# Math200b, lecture 20

Golsefidy

## Normal extensions.

In the previous lecture we were proving the following theorem:

**Theorem 1** *Suppose* $F$ *is a field,* $\overline{F}$ *is an algebraic closure of* $F$*, and* $F \subseteq E \subseteq \overline{F}$ *is a subfield. Then the following statements are equivalent.*

1. *For any* $\sigma \in \mathrm{Aut}(\overline{F}/F)$*,* $\sigma(E) = E$*.*

2. *For any* $\alpha \in E$*, there are* $\alpha_i \in E$ *such that*

$$m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \alpha_i).$$

3. *There is a non-empty subset* $\mathcal{F}$ *of* $F[x] \setminus F$ *such that* $E$ *is a splitting field of* $\mathcal{F}$ *over* $F$*.*

4. *There is a family* $\{E_i\}_{i\in I}$ *of subfields of* $\overline{F}$*, and a family of polynomials* $\{p_i\}_{i\in I} \subseteq F[x] \setminus F$ *such that*

   (a) $E_i \subseteq \overline{F}$ *is a splitting field of* $p_i(x)$.

   (b) *For any* $i, j \in I$, *there is* $k \in I$ *such that* $E_i \cup E_j \subseteq E_k$.

   (c) $E = \bigcup_{i\in I} E_i$.

*Proof.* (Continue) (4)⇒(1). For any $\sigma \in \mathrm{Aut}(\overline{F}/F)$ and any $i \in I$, we have already proved that $\sigma(E_i) = E_i$; and so

$$\sigma(E) = \bigcup_{i\in I} \sigma(E_i) = \bigcup_{i\in I} E_i = E.$$

■

**Theorem 2** *Suppose* $\overline{F}$ *is an algebraic closure of* $F$, $F \subseteq E \subseteq \overline{F}$ *is a subfield, and* $E/F$ *is a normal extension. Then the restriction map* $r_E : \mathrm{Aut}(\overline{F}/F) \longrightarrow \mathrm{Aut}(E/F)$, $r_E(\sigma) := \sigma|_E$ *is a well-defined onto group homomorphism, and* $\ker r_E = \mathrm{Aut}(\overline{F}/E)$*; in particular we have and* $\mathrm{Aut}(\overline{F}/E) \trianglelefteq \mathrm{Aut}(\overline{F}/F)$ *and*

$$\mathrm{Aut}(E/F) \simeq \mathrm{Aut}(\overline{F}/F)/\mathrm{Aut}(\overline{F}/E).$$

*Proof.* Since $E/F$ is a normal extension, for any $\sigma \in \mathrm{Aut}(\overline{F}/F)$ $\sigma(E) = E$; and so $r_E(\sigma) \in \mathrm{Aut}(E/F)$, which means $r_E$ is a well-defined function. It is easy to see that $r_E$ is a group homomorphism.

Notice that, since $F \subseteq E \subseteq \overline{F}$, $\overline{F}$ is an algebraic closure of $E$. And so any $\overline{\sigma} : E \xrightarrow{\sim} E$ can be extended to $\sigma : \overline{F} \xrightarrow{\sim} \overline{F}$; in particular $\sigma|_F = \overline{\sigma}|_F = \mathrm{id}_F$. Hence $\sigma \in \mathrm{Aut}(\overline{F}/F)$ and $r_E(\sigma) = \overline{\sigma}$, which means that $r_E$ is surjective.

By definition, it is clear that $\ker r_E = \mathrm{Aut}(\overline{F}/E)$; and so by the first isomorphism theorem we have

$$\mathrm{Aut}(E/F) \simeq \mathrm{Aut}(\overline{F}/F)/\mathrm{Aut}(\overline{F}/E).$$

■

**Theorem 3** *Suppose* $\overline{F}$ *is an algebraic closure of* $F$, $F \subseteq E_1 \subseteq E_2 \subseteq \overline{F}$ *are subfields, and* $E_1/F$ *and* $E_2/F$ *are normal extensions. Then the restriction maps give us well-defined compatible onto group homomorphisms:*

$$\mathrm{Aut}(\overline{F}/F) \xrightarrow{r_{E_2}} \mathrm{Aut}(E_2/F) \xrightarrow{r_{E_2/E_1}} \mathrm{Aut}(E_1/F); \qquad (r_{E_1} : \mathrm{Aut}(\overline{F}/F) \to \mathrm{Aut}(E_1/F))$$

*moreover* $\ker r_{E_2/E_1} = \mathrm{Aut}(E_2/E_1) \trianglelefteq \mathrm{Aut}(E_2/F)$ *and*

$$\mathrm{Aut}(E_1/F) \simeq \mathrm{Aut}(E_2/F)/\mathrm{Aut}(E_2/E_1).$$

*Similarly if* $E_1 \subseteq E_2 \subseteq E_3 \subseteq \overline{F}$ *and* $E_i/F$ *are normal extensions, then* $r_{E_3/E_1} = r_{E_2/E_1} \circ r_{E_3/E_2}$.

