Math 562 **Friday, April 27**
Exam 3 **Drew Armstrong**

There are 3 problems and 4 pages. This is a closed book test. Any student caught cheating will receive a score of zero.

1. Let $F \subseteq K$ be a finite-dimensional (hence algebraic) extension of characteristic 0 fields.

(a) **[1 pt] State the definition** of the Galois group $G := \mathsf{Gal}(K/F)$.

Proof. Let $\mathrm{Aut}(K)$ be the group (under composition) of field automorphisms of K. Then G is the subgroup $\{\mu \in \mathrm{Aut}(K) : \mu(a) = a \ \ \forall a \in F\} \leq \mathrm{Aut(K)}$ that fixes F pointwise. $\square$

(b) **[3 pts] Prove** that G is finite. [Hint: Primitive Element Theorem.]

Proof. Since the extension K/F of characteristic 0 fields is finite and algebraic, Steinitz' Primitive Element Theorem tells us that there exists $\gamma \in K$ such that $K = F(\gamma)$. Now an element $\mu \in G$ is determined by the single value $\mu(\gamma) \in K$. Furthermore, by (c) we know that $\mu(\gamma)$ is a root of the minimal polynomial $m_\gamma(x) \in F[x]$. There are at most $\deg(m_\gamma(x))$ such roots, hence $|G| \leq \deg(m_\gamma(x))$. $\square$

(c) **[1 pt]** For all $f(x) \in F[x]$, $\alpha \in K$, $\mu \in G$, **prove** that $\mu(f(\alpha)) = f(\mu(\alpha))$.

Proof. Let $f(x) = \sum_{k \geq 0} a_k x^k$. Then since $\mu(a_k) = a_k$ for each coefficient $a_k \in F$, we have

$$\mu(f(\alpha)) = \mu\left(\sum_{k\geq 0} a_k \alpha^k\right) = \sum_{k \geq 0} \mu(a_k)\mu(\alpha)^k = \sum_{k\geq 0} a_k \mu(\alpha)^k = f(\mu(\alpha)).$$

$\square$

[Now here I made a boo boo. For part (d) we must assume that $F = K^G$ (i.e. that the extension K/F is normal). It seems that this didn't bother the students (the power of suggestion is strong). But to you on the internets: I intended Probem 1 to deal with not-necessarily-normal field extensions. In this regard parts (d),(e),(f) — part (f) in particular — are quite silly. Read with caution. Also, I apologize.]

(d) **[2 pts]** Given any $\beta \in K$, consider its G-orbit $\{\beta = \beta_1, \beta_2, \ldots, \beta_r\}$. **Explain** why the polynomial $g(x) := (x - \beta_1) \cdots (x - \beta_r) \in K[x]$ is actually in $F[x]$.

Proof. The coefficients of $g(x)$ are symmetric in the β_i (in fact they're the elementary symmetric combinations of the β_i). Since an element $\mu \in G$ acts by permuting the β_i (why?), we find that each coefficient is fixed by each element of G. Hence the coefficients are in $K^G = F$. $\square$

(e) **[2 pts]** Use (c) and (d) to **prove** that $g(x)$ is the minimal polynomial for β over F. [Hint: Consider any $f(x) \in F[x]$ with $f(\beta) = 0$. Show that $g(x)$ divides $f(x)$.]

Proof. We have $g(x) \in F[x]$ with $g(\beta) = 0$. Choose any other $f(x) \in F[x]$ with $f(\beta) = 0$. Since $\{\beta = \beta_1, \ldots, \beta_r\}$ is a G-orbit, there exists for each i some $\mu_i \in G$ such that $\mu_i(\beta) = \beta_i$. Then by (c) we have $f(\beta_i) = f(\mu_i(\beta)) = \mu_i(f(\beta)) = \mu_i(0) = 0$ for all i. By the Factor Theorem we can write $f(x) = (x - \beta_1)\cdots(x - \beta_r)h(x)$ for some $h(x) \in F[x]$; in other words $g(x)$ divides $f(x)$. We conclude that $g(x)$ is the minpoly. □

(f) **[1 pt]** Use (d) and (e) to **prove** that $[K : F]$ divides $|G|$. [Hint: Orbit-Stabilizer.]

Proof. Let β be a primitive element for K/F so that $[K : F] = \deg(m_\beta(x)) = r$. Since r is the size of a G-orbit, it divides $|G|$ by the Orbit-Stabilizer Theorem. □

[Actually, since we assumed $F = K^G$ in part (d), it's true that $[K : F] = |G|$.]

2. Now let $F \subseteq K$ be a **normal** extension of characteristic 0 fields, and let $G := \mathsf{Gal}(F/K)$.

(a) **[1 pt] State some definition** of "normal" for the field extension $F \subseteq K$.

Proof. We say that K/F is normal if K is a splitting field for some polynomial $f(x) \in F[x]$. □

(b) **[1 pt]** Given a subgroup $H \leq G$, **state the definition** of K^H.

Proof.

$$K^H := \{a \in K : \mu(a) = a \ \forall \mu \in H\}$$

□

(c) **[2 pt] Prove** that K^H is a **subfield** of K.

Proof. We have $\mu(0) = 0$ and $\mu(1) = 1$ for all $\mu \in H$, hence $0, 1 \in K^H$. For $a, b \in K^H$ we have $\mu(a + b) = \mu(a) + \mu(b) = a + b$ and $\mu(ab) = \mu(a)\mu(b) = ab$, hence $a + b, ab \in K^H$. Finally, if $0 \neq a \in K^H$ and $\mu \in H$ then we have $1 = \mu(1) = \mu(aa^{-1}) = \mu(a)\mu(a^{-1}) = a\mu(a^{-1})$. We conclude that $\mu(a^{-1}) = a^{-1}$, hence $a^{-1} \in K^H$. □

(d) **[1 pt]** What does the Fundamental Theorem tell us about $\mathsf{Gal}(K/K^H)$? [Hint: It's equal to...]

Proof. $\mathsf{Gal}(K/K^H) = H$. □

(e) **[1 pt]** If $H \trianglelefteq G$ is normal, what does the Fundamental Theorem tell us about the quotient group G/H? [Hint: It's isomorphic to...]

Proof. $G/H = \mathsf{Gal}(K/F)/\mathsf{Gal}(K/K^H) \approx \mathsf{Gal}(K^H/F)$. □

3. Let $\gamma := \sqrt[3]{2} \in \mathbb{R}$ and $\omega := e^{2\pi i/3} \in \mathbb{C}$.

(a) **[1 pt] State one reason** why the extension $\mathbb{Q}(\gamma, \omega)/\mathbb{Q}$ is normal.

Proof. We've seen that $\mathbb{Q}(\gamma, \omega)$ is the splitting field for $x^3 - 2 \in \mathbb{Q}[x]$, hence it's normal. □

(b) **[3 pts] Draw** the lattice of all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\gamma, \omega)$. **Label** the edges with the degrees of the extensions. **Indicate** which of the fields are normal over $\mathbb{Q}$.

Proof. There are six intermediate fields:

$$\mathbb{Q}(\gamma, \omega), \mathbb{Q}(\gamma), \mathbb{Q}(\omega\gamma), \mathbb{Q}(\omega^2\gamma), \mathbb{Q}(\omega), \mathbb{Q}.$$

Of these, three are normal over $\mathbb{Q}$:

$$\mathbb{Q}(\gamma, \omega), \mathbb{Q}(\omega), \mathbb{Q}.$$

The picture is in the Course Notes. $\square$

(c) **[0 pts]** Have a nice summer.