Math 547, Exam 4, Spring , 2005 Solutions

The exam is worth 50 points. Each problem is worth 10 points.

Write your answers as legibly as you can on the blank sheets of paper provided. Use only **one side** of each sheet. Take enough space for each problem. Turn in your solutions in the order: problem 1, problem 2, ... ; although, by using enough paper, you can do the problems in any order that suits you.

I will e-mail your grade to you as soon as I finish grading the exams.

If you want me to leave your exam outside my door (so that you can pick it up before Wednesday's class), then **TELL ME** and I will do it. The exam will be there as soon as I e-mail your grade to you.

I will post the solutions on my website later today.

1. **Let $K \subseteq L$ be fields, $f(x)$ be a polynomial in $K[x]$, $\sigma \in \operatorname{Aut}_K L$, and $\ell \in L$. Suppose that $f(\ell) = 0$. Prove $f(\sigma(\ell)) = 0$. Give all details.**

Let $f(x) = \sum_{j=0}^{n} k_j x^j$, with each $k_j \in K$. We have $0 = f(\ell)$. Apply the ring homomorphism σ to both sides to get

$$0 = \sigma(0) = \sigma(f(\ell)) = \sigma\left(\sum_{j=0}^{n} k_j \ell^j\right) = \sum_{j=0}^{n} \sigma(k_j)(\sigma(\ell))^j.$$

The hypothesis also tells us that $\sigma(k_j) = k_j$ for all j; so

$$0 = \sum_{j=0}^{n} k_j(\sigma(\ell))^j = f(\sigma(\ell)).$$

2. **Let $K \subseteq L$ be fields, $f(x)$ be an irreducible polynomial of $K[x]$, and α_1 and α_2 be elements of L with $f(\alpha_1) = f(\alpha_2) = 0$. Prove that there exists a ring isomorphism $\sigma\colon K[\alpha_1] \to K[\alpha_2]$ with $\sigma(\alpha_1) = \alpha_2$ and $\sigma(k) = k$ for all $k \in K$. Give all details.**

There is a surjective ring homomorphism $\phi_1\colon K[x] \to K[\alpha_1]$ with $\phi_1(g(x)) = g(\alpha_1)$ for all $g(x) \in K[x]$. The kernel of ϕ_1 is generated by the minimal polynomial $f(x)$ of α_1. The first isomorphism theorem ensures the existence of a ring isomorphism with $\bar\phi_1(\bar g) = \phi_1(g) = g(\alpha_1)$ for all $g \in K[x]$. We repeat the above procedure to produce a ring isomorphism $\bar\phi_2\colon K[x]/(f(x)) \to K[\alpha_2]$, with $\bar\phi_2(\bar g) = g(\alpha_2)$ for all $g \in K[x]$. It follows that $\bar\phi_2 \circ \bar\phi_1^{-1}\colon K[\alpha_1] \to K[\alpha_2]$ is a ring isomorphism. It is clear that

$$\bar\phi_2 \circ \bar\phi_1^{-1}(\alpha_1) = \bar\phi_2(\bar x) = \alpha_2.$$

3. **State the Fundamental Theorem of Galois Theory. Please give hypotheses and conclusions.**

Let K be a field with $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, let $f(x)$ be a polynomial in $K[x]$, and let F be the splitting field of f over K. Then

a. $|\operatorname{Aut}_K F| = \dim_K F$.

b. There is a one-to-one, inclusion reversing, correspondence between the subgroups H of $\operatorname{Aut}_K F$ and the intermediate fields E with $K \subseteq E \subseteq F$. The correspondence is given as follows. If H is a subgroup of $\operatorname{Aut}_K F$, then the corresponding field is F^H, which is defined to be

$$\{\alpha \in F \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in H\}.$$

If E is a field with $K \subseteq E \subseteq F$, then the corresponding group is

$$\operatorname{Aut}_E F = \{\sigma \in \operatorname{Aut}_K F \mid \sigma(e) = e \text{ for all } e \in E\}.$$

c. If F^H is one of the fields with $K \subseteq F^H \subseteq F$ for some subgroup H of $\operatorname{Aut}_K F$, then $\dim_{F^H} F = |H|$.