*Proof.* We have already proved that $r_{E_i}$ are well-defined onto group homomorphisms. By a similar argument $r_{E_2/E_1}$ is a well-defined group homomorphism. Since clearly we have $r_{E_1} = r_{E_2/E_1} \circ r_{E_2}$, we deduce that $r_{E_2/E_1}$ is onto. By definition $\ker r_{E_2/E_1} = \mathrm{Aut}(E_2/E_1)$; and so by the first isomorphism theorem we get the mentioned isomorphism. The last part of Theorem is clear. ∎

**Theorem 4** *Suppose* $\overline{F}$ *is an algebraic closure of* $F$, $F \subseteq E \subseteq \overline{F}$ *is a subfield, and* $E/F$ *is a normal extension. Let* $\mathcal{F} := \{E' |\, E' \subseteq E, E'/F$ *finite normal* $\}$. *Then*

$$r : \mathrm{Aut}(E/F) \to \{(\sigma_{E'}) \in \prod_{E' \in \mathcal{F}} \mathrm{Aut}(E'/F) |\, r_{E''/E'}(\sigma_{E''}) = \sigma_{E'}\},$$

$$r(\sigma) := (r_{E/E'}(\sigma))_{E' \in \mathcal{F}}$$

*is a group isomorphism.*

The RHS in the display of the second part of the above theorem is called the inverse limit of $\mathrm{Aut}(E'/F)$'s and it is denoted by

$\varprojlim_{E'\in\mathcal{F}} \mathrm{Aut}(E'/F)$. So we are showing that

$$\mathrm{Aut}(E/F) \simeq \varprojlim_{E'\in\mathcal{F}} \mathrm{Aut}(E'/F).$$

Before we get to the proof of Theorem 4 we make the following observation:

**Lemma 5** $E/F$ *is a finite normal extension if and only if* $E$ *is a splitting field of some* $p(x) \in F[x] \setminus F$ *over* $F$.

*Proof of Lemma.* ($\Rightarrow$) Since $E/F$ is a finite extension, there are $\alpha_i$'s in $E$ such that $E = F[\alpha_1, \ldots, \alpha_n]$. Let $p(x) := \prod_{i=1}^n m_{\alpha_i,F}(x)$. Since $E/F$ is a normal extension, all the zeros of $m_{\alpha_i,F}(x)$'s are in $E$; and so all the zeros of $p(x)$ are in $E$. As $E$ is generated by $\alpha_i$'s over $F$, we deduce that $E$ is a splitting field of $p(x)$ over $F$.

($\Leftarrow$) Since $E$ is a splitting of $p(x)$, $E/F$ is a normal extension, and for some $\alpha_i$'s in $E$ we have $E = F[\alpha_1, \ldots, \alpha_n]$ and $p(x) = \prod_{i=1}^n (x - \alpha_i)$. Hence $\alpha_i$'s are algebraic over $F$; and so

$$[E : F] = \prod_{i=1}^n [F[\alpha_1, \ldots, \alpha_i] : F[\alpha_1, \ldots, \alpha_{i-1}]] \leq \prod_{i=1}^n [F[\alpha_i] : F] < \infty.$$

$\blacksquare$

*Proof of Theorem 4.* **Well-definedness.** For any $E' \in \mathcal{F}$, $r_{E/E'}$ is an onto group homomorphism; and so

$$\widehat{r} : \mathrm{Aut}(E/F) \to \prod_{E' \in \mathcal{F}} \widehat{r}(\sigma) := \{r_{E/E'}(\sigma)\}_{E' \in \mathcal{F}},$$

is a group homomorphism. By Theorem 3 we get that $\widehat{r}(\sigma) \in \varprojlim_{E' \in \mathcal{F}} \mathrm{Aut}(E'/F)$; and so $r$ is a well-defined group homomorphism.

**Injectivity.** Since $E/F$ is a normal extension, there are $E_i$ such that $E_i$ is a splitting field of a polynomial $p_i(x) \in F[x]$ over $F$ and $E = \bigcup_{i \in I} E_i$. Hence $E = \bigcup_{E' \in \mathcal{F}} E'$. Then for any $\alpha \in E$ there is $E'_\alpha \in \mathcal{F}$ such that $\alpha \in E'_\alpha$; so if $\sigma \in \ker r$, then for any $\alpha \in E$ we have

$$\sigma(\alpha) = r_{E/E'_\alpha}(\sigma)(\alpha) = \alpha,$$

which implies that $\sigma = \mathrm{id}_E$; and so $r$ is injective.

