_{\sigma\in \mathrm{Embed}(F[\alpha],E)} [E:F[\alpha]] && \text{(The above lemma)} \\ &= (\#\text{ of distinct zeros of } m_{\alpha,F}(x) \text{ in } E)(F[\alpha],E) \\ &\le [F[\alpha]:F][E:F[\alpha]] = [E:F]. \end{aligned}$$

Since by our assumption equality holds we have

$$\#\text{ of distinct zeros of } m_{\alpha,F}(x) \text{ in } E = [F[\alpha]:F] = \deg m_{\alpha,F}(x).$$

Hence all the zeros of $m_{\alpha,F}$ are in E and they are distinct. Hence E/F is a normal separable extension.

(3) $\Rightarrow$ (1) Suppose $\alpha_1,\ldots,\alpha_n$ is an F-basis of E. Then E is a splitting field of $f(x) := \prod_{i=1}^n m_{\alpha_i,F}(x)$ as E/F is a normal extension. Since E/F is a separable extension, $m_{\alpha_i,F}(x)$ does not have multiple zeros in E and they are irreducible factors of $f(x)$ in $F[x]$; and so $f(x)$ is a separable polynomial. □

Definition 3. *An algebraic extension E/F is called a Galois extension if E/F is a normal separable extension. When E/F is a Galois extension, we write* $\mathrm{Gal}(E/F)$ *instead of* $\mathrm{Aut}(E/F)$.

We have seen that if E/F is a finite Galois extension, then $\mathrm{Gal}(E/F)$ determines $[E:F]$. Next we will see that knowing $\mathrm{Gal}(E/F)$ as a subgroup $\mathrm{Aut}(E)$ uniquely determines F. The following is the key technical lemma.

Lemma 4. *Suppose G is a finite group of* $\mathrm{Aut}(E)$. *Suppose V is a non-zero E-subspace of E^n. Suppose for $\sigma \in G$ and $v := (a_1,\ldots,a_n) \in V$ we have that $\sigma(v) := (\sigma(a_1),\ldots,\sigma(a_n)) \in V$. Then*

$$V^G := \{v \in V | \forall \sigma \in G, \sigma(v) = v\} \neq 0.$$

Proof. Suppose $v \in V$ has the smallest number of non-zero components among the non-zero elements of V. After reordering its components we can assume that $v = (a_1,\ldots,a_k,0\ldots,0)$ for some $a_i \in E^\times$. Since V is an E-subspace, $a_1^{-1}v \in V$.

So W.L.O.G. we can and will assume that the first component of v is 1. Next we show that $v \in V^G$; and so $V^G \neq 0$.

For any $\sigma \in G$, we have $\sigma(v) - v = (0, \sigma(a_2) - a_2, \ldots, \sigma(a_k) - a_k, 0, \ldots, 0)$ has at most $k-1$ non-zero components. Since k is the smallest number of non-zero components of non-zero elements of V and $\sigma(v) - v \in V$, we deduce that $\sigma(v) - v = 0$; and claim follows. □

Lemma 5. *Suppose G is a finite group of* $\mathrm{Aut}(E)$*. Then*

(1) $\mathrm{Fix}(G) := \{e \in E | \, \forall \sigma \in G, \sigma(e) = e\}$ *is a subfield of E.*

(2) $[E : \mathrm{Fix}(G)] \leq |G|$.

Proof. (1) is clear. (2) Suppose $|G| = n$ and $G = \{\sigma_1, \ldots, \sigma_n\}$. It is enough to show that any $n+1$ elements of E are F-linearly dependent where $F := \mathrm{Fix}(G)$. Suppose $\alpha_1, \ldots, \alpha_{n+1}$ are $n+1$ arbitrary elements of E. We have to show that there are $c_1, \ldots, c_{n+1} \in F$ such that $c_1\alpha_1 + \cdots + c_{n+1}\alpha_{n+1} = 0$. If there are such c_i's, for any j we get

$$0 = \sigma_j(c_1\alpha_1 + \cdots + c_{n+1}\alpha_{n+1}) = c_1\sigma_j(\alpha_1) + \cdots + c_{n+1}\sigma_j(\alpha_{n+1});$$

and so $v := (c_1, \ldots, c_{n+1})$ will be in the left kernel of the matrix $[\sigma_j(\alpha_i)]$; that means

$$\begin{pmatrix} c_1 & \cdots & c_{n+1} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_{n+1}) & \cdots & \sigma_n(\alpha_{n+1}) \end{pmatrix} = 0.$$

Let $V \subseteq E^{n+1}$ be the left kernel of the above matrix. We need to show that $V \cap F^{n+1} \neq 0$. Notice that $V \cap F^{n+1}$ is the set V^G of fixed points of G in V. Therefore by the previous lemma, it is enough to show $V \neq 0$ and V is G-invariant. Since V is the left kernel of an $(n+1) \times n$ matrix, it is a non-zero E-subspace of E^{n+1}.