4. **Let F be the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$. Find all fields K with $\mathbb{Q} \subseteq K \subseteq F$. Give complete details.**

The roots of f in $\mathbb{C}$ are $r_1 = \theta$, $r_2 = \omega\theta$, and $r_3 = \omega^2\theta$, where $\theta = \sqrt[3]{2}$, and $\omega = e^{\frac{2\pi i}{3}}$. It follows that $K = \mathbb{Q}[\theta, \omega]$. The polynomial f is irreducible over $\mathbb{Q}$ by the Eisenstein criteria; so, f is the minimal polynomial of θ over $\mathbb{Q}$; and $\dim_{\mathbb{Q}} \mathbb{Q}[\theta] = 3$. We know that ω is a root of $g(x) = x^2 + x + 1$. Furthermore, $g(x)$ is irreducible over $\mathbb{Q}[\theta]$ because the only possible factorization would be a factorization into linear factors. We know that g does not factor into linear factors over $\mathbb{Q}[\theta]$ because the roots of g are ω and ω^2. Neither of these roots are real numbers and $\mathbb{Q}[\theta] \subseteq \mathbb{R}$. It follows that $\dim_{\mathbb{Q}[\theta]} F = 2$. We now use problem 2 to produce an automorphism σ of F which fixes $\mathbb{Q}[\theta]$ and sends ω to ω^2. We know that

$$6 = \dim_{\mathbb{Q}} F = \underbrace{\dim_{\mathbb{Q}} \mathbb{Q}[\omega]}_{2} \dim_{\mathbb{Q}[\omega]} F.$$

It follows that f is the minimal polynomial of θ over $\mathbb{Q}[\omega]$. We use problem 2 again to produce an automorphism τ of F which fixes $\mathbb{Q}[\omega]$ and sends θ to $\theta\omega$. We notice that on the roots of f: $r_1 = \theta$, $r_2 = \omega\theta$, $r_3 = \omega^2\theta$, the action of σ is $(2,3)$ and the action of τ is $(1,2,3)$, The permutations $(2,3)$ and $(1,2,3)$ generate all of S_3 and $\operatorname{Aut}_{\mathbb{Q}} F$ is a subgroup of S_3. We conclude that σ and τ generate $\operatorname{Aut}_{\mathbb{Q}} F$ and $\operatorname{Aut}_{\mathbb{Q}} F = S_3$. The subgroups of S_3 are S_3, $<(1,2,3)>$, $<(1,2)>$, $<(1,3)>$, $<(2,3)>$, and $<(1)>$. The corresponding fields are:

$$F^{S_3} = \mathbb{Q}, \quad F^{<(1,2,3)>} = \mathbb{Q}[\omega], \quad F^{<(1,2)>} = \mathbb{Q}[\omega^2\theta], \quad F^{<(1,3)>} = \mathbb{Q}[\omega\theta],$$

$$F^{<(2,3)>} = \mathbb{Q}[\theta], \quad F^{<(1)>} = F.$$

5. **We know that** $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$**. We also know that** $g(x) = x^6 + x^3 + 1$ **is irreducible over** $\mathbb{Q}$**. (There is no need to re-prove these facts.) Let** F **be the splitting field of** $g(x)$ **over** $\mathbb{Q}$**. Find** $\operatorname{Aut}_{\mathbb{Q}} F$**. Be sure to tell me the elements of** $\operatorname{Aut}_{\mathbb{Q}} F$ **as well as the group structure. Give complete details.**

The roots of g in $\mathbb{C}$ are ζ, ζ^2, ζ^4, ζ^5, ζ^7, ζ^8. So, $F = \mathbb{Q}[\zeta]$, and $\dim_{\mathbb{Q}} F = 6$. If σ is in $\operatorname{Aut}_{\mathbb{Q}} F$, then the entire action of σ is completely determined by the value of $\sigma(\zeta)$. Problem 1 tells us that $\sigma(\zeta)$ must be ζ^j for $j \in \{1, 2, 4, 5, 7, 8\}$. Problem 2 tells us that each of the six listed candidates for σ really is a ring isomorphism. So, we have learned that $\operatorname{Aut}_{\mathbb{Q}} F$ consists of the six functions $\sigma_j(\zeta) = \zeta^j$ for $j \in \{1, 2, 4, 5, 7, 8\}$. It is easy to see that σ_2 generates this group. Indeed,

$$\sigma_2^2 = \sigma_4, \quad \sigma_2^3 = \sigma_8, \quad \sigma_2^4 = \sigma_7, \quad \sigma_2^5 = \sigma_5, \quad \sigma_2^6 = \sigma_1.$$

We conclude that $\operatorname{Aut}_{\mathbb{Q}} F$ is the cyclic group of order six which is generated by the function σ_2.