**Surjectivity.** Suppose $\{\sigma_{E'}\}_{E' \in \mathcal{F}} \in \varprojlim_{E' \in \mathcal{F}} \mathrm{Aut}(E'/F)$. Let $\sigma : E \to E$ be $\sigma(\alpha) = \sigma_{E_0}(\alpha)$ if $\alpha \in E_0$ and $E_0 \in \mathcal{F}$. As we discussed above $E = \bigcup_{E' \in \mathcal{F}} E'$; and so for any $\alpha \in E$ there is $E_0 \in \mathcal{F}$ such that $\alpha \in E_0$. Next we show that $\sigma(\alpha)$ is independent of the choice of $E_0$; and so it is a well-defined function. Suppose $E_0$ and $E_1$ are in $\mathcal{F}$ and $\alpha \in E_0 \cap E_1$. Then $E_0$ is a splitting field of some $p_0(x) \in F[x]$ over $F$ and $E_1$ is a splitting field of some $p_1(x) \in F[x]$ over $F$. Let $E_2 \subseteq E$ be a splitting field of $p_0(x)p_1(x)$ over $F$; notice that since $E/F$ is a normal extension and $E_0 \cup E_1 \subseteq E$, there is such an $E_2$. We have $E_0 \cup E_1 \subseteq E_2$. Since $\{\sigma_{E'}\}_{E' \in \mathcal{F}} \in \varprojlim_{E' \in \mathcal{F}} \mathrm{Aut}(E'/F)$, we have $r_{E_2/E_1}(\sigma_{E_2}) = \sigma_{E_1}$ and $r_{E_2/E_0}(\sigma_{E_2}) = \sigma_{E_0}$. Hence

$$\sigma_{E_0}(\alpha) = r_{E_2/E_0}(\sigma_{E_2})(\alpha) = \sigma_{E_2}(\alpha) = r_{E_2/E_1}(\sigma_{E_2})(\alpha) = \sigma_{E_1}(\alpha).$$

For $\alpha_1, \alpha_2 \in E \setminus \{0\}$, there are $E_i \in \mathcal{F}$ such that $\alpha_i \in E_i$. By the above argument, there is $E_3 \in \mathcal{F}$ such that $\alpha_1, \alpha_2 \in E_3$. Hence $\alpha_1 \pm \alpha_2 \in E_3$ and $\alpha_1\alpha_2^{\pm 1} \in E_3$; and so $\sigma(\alpha_i) = \sigma_{E_3}(\alpha_i)$, $\sigma(\alpha_1 \pm \alpha_2) = \sigma_{E_3}(\alpha_1 \pm \alpha_2)$, and $\sigma(\alpha_1\alpha_2^{\pm 1}) = \sigma_{E_3}(\alpha_1\alpha_2^{\pm 1})$. Since $\sigma_{E_3}$ is a homomorphism, we deduce that $\sigma(\alpha_1 \pm \alpha_2) = \sigma(\alpha_1) \pm \sigma(\alpha_2)$ and $\sigma(\alpha_1\alpha_2^{\pm 1}) = \sigma(\alpha_1)\sigma(\alpha_2)^{\pm 1}$; and so $\sigma$ is a homomorphism. Since $\sigma(1) = \sigma_F(1) = 1$ and $E$ is a field, $\sigma$ is injective. Notice that

$$\sigma(E) = \sigma(\bigcup_{E' \in \mathcal{F}} E') = \bigcup_{E' \in \mathcal{F}} \sigma(E') = \bigcup_{E' \in \mathcal{F}} \sigma_{E'}(E') = \bigcup_{E' \in \mathcal{F}} E' = E;$$

and so $\sigma$ is an automorphism of $E$. Since $\sigma|_F = \sigma_F \in \mathrm{Aut}(F/F) = \{1\}$, we have that $\sigma \in \mathrm{Aut}(E/F)$. By definition of $\sigma$, we have $r_{E/E'}(\sigma) = \sigma_{E'}$ for any $E' \in \mathcal{F}$; and so $r(\sigma) = \{\sigma_{E'}\}_{E' \in \mathcal{F}}$, which implies that $r$ is onto. ∎

**Remark.** We will show that $\mathrm{Aut}(E'/F)$ is a finite group if $E'/F$ is a finite normal extension; and so discrete topology makes it a compact group. By Tychonoff's theorem, $\prod_{E'\in\mathcal{F}} \mathrm{Aut}(E'/F)$ is a compact group. It is easy to check that $\varprojlim_{E'\in\mathcal{F}} \mathrm{Aut}(E'/F)$ is a closed subgroup of $\prod_{E'\in\mathcal{F}} \mathrm{Aut}(E'/F)$; and so the induced product topology makes it a compact group. Therefore the above isomorphism makes $\mathrm{Aut}(E/F)$ a compact group. This topology on $\mathrm{Aut}(E/F)$ is called Krull topology.