Suppose $v \in V$ and $\sigma \in G$; then $v[\sigma_j(\alpha_i)] = 0$ implies that $\sigma(v)[(\sigma \circ \sigma_j)(\alpha_i)] = 0$. This is equivalent to say $(\sigma(v))((\sigma \circ \sigma_k)(\alpha_1, \ldots, \alpha_{n+1})^T) = 0$ for any $1 \leq k \leq n$. Notice that $\{\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_n\}$ is just a permutation of $\{\sigma_1, \ldots, \sigma_n\}$. Hence for any $1 \leq k \leq n$, we have $(\sigma(v))(\sigma_k(\alpha_1, \ldots, \alpha_{n+1})^T) = 0$, which is equivalent to say $\sigma(v) \in V$. Thus V is invariant under the action of G; and claim follows. □

Theorem 6. *Suppose G is a finite subgroup of* $\mathrm{Aut}(E)$*. Then (1)* $E/\mathrm{Fix}(G)$ *is a Galois extension, and (2)* $\mathrm{Gal}(E/\mathrm{Fix}(G)) = G$*.*

Proof. Let $F := \mathrm{Fix}(G)$. By the previous lemma, $[E : F] \le |G|$; and so it is a finite extension. Hence by an earlier lemma, we have $|\mathrm{Aut}(E/F)| \le [E : F]$. And it is clear that $G \subseteq \mathrm{Aut}(E/F)$. So overall we have

$$|G| \le |\mathrm{Aut}(E/F)| \le [E : F] \le |G|.$$

Thus all equalities should hold. This implies that $|\mathrm{Aut}(E/F)| = [E : F]$ and $|\mathrm{Aut}(E/F)| = |G|$. Hence E/F is a Galois extension and $\mathrm{Aut}(E/F) = G$. □

During lecture we gave an alternative argument to show E/F is a normal extension. Since the idea behind that argument is useful, it is reproduced here: for $\alpha \in E$, let $f_\alpha(x) := \prod_{\sigma\in G}(x - \sigma(\alpha))$. As any element of G only permutes the linear factors of $f_\alpha(x)$, we get that for any $\sigma \in G$, $\sigma(f_\alpha) = f_\alpha$. Hence $f_\alpha(x) \in \mathrm{Fix}(G)[x] = F[x]$. Since $f_\alpha(\alpha) = 0$, we deduce that $m_{\alpha,F}(x)|f_\alpha(x)$. Thus zeros of $m_{\alpha,F}(x)$ are among the G-orbit of α; and so all of them are in E. This implies that E/F is a normal extension.

Corollary 7. *Suppose E/F is a finite Galois extension. Then*

$$\mathrm{Fix}(\mathrm{Gal}(E/F)) = F.$$

Proof. Let $F' := \mathrm{Fix}(\mathrm{Gal}(E/F))$. Then by the above Theorem E/F' is a Galois extension and $\mathrm{Gal}(E/F') = \mathrm{Gal}(E/F)$. Hence

$$[E : F] = |\mathrm{Gal}(E/F)| = |\mathrm{Gal}(E/F')| = [E : F']. \tag{1}$$

It is also clear that $F \subseteq \mathrm{Fix}(\mathrm{Gal}(E/F)) = F'$. Therefore by (1) we have that $[F' : F] = 1$; and claim follows. □

So far we have proved the following:

Theorem 8. *Suppose E/F is a finite extension. Then the following statements are equivalent:*

1. *E is a splitting field of a separable polynomial over F.*
2. *$|\mathrm{Aut}(E/F)| = [E : F]$.*
3. *E/F is a Galois extension.*
4. *$F = \mathrm{Fix}(\mathrm{Aut}(E/F))$.*
5. *$F = \mathrm{Fix}(G)$ for some finite subgroup G of $\mathrm{Aut}(E)$.*