# MATH 552 NOTES – LECTURE 4

**Normal field extensions:** We say that an algebraic extension $E/F$ is *normal* if $E$ contains a splitting field of the minimal polynomial of every element of $E$, or equivalently, if every irreducible polynomial $f \in F[t]$ either remains irreducible in $E[t]$ or factors in $E[t]$ as a product of linear terms.

If $E$ is a field of characteristic $p$, $E/E^p$ is normal. Indeed, every $r \in E$ has minimum polynomial $t^p - r^p = (t-r)^p$.

**Theorem 1.** *If $E/F$ is a finite field extension, the following are equivalent:*

*a) $E$ is a splitting field of a separable polynomial;*

*b) $F = G'$ for some group $G$ of automorphisms of $E$;*

*c) $E$ is normal and separable over $F$.*

*In this case, $G = \mathrm{Gal}(E/F)$ and $F = E^G$.*

We say that $E/F$ is a [finite] *Galois extension*, or that $E$ is *Galois* over $F$, if these conditions apply.

*Proof.* (a⇒b) Suppose $E$ is a splitting field of a separable $f \in F[t]$, then $|\mathrm{Gal}(E/F)| = [E : F]$ by Corollary 4 of Lecture 3. If $r \in E$, $r \notin F$, its minimal polynomial $f$ has another root, $s$, and the evident isomorphism $F(r) \to F(s)$ extends to an automorphism of $E$ by Thm. 3 of Lecture 3.

(b⇒c) If $r \in E$ has minimal polynomial $f \in F[t]$, and $G \cdot r = \{r_1, ..., r_n\}$, each $r_i$ is a root of $f$. The separable polynomial $f_1(t) = \prod(t - r_i)$ is $G$-invariant and hence belongs to $F[t] = E[t]^G$. Since it divides the irrreducible $f$, we have $f = f_1$. Hence $E/F$ is normal and separable.

(c⇒a) Write $E = F(r_1, ..., r_m)$ with $f_1, ..., f_m$ their (separable) minimal polynomials in $F[t]$. Then $E$ is the splitting field of the product $\prod f_i(t)$. □

**Example 2.** If $r = e^{2\pi i/8}$ then $\mathbb{Q}(r)$ is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q}) = C_2 \times C_2$. Indeed, the minimal polynomial of $r$ is $t^4 + 1$; the other roots are $r^3, r^5, r^7$. Complex conjugation and $g : E \to E$, $g(r) = r^3$, $g(r^5) = r^7$ are generators of the Galois group (**why?**).

---

*Date*: Jan. 27, 2022.

Recall from Thm. 6 of Lecture 3 that the Galois correspondence is an order-reversing operation, and is a bijection between the closed subfields of $E$ and closed subgroups of $G$.

**Theorem 3** (**Fundamental Theorem of Galois Theory**). *Let $E/F$ be a finite Galois extension with Galois group $G$. Then under the Galois correspondence, $|H| = [E : H']$ and $|G/H| = [H' : F]$.*

*Moreover, the normal subgroups of $G$ correspond to the normal subfields of $E$: $H \lhd G$ iff $H'$ is a normal subfield and $G/H \cong \mathrm{Gal}(H'/F)$.*

*Proof.* By Theorem 1(b) above, if $H$ is a subgroup of $G$ and $K = H'$ $(= E^H)$ then $E/K$ is Galois with $\mathrm{Gal}(E/K) = H$. This is the first assertion. It also implies that the conjugate subgroup $gHg^{-1}$ fixes the conjugate subfield $g(K)$. Thus $H \lhd G$ if and only if $g(K) = K$ for every $g \in G$, so $G/H$ acts on $K$. Since $K^G = K^{G/H}$, Theorem 1 again implies that $K/F$ is Galois with $G/H \cong \mathrm{Gal}(K/F)$. □

**Example 4.** If $p$ is a Fermat prime[1] like $p = 3, 5, 17$ or $257$, and $E = \mathbb{Q}(\zeta)$, $\zeta = e^{2\pi i/p}$, then $E/\mathbb{Q}$ is Galois and $\mathrm{Gal}(E/\mathbb{Q})$ is cyclic of order $p-1$. If $r \in \mathbb{Z}/p$ is a primitive root of unity (an element of order $p-1$) then $g(\zeta) = \zeta^r$ determines an automorphism $\alpha$ of $E$ of order $p-1$: $\alpha(\sum a_i\zeta^i) = \sum a_i\zeta^{ri}$. Under the Galois pairing the normal subfields of $E$ correspond to the subgroups $\langle r^{2^i}\rangle$ of $\mathbb{Z}/p^\times$. (Of course, all subgroups of the abelian group $\mathrm{Gal}(E/\mathbb{Q})$ are normal.)

**Lemma 5.** *If $U$ is a finite subgroup of units in a field $F$, then $U$ is a cyclic group. In particular, if $\mathbb{F}_q$ is a finite field of order $q$, the group $\mathbb{F}_q^\times$ of units is cyclic of order $q-1$.*

*Proof.* If $n$ divides $|U|$, the equation $x^n - 1$ has at most $n$ roots. Hence (if $p$ divides $|U|$) there are no subgroups $C_p \times C_p$ of $U$. By the Fundamental theorem of finite abelian groups, $U$ is a cyclic abelian group. □

**Exercise:** Let $\zeta = e^{2\pi i/q}$ be a primitive $q^{th}$ root of unity.
(a) Show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the group of units of the ring $\mathbb{Z}/q\mathbb{Z}$.
(b) If $q = p^n$ For an odd prime $p$, and $n \le 3$, show that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a cyclic group. Example 2 shows that this fails for $p = 2$.

[1] of the form $2^k + 1$