## Aut of finite normal extensions.

By Theorem 4 in principle understanding of an infinite normal extension can be reduced to understanding of finite normal extensions. So next we focus on such extensions.

**Theorem 6** *Suppose* $\sigma : F \to F'$ *is a field isomorphism. Suppose* $E$ *is a splitting field of* $f(x) \in F[x]$ *over* $F$ *and* $E'$ *is a splitting field of* $\sigma(f)$ *over* $F'$*. Then*

$$|\{\widehat{\sigma} : E \to E' | \widehat{\sigma} \text{ is an isomorphism }, \widehat{\sigma}|_F = \sigma\}| \le [E : F];$$

*and equality holds if and only if all the irreducible factors of* $f$ *do not have multiple zeros in* $E$*.*

*Proof.* Suppose $f(x) = \prod_{i=1}^{m} f_i(x)^{n_i}$ where $f_i(x)$ are distinct irreducible polynomials in $F[x]$. We say that $f_{sf}(x) := \prod_{i=1}^{m} f_i(x)$ is the square-free factor of $f(x)$. First we observe that $E$ is a splitting field of $f(x)$ over $F$ if and only if it is a splitting field of $f_{sf}(x)$ over $F$. We also observe that $\sigma(f_{sf}) = \sigma(f)_{sf}$. So W.L.O.G. we can and will assume that $f(x)$ is square-free.

Now we proceed by induction on the degree of $f(x)$. Suppose $\alpha$ is a zero of $f_1(x)$. Next we show that

$$|\{\overline{\sigma} : F[\alpha] \hookrightarrow E' \,|\, \overline{\sigma}|_F = \sigma\}| = \# \text{ of distinct zeros of } f_1(x) \text{ in } E.$$

To prove this, it is enough to notice that

(1) $\overline{\sigma}$ is uniquely determined by its value at $\alpha$;

(2) $\overline{\sigma}(\alpha)$ is a zero of $\sigma(f_1)$;

(3) for any zero $\alpha' \in E'$ of $\sigma(f_1)$, there is a field isomorphism $\overline{\sigma} : F[\alpha] \to F'[\alpha']$ such that $\overline{\sigma}|_F = \sigma$ and $\overline{\sigma}(\alpha) = \alpha'$;

(4) since there is an isomorphism $\widehat{\sigma} : E \to E'$ such that $\widehat{\sigma}|_F = \sigma$, the number of distinct zeros of $\sigma(f_1)$ in $E'$ is equal to the number of distinct zeros of $f_1$ in $E$.

For a given $\overline{\sigma}$ as above, we have $f(x) = (x - \alpha)h(x)$ and $\sigma(f) = \overline{\sigma}(f) = (x - \overline{\sigma}(\alpha))\overline{\sigma}(h)$ for some $h(x) \in F[\alpha][x]$. We notice that $E$ is a splitting field of $h(x)$ over $F[\alpha]$ and $E'$ is a splitting field of $\overline{\sigma}(h)$ over $\overline{\sigma}(F[\alpha])$ (justify this). And so by the induction hypothesis,

$$|\{\widehat{\sigma} : E \longrightarrow E' |\, \widehat{\sigma} \text{ is an isomorphism }, \widehat{\sigma}|_{F[\alpha]} = \overline{\sigma}\}| \leq [E : F[\alpha]].$$

Let $\mathrm{Isom}_{\sigma}(E, E') := \{\widehat{\sigma} : E \longrightarrow E' |\, \widehat{\sigma} \text{ is an isomorphism }, \widehat{\sigma}|_F = \sigma\}$, and $\mathrm{Em}_{\sigma}(F[\alpha], E') := \{\overline{\sigma} : F[\alpha] \hookrightarrow E' |\, \overline{\sigma}|_F = \sigma\}$. Consider the restriction function

$$r : \mathrm{Isom}_{\sigma}(E, E') \longrightarrow \mathrm{Em}_{\sigma}(F[\alpha], E').$$

