II. INTERACTIVE REVIEW

1. [Reviews compositum, splitting fields.]
Throughout, suppose that K, E, F, L are fields with $K \subseteq E \subseteq L$, $K \subseteq F \subseteq L$, and $[L : K] < \infty$.
   (i) How can we explicitly express E and F in terms of K and L?
   (ii) Using (i), explicitly express the compositum EF in terms of K and L.

   From hereon, suppose that $E : K$ is a splitting field extension for some $g \in K[t] \setminus K$.
   (iii) What is a natural way to choose m and $\alpha_1, \ldots, \alpha_m$ so that $E = K(\alpha_1, \ldots, \alpha_m)$?
   (iv) Is $EF : F$ a splitting field extension? Justify your answer.

2. [Reviews the Fundamental Theorem of Galois Theory.]
Suppose that $L : K$ is a Galois extension and let $G = Gal(L : K)$. According to the Fundamental Theorem of Galois Theory, there is a one-to-one correspondence between what 2 sets? How does this correspondence work?

3. [Reviews finite fields, prime subfield, splitting fields, separable polynomials/extensions, Frobenius, Galois groups, Galois correspondence.]
Throughout, suppose that p is prime and $q = p^n$ for some $n \in \mathbb{Z}_+$.
   (i) Suppose K is a field of order q. What is the characteristic of K? [**Note: we are not yet saying we know there is a field of order q.**]
   (ii) Still suppose K is a field of order q. What polynomial has every element of K as a root?
   (iii) Still suppose K is a field of order q. Describe the prime subfield of K.
   (iv) In these next few steps we want to show there **is** a field of order q. Is the polynomial $t^q - t \in \mathbb{Z}/p\mathbb{Z}[t]$ separable?
   (v) How can we construct a field K of order q?
   (vi) With K as in (v), is $K : \mathbb{Z}/p\mathbb{Z}$ a Galois extension?

   From hereon, let F be the prime subfield of K where $|K| = q$. Note that as $F \simeq \mathbb{Z}/p\mathbb{Z}$, $K : F$ is a splitting field for $t^q - t$. Let $G = Gal(K : F)$.
   (vii) Describe $G = Gal(K : F)$.
   (viii) Let H be a subgroup of G. What can we say about the order and structure of H?
   (ix) Let d be a divisor of n; set $d' = n/d$, and let H be a subgroup of G with order d'. Describe H.
   (x) With d, d', H as in (ix), let $M = Fix_K(H)$. What is $|M|$?

III. CRUCIAL HYPOTHESES REVIEW

When, on an exam, you want to apply a proved result from the course, you should state or demonstrate that the crucial hypotheses have been met.

(i) Suppose $\sigma : K_1 \to K_2$ is a field isomorphism, L_1, L_2 are fields with $K_1 \subseteq L_1$, $K_2 \subseteq L_2$, and $\alpha \in L_1$, $\beta \in L_2$. Supposing α is algebraic over K_1, when can we extend σ to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ so that $\tau(\alpha) = \beta$?

(ii) Suppose $L : K$ is a field extension and $\sigma : L \to L$ is a K-homomorphism. When do we know that σ is an automorphism of L?

(iii) For M a field, when does every $f \in M[t] \setminus M$ split over M?

(iv) For a field K, does an algebraic closure of K exist?

(v) For $L : K$ a field extension, when is an algebraic closure $\overline{L}$ of L also an algebraic closure of K?

(vi) Say $\overline{K}$ is an algebraic closure of K and $L : \overline{K}$ is a field extension. When can we conclude that $L \simeq \overline{K}$?

(vii) Suppose $L : K$ is an extension and $\sigma : K \to \overline{K}$ is a homomorphism. When can we extend σ to a homomorphism $\tau : L \to \overline{K}$?

(viii) Suppose $L : K$ is an algebraic extension with $K \subseteq L \subseteq \overline{K}$, and $\tau : L \to \overline{K}$ is a K-homomorphism. When do we know that $\tau \in Aut(L)$?

(ix) Suppose $L : M : K$ is a tower of fields with $K \subseteq M \subseteq L$, with $L : M$ a normal extension. Suppose $\sigma : L \to L$ is a K-homomorphism. When can we say that $\sigma(M) \subseteq M$?

(x) Suppose that $M : K$ is an extension with $K \subseteq M$, $f \in K[t] \subseteq K$, $g \in M[t] \setminus M$. Also suppose that f is separable over K. From this, when can we conclude that g is separable over M?

(xi) Suppose that $L : K$ is a splitting field extension for some $f \in K[t] \setminus K$. When do we know that every element of L is separable over K?

(xii) Suppose K is a field, and $f \in K[t] \setminus K$. There are two (mutually exclusive) hypotheses that guarantee that f is separable over K. What are these?

(xiii) Suppose $L : K$ is a finite Galois extension, $G = Gal(L : K)$, H is a subgroup of G, and $M = FixL(H)$. When is $M : K$ a Galois extension, and when it is, what can we say about its Galois group?

FUNDAMENTALS FROM SECTIONS 13, 15, 16

- Suppose $f \in \mathbb{Q}[t]$ is irreducible of degree 3 or 4, and $L : \mathbb{Q}$ is a splitting field extension for f. Then n divides $[L : \mathbb{Q}]$ (WHY?). Also, $Gal(L : \mathbb{Q})$ is isomorphic to a subgroup of S_n (WHY?). Further, $Gal(L : \mathbb{Q})$ is isomorphic to a **transitive** subgroup of S_n (WHY?).

  So when $\deg f = 3$, what subgroups of S_3 could $Gal(L : \mathbb{Q})$ be isomorphic to?

  When $\deg f = 4$, what subgroups of S_4 could $Gal(L : \mathbb{Q})$ be isomorphic to? (The transitive subgroups of S_4 with order divisible by 4 are isomorphic to S_4, A_4, D_4, C_4, V_4 where $D_4 = \langle a, b : \ a^4 = 1 = b^2, \ ba = a^3 b \ \rangle$, C_4 is cyclic of order 4, and $V_4 = \langle a, b : \ a^2 = 1 = b^2, \ ab = ba \ \rangle$.)
- Take $n \in \mathbb{Z}_+$. The cyclotomic polynomial $\Phi_n \in \mathbb{Q}[t]$ is the minimal polynomial for any primitive nth root of unity in $\mathbb{C}$; so

$$\Phi_n = \prod_{\zeta} (t - \zeta)$$

  where ζ varies over all primitive nth roots of unity in $\mathbb{C}$.

  We can determine Φ_n inductively by knowing that $\Phi_1 = t - 1$ and that for $n > 1$,

$$t^n - 1 = \prod_{d|n} \Phi_d.$$

  Also, for ζ a primitive nth root of unity, $\mathbb{Q} : \mathbb{Q}$ is a splitting field extension for Φ_n (WHY?) with $Gal(\mathbb{Q}(\zeta) : \mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ (WHY?).
- Suppose K is a field, q is a prime so that $q \neq \text{char}K$, and take $\theta \in K^\times$. If $t^q - \theta$ is reducible over K, then $t^q - \theta$ has a root in K. When $t^q - \theta$ is reducible over K, when does $t^q - \theta$ split over K?