

# Math 547, Final Exam Information.

Wednesday, April 28, 9 - 12, LC 303B.

**The Final exam is cumulative.**

**Useful materials.**

1. Homework 1 - 8.
2. Exams I, II, III, and solutions.
3. Class notes.

**Topic List (not necessarily comprehensive):**

**You will need to know: theorems, results, facts, and definitions from class.**

## 1. Separability.

**Definition.** Let  $K$  be a field, let  $f(x) \in K[x]$ , and let  $F$  be a splitting field for  $f(x)$  over  $K$ . Suppose that  $f(x) = a(x - r_1)^{m_1} \cdots (x - r_t)^{m_t}$ . Then we have:

- (a) The root  $r_i$  has multiplicity  $m_i$ ;
- (b) Suppose that  $m_i = 1$ . Then  $r_i$  is a simple root.

**Recall** that a field  $F$  has characteristic  $m$  if and only if  $m \geq 1$  in  $\mathbb{Z}$  is minimal with the property that for all  $a \in F$ , we have  $a + \cdots + a = m \cdot a = 0$ . If no such  $m$  exists, then  $F$  has characteristic zero; if  $F$  has characteristic  $m > 0$ , then  $m$  must be a prime  $p$ .

**Proposition (8.2.4).** Let  $K$  be a field and let  $f(x) \in K[x]$  be monic and irreducible. Then the following conditions are equivalent:

- (a) The polynomial  $f(x)$  has a multiple root in a splitting field.
- (b)  $\gcd(f(x), f'(x)) \neq 1$ ;
- (c)  $\text{char}(K) = p > 0$  and  $f(x) = a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_1 x^p + a_0$ .

**Definition.** Let  $K$  be a field and let  $f(x) \in K[x]$ . Then

- (a)  $f(x)$  is separable if and only if all of its roots in a splitting field are simple.
- (b) Let  $F \supseteq K$  be algebraic. Then  $F$  is separable over  $K$  if and only if for all  $u \in F$ , the minimal polynomial for  $u$  over  $K$ ,  $f_{K,u}(x)$ , is separable.
- (c) The field  $K$  is perfect if and only if every irreducible  $f(x) \in K[x]$  is separable.

**Theorem (8.2.6).** *Let  $K$  be a field.*

- (a) *Suppose that  $\text{char}(K) = 0$ . Then  $K$  is perfect.*
- (b) *Suppose that  $\text{char}(K) = p > 0$ . Then  $K$  is perfect if and only if every  $u \in K$  has a  $p$ th root in  $K$ ; I.e., for all  $u \in K$ , there exists  $v \in K$  with  $u = v^p$ .*

**Note** that if  $\text{char}(K) = 0$  (e.g., if  $K = \mathbb{Q}, \mathbb{R}$ , or  $\mathbb{C}$ ), then every extension  $F \supseteq K$  is separable over  $K$ .

## 2. Information leading up to the Fundamental Theorem of Galois Theory.

**Theorem (8.1.6).** *Let  $K$  be a field, and suppose that  $f(x) \in K[x]$  has degree  $\geq 1$ , is separable, and has splitting field  $F$ . Then we have  $|G_{F/\mathbb{Q}}| = [F : \mathbb{Q}]$ .*

**Definition.** *Let  $F$  be a field.*

- (a) *The automorphism group of  $F$  is  $\text{Aut}(F) = \{\sigma \mid \sigma : F \rightarrow F \text{ is an automorphism}\}$ .*
- (b) *Let  $G \subseteq \text{Aut}(F)$  be a subgroup. Then the fixed field of  $G$  in  $F$  is*

$$F^G = \{a \in F : \forall \sigma \in G, \sigma(a) = a\}.$$

*Example.* Let  $F = \mathbb{C}$ , and let  $G = \{1_{\mathbb{C}}, \sigma_c\}$  ( $\sigma_c$  is complex conjugation.) Then we have  $F^G = \mathbb{R}$ .

*Example.* Let  $m \geq 3$  in  $\mathbb{Z}$ , let  $F = \mathbb{Q}(\zeta_m)$ , and let  $G = \{1_F, \sigma_c\}$ . Then we have  $F^G = \mathbb{Q}(\cos(\frac{2\pi}{m})) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ .

**Definition.** *Let  $F \subseteq K$  be an algebraic extension of fields. Then  $F$  is normal over  $K$  if and only if every irreducible polynomial in  $K[x]$  that has a root in  $F$  actually splits in  $F$ .*

*Example.* The fields  $\mathbb{Q}(\zeta_3, \sqrt[3]{5})$ ,  $\mathbb{Q}(\zeta_{17})$ , and  $\mathbb{Q}(\sqrt{7})$  are normal.

