Math 547, Final Exam, Spring , 2005

The exam is worth 100 points. Each problem is worth 11 1/9 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.

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 $\mathrm{Aut}_K F$, 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

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

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

4. **Let I be an ideal of the ring R. Prove that I is a maximal ideal of R if and only if R/I is a field.**

$\Rightarrow$ We need show that each non-zero element of $\frac{R}{I}$ has a multiplicative inverse in $\frac{R}{I}$. Pick a non-zero element of $\frac{R}{I}$. This element has the form $\bar{a}$ where a is an element of R which is not an element of I. We must show that the element $\bar{a}$ of $\frac{R}{I}$ has an inverse in $\frac{R}{I}$.

Let (I, a) denote the smallest ideal of R which contains I and a. Observe that $(I, a) = \{m + ra \mid m \in I \text{ and } r \in R\}$. The hypothesis ensures us that $(I, a) = R$. In other words, there exist elements $m \in I$ and $r \in R$ with $1 = m + ra$. We conclude that $\bar{r}$ is the inverse of $\bar{a}$ in $\frac{R}{I}$.

$\Leftarrow$ Suppose J is an ideal of R with $I \subsetneq J$. Let $j \in J$ with $j \notin I$. The hypothesis that R/I is a field ensures that there exists an element r of R with $rj - 1 \in I$. It follows that 1 is equal to rj plus an element of I. Thus, $1 \in J$ and J is equal to all of R.

5. **Prove that $\mathbb{Q}[x]$ is a Principal Ideal Domain.**

Let I be a non-zero ideal in $\mathbb{Q}[x]$. Let f be a non-zero polynomial in I of least degree. We show that $I = (f)$. It is clear that $(f) \subseteq I$. We show that $I \subseteq (f)$. Let g be an arbitrary element of I. Divide f into g and get $g = hf + r$ for polynomials h and r of $\mathbb{Q}[x]$ where either r is the zero polynomial or r has degree less than the degree of f. We see that $r = g - hf \in I$. We chose f to be a non-zero polynomial in I of least degree. It follows that r is the zero polynomial and $g \in (f)$.

6. **Let I be an ideal in a Principal Ideal Domain R. Prove that the following statements are equivalent. (That is, if one of the statements is true, then they all are true. If one of the statements is false, then they all are false.)**
   (a) There is an irreducible element r of R with $I = (r)$.
   (b) The ideal I is a non-zero prime ideal.
   (c) The ideal I is a maximal ideal.

$(a) \implies (c)$ Suppose J is an ideal of R with $I \subsetneq J$. The ring R is a Principal ideal domain, so $J = (j)$ for some element j of R. The fact that $f \in I \subset J = (j)$ tells us that $f = jr$ for some r in R. The fact that $I \neq J$ tells us that r is not

a unit in R. The hypothesis that f is irreducible ensures that j is a unit of R; hence, $J = R$, and I is a maximal ideal of R.

$(c) \implies (b)$ It is always true that every maximal ideal is a prime ideal. Indeed, if I is a maximal ideal, then R/I is a field; hence, R/I is a domain; hence, I is a prime ideal.

$(b) \implies (a)$ The ring R is a Principal ideal domain; so, $I = (r)$ for some r in R. We must show that r is irreducible. Suppose $r = st$ for some s, t in R. The hypothesis that I is prime ensures that at least one of s or t is in I. We may assume, without loss of generality, that s is in I. So, $s = rw$ for some w in R and $r = st = rwt$. The ring R is a domain; so $1 = wt$ and t is a unit. We have shown that in every factorization of r, one of the factors must be a unit. Thus, r is irreducible.

7. **Let K be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. We have shown that $K = \mathbb{Q}[\sqrt[5]{2}, \omega]$, where $\omega = e^{\frac{2\pi i}{5}}$. We have also shown that $\dim_{\mathbb{Q}} K = 20$, and that there exist auotmorphisms σ, τ in $\mathrm{Aut}_{\mathbb{Q}} K$ with**

$$\sigma(\sqrt[5]{2}) = \sqrt[5]{2} \quad \sigma(\omega) = \omega^2$$

$$\tau(\sqrt[5]{2}) = \omega\sqrt[5]{2} \quad \tau(\omega) = \omega.$$

Furthermore we have shown that $\mathrm{Aut}_{\mathbb{Q}} K$ is generated by σ and τ. You do not have to re-prove any of the above facts. However, I do want complete details for the following things: Find a field E with $\mathbb{Q} \subseteq E \subseteq K$ and $\dim_{\mathbb{Q}} E = 2$. Find the subgroup H of $\mathrm{Aut}_{\mathbb{Q}} K$ with $K^H = E$. ("Find" means tell me generators.)