Notice that any $\overline{\sigma} \in \mathrm{Em}_{\sigma}(F[\alpha], E')$ can be extended to an isomorphism from $E$ to $E'$; this implies that $r$ is onto. So we have

$$
\begin{aligned}
|\mathrm{Isom}_\sigma(E, E')| &= \sum_{\overline{\sigma}\in \mathrm{Em}_\sigma(F[\alpha],E')} |r^{-1}(\overline{\sigma})| \\
&\leq \sum_{\overline{\sigma}\in \mathrm{Em}_\sigma(F[\alpha],E')} [E : F[\alpha]] \\
&= |\mathrm{Em}_\sigma(F[\alpha], E')|[E : F[\alpha]] \\
&= (\# \text{ of distinct zeros of } f_1(x) \text{ in } E)[E : F[\alpha]] \\
&\leq (\deg f_1)[E : F[\alpha]] \\
&= [F[\alpha] : F][E : F[\alpha]] = [E : F].
\end{aligned}
$$

Now we focus on exactly when equality holds. Suppose equality holds. Then by the above argument, we have that

$$\deg f_1 = \# \text{ of distinct zeros of } f_1(x) \text{ in } E.$$

Therefore all zeros of $f_1$ are distinct; by symmetry the same is true for $f_i$'s.

Next we assume that all the zeros of $f_i$'s are distinct in $E$, and by induction on $\deg f$ we prove that equality holds. Since $f_i \neq f_j$ are irreducible in $F[x]$, $\gcd(f_i, f_j) = 1$. This implies that there are $a, b \in F[x]$ such that $a(x)f_i(x) + b(x)f_j(x) = 1$. Hence $f_i$ and $f_j$ do not have common factors in $E[x]$. Thus $f(x) = f_{sf}(x)$

is square-free in $E[x]$. And so all the irreducible factors of $f(x)$ in $F[\alpha][x]$ have distinct zeros in $E$. Hence by the induction hypothesis in the above setting for any $\overline{\sigma} \in \mathrm{Em}_\sigma(F[\alpha], E')$ we have $|r^{-1}(\overline{\sigma})| = |\mathrm{Isom}_{\overline{\sigma}}(E, E')| = [E : F[\alpha]]$. We also notice that

$$\deg f_1 = \# \text{ of distinct zeros of } f_1(x) \text{ in } E.$$

Hence we get

$$\begin{aligned}
|\mathrm{Isom}_\sigma(E, E')| &= \sum_{\overline{\sigma} \in \mathrm{Em}_\sigma(F[\alpha], E')} |r^{-1}(\overline{\sigma})| \\
&= \sum_{\overline{\sigma} \in \mathrm{Em}_\sigma(F[\alpha], E')} [E : F[\alpha]] \\
&= |\mathrm{Em}_\sigma(F[\alpha], E')|[E : F[\alpha]] \\
&= (\# \text{ of distinct zeros of } f_1(x) \text{ in } E)[E : F[\alpha]] \\
&= (\deg f_1)[E : F[\alpha]] \\
&= [F[\alpha] : F][E : F[\alpha]] = [E : F];
\end{aligned}$$

and claim follows. ■

A polynomial $f(x) \in F[x]$ is called separable if all of its irreducible factors have distinct zeros in a splitting field $E$ of $f(x)$ over $F$.

**Theorem 7** *Suppose* $E$ *is a splitting field of* $f(x) \in F[x]$ *over* $F$. *Then*

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

*moreover equality holds if and only if* $f(x)$ *is a separable polynomial.*

*Proof.* Notice that $\operatorname{Aut}(E/F) = \operatorname{Isom}_{\mathrm{id}_F}(E,E)$; and claim follows from the previous theorem. ■

An algebraic extension $E/F$ is called separable if for any $\alpha \in E$, $m_{\alpha,F}(x)$ is a separable polynomial. Here is an example of an algebraic extension which is not separable: let $E := \mathbb{F}_p(t)$ and $F := \mathbb{F}_p(t^p)$. Then $t$ is a zero of $x^p - t^p$. Notice that by Eisenstein's criterion $x^p - t^p \in F[x]$ is irreducible; and so $m_{t,F}(x) = x^p - t^p$. Since the characteristic of $E$ is $p$, we have $m_{t,F}(x) = (x-t)^p$; and so it has multiple zeros in $E$. This implies that $E/F$ is not a separable extension. It is worth pointing out that $E$ is a splitting field of $x^p - t^p$ over $F$ as $E$ is generated by $F$ and $t$ (which is a zero of $x^p - t^p$). Hence $E/F$ is a finite normal extension which is not separable.