*Example.* The field  $\mathbb{Q}(\sqrt[7]{5})$  is not normal.

**Theorem (8.3.6).** *Let  $F \supseteq K$  be algebraic with  $[F : K]$  finite. Then the following conditions of  $F$  are equivalent:*

- (a) *The field  $F$  is a splitting field of a separable polynomial in  $K[x]$ .*
- (b) *There exists a finite subgroup  $G \subseteq \text{Aut}(F)$  with  $K = F^G$ .*
- (c) *The field  $F$  is normal and separable over  $K$ .*

**Note** that when  $\text{char}(K) = 0$ , the separability conditions in parts (a) and (c) may be omitted.

**Theorem.** *Let  $K$  be a field, and suppose that  $F$  is a splitting field of a separable polynomial in  $K[x]$ .*

- (a) *We have  $F^{G_{F/K}} = K$ . (Theorem 8.3.3).*
- (b) *Let  $H \subseteq \text{Aut}(F)$  be a finite subgroup. Then we have  $G_{F/F^H} = H$ . (Corollary 8.3.7).*

Important inputs for the above two theorems are Artin's Lemma and the Primitive Element Theorem.

**Lemma (Artin).** *Let  $F$  be a field, and suppose that  $H \subseteq \text{Aut}(F)$  is a finite subgroup. Then we have  $[F : F^H] \leq |H|$ .*

**Theorem (Existence of a primitive element).** *Let  $F \supseteq K$  be fields, and suppose that  $F$  is separable over  $K$  with  $[F : K]$  finite. Then there exists  $u \in F$  with  $F = K(u)$ . I.e., if  $F$  is finite and separable over  $K$ , then  $F$  is a simple extension of  $K$ .*

### 3. The Fundamental Theorem of Galois Theory.

**Theorem (The Fundamental Theorem of Galois Theory).** *Let  $F \supseteq K$  be fields, and suppose that  $F$  is a splitting field of a separable polynomial in  $K[x]$ . Then the following are true.*

(a) *There exists an order-reversing bijection:*

$$\begin{aligned} \{\text{Subgroups: } \langle 1 \rangle \subseteq H \subseteq G_{F/K}\} &\leftrightarrow \{\text{Intermediate fields: } K \subseteq E \subseteq F\} \\ G_{F/F^H} = H &\mapsto F^H \\ G_{F/E} &\leftarrow E = F^{G_{F/E}}. \end{aligned}$$

(b) *With  $H$  (a subgroup of  $G_{F/K}$ ) and  $E$  (an intermediate field between  $K$  and  $F$ ) as above, we have:*

- i.  $[G_{F/K} : H] = [F^H : K]; |H| = [F : F^H]$ .
- ii.  $[G_{F/K} : G_{F/E}] = [E : K]; |G_{F/E}| = [F : E]$ .

(c) *With  $H$  and  $E$  as above, we have:*

- i.  $H \triangleleft G_{F/K}$  if and only if  $F^H$  is normal over  $K$ .
- ii.  $E$  is normal over  $K$  if and only if  $G_{F/E} \triangleleft G_{F/K}$ . Moreover, in this case, we have

$$G_{E/K} \cong G_{F/K}/G_{F/E}.$$

*Example.* Let  $F = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ . Define  $\phi, \psi \in G_{F/\mathbb{Q}}$  by

$$\begin{aligned} \phi : \sqrt[3]{2} &\mapsto \sqrt[3]{2}, \quad \zeta_3 \mapsto \zeta_3^2, \\ \psi : \sqrt[3]{2} &\mapsto \zeta_3 \sqrt[3]{2}, \quad \zeta_3 \mapsto \zeta_3. \end{aligned}$$

Then  $G_{F/\mathbb{Q}} = \langle \phi, \psi \mid o(\phi) = 2, o(\psi) = 3, \phi\psi = \psi^2\phi \rangle \cong S_3$ .

In this setting, the Galois correspondence gives:

$$\begin{aligned} \langle \psi \rangle &\mapsto F^{\langle \psi \rangle} = \mathbb{Q}(\zeta_3) \\ \langle \phi \rangle &\mapsto F^{\langle \phi \rangle} = \mathbb{Q}(\sqrt[3]{2}) \\ \langle \psi\phi \rangle &\mapsto F^{\langle \psi\phi \rangle} = \mathbb{Q}(\zeta_3^2 \sqrt[3]{2}) \\ \langle \psi^2\phi \rangle &\mapsto F^{\langle \psi^2\phi \rangle} = \mathbb{Q}(\zeta_3 \sqrt[3]{2}). \end{aligned}$$