Let $u = \omega + \omega^4$ and $E = \mathbb{Q}[u]$. It is clear that $u \notin \mathbb{Q}$; indeed, $\sigma(u) = \omega^2 + \omega^3 \neq u$. It is easy to see that u satisfies a quadratic polynomial with coefficients in $\mathbb{Q}$. Indeed, $u^2 = \omega^2 + \omega^3 + 2$; so

$$u + u^2 = (\omega + \omega^2 + \omega^3 + \omega^4) + 2 = -1 + 2 = 1.$$

Thus, u is a root of $x^2 + x - 1 = 0$, and $\dim_{\mathbb{Q}} E = 2$. I notice that $\tau(u) = u$ and $\sigma^2(u) = u$. Thus, $<\sigma^2, \tau>$ is a subgroup of H. The fundamental Theorem of Galois Theory tells us that H has 10 elements. Lagrange's Theorem tells us that 2, which is equal to the order of σ^2 and 5, which is equal to the order of τ, each divide the order of $<\sigma^2, \tau>$. It follows that $<\sigma^2, \tau>$ has order 10 and is equal to H.

8. **Let H be the subgroup $<(1,2,3,4),(1,3)>$ of S_4. Let S_4/H be the set of left cosets of H in S_4. Let H act on S_4/H by left translation. In other words, if h is in H and gH is a left coset of H in S_4 (i.e., $g \in S_4$), then h sends gH to the left coset hgH.**
   (a) Find the orbit of each element of S_4/H.
   (b) Find the normalizer of H in S_4. Recall that the normalizer of H in S_4 is

$$N_{S_4}(H) = \{g \in S_4 \mid gHg^{-1} = H\}.$$

We see that

$$H = \{(1), (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,3), (1,2)(3,4), (2,4), (1,4)(2,3)\},$$

$$(1,2)H = \{(1,2), (2,3,4), (1,3,2,4), (1,3,2,4), (1,4,3), (1,3,2), (3,4), (1,2,4), (1,4,2,3)\},$$

and

$$(1,4)H = \{(1,4), (1,2,3), (1,3,4,2), (2,4,3), (1,3,4), (1,2,4,3), (1,4,2), (2,3)\}$$

It is clear that the orbit of H is $\{H\}$. We see that $(1), (1,3)(2,4), (1,2)(3,4)$, and $(1,4)(2,3)$ all carry $(1,2)H$ to $(1,2)H$, and $(1,2,3,4), (1,4,3,2), (1,2,3)$, and $(2,4)$ all carry $(1,2)H$ to $(1,4)H$. We conclude that the orbit of $(1,2)H$ is $\{(1,2)H, (1,4)H\}$. The normalizer of H in S_4 is the union of all of the cosets which have orbits consisting of only one element. So, the normalizer of H in S_4 is simply H. (Of course, you know that $N_{S_4}(H) = H$ without doing any work. Indeed, $N_{S_4}(H)$ is a subgroup of S_4, with H a normal subgroup of $N_{S_4}(H)$. The only subgroups of S_4 which contain H are S_4 and H. It is easy to see that H is not a normal subgroup of S_4; so we see that $N_{S_4}(H) = H$.)

9. **Let K be the splitting field of $x^{17}-1$ over $\mathbb{Q}$. We know that $K = \mathbb{Q}[\omega]$, for $\omega = e^{\frac{2\pi i}{17}}$. We also know that $\mathrm{Aut}_{\mathbb{Q}} K$ is the cyclic group of order 16 which is generated by the automorphism σ where $\sigma(\omega) = \omega^3$. You do not have to re-prove any of the above facts. However, I do want complete details for the following things: Find a subgroup H of $\mathrm{Aut}_{\mathbb{Q}} K$ with 8 elements. Find the field K^H. ("Find" means tell me generators.)**

The element σ^2 of $\mathrm{Aut}_{\mathbb{Q}} K$ has order 8; so H is generated by σ^2. We see that σ^2 carries

$$\omega \mapsto \omega^9 \mapsto \omega^{13} \mapsto \omega^{15} \mapsto \omega^{16} \mapsto \omega^8 \mapsto \omega^4 \mapsto \omega^2 \mapsto \omega.$$

It follows that if

$$u = \omega + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2,$$

then $\sigma^2(u) = u$. Thus, $u \in K^H$. On the other hand, σ moves u, so $u \notin \mathbb{Q}$. The fact that $\dim_{\mathbb{Q}} K^H = 2$ ensures that there do not exist any field properly between $\mathbb{Q}$ and K^H; and therefore, $K^H = \mathbb{Q}[u]$.