

**Math 547, Exam 3. 4/16/10.**

**Name:** \_\_\_\_\_

- Read problems carefully. Show all work.
- No notes, calculator, or text.
- The exam is approximately 15 percent of the total grade.
- There are 100 points total. Partial credit may be given.

1. **(20 points)** Let  $F$  and  $K$  be fields with  $F \supseteq K$ , and let  $a$  and  $b \in F$  be algebraic. Further, suppose that

- (a) the degree of  $a$  over  $K$  is  $m$ ,
- (b) the degree of  $b$  over  $K$  is  $n$ , and
- (c)  $\gcd(m, n) = 1$ .

Show that  $[K(a, b) : K] = mn$ .

*Proof.* We have the following:

$$\begin{aligned} a \in K(a, b) &\implies m = [K(a) : K] \mid [K(a, b) : K] \\ b \in K(a, b) &\implies n = [K(b) : K] \mid [K(a, b) : K]. \end{aligned}$$

Since  $\gcd(m, n) = 1$ , we have  $mn \mid [K(a, b) : K]$ , so  $mn \leq [K(a, b) : K]$ . On the other hand, we know that

$$[K(a, b) : K] \leq [K(a) : K] \cdot [K(b) : K] = mn.$$

It follows that  $[K(a, b) : K] = mn$ . □

2. (15 points) Write down a basis for  $K = \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$  over  $\mathbb{Q}$ .

Make sure to justify your answer.

**Claim:** A basis is  $\{1, i, 2^{1/4}, 2^{1/2}, 2^{3/4}, i \cdot 2^{1/4}, i \cdot 2^{1/2}, i \cdot 2^{3/4}\}$ .

*Proof.* We first note that  $x^4 - 2$  is 2-Eisenstein, and therefore, irreducible in  $\mathbb{Q}[x]$ . Hence, we have  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ , and a basis for  $\mathbb{Q}(\sqrt[4]{2})$  over  $\mathbb{Q}$  is  $B_1 = \{1, 2^{1/4}, 2^{1/2}, 2^{3/4}\}$ .

Next, we observe that  $x^2 + 1$  is irreducible in  $\mathbb{Q}(\sqrt[4]{2})[x]$  since  $i = \sqrt{-1} \notin \mathbb{Q}(\sqrt[4]{2})$ . In particular, we see that  $i \notin \mathbb{R}$ , but  $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ . Therefore, we have  $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1}) : \mathbb{Q}(\sqrt[4]{2})] = 2$ , and a basis for  $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$  over  $\mathbb{Q}(\sqrt[4]{2})$  is  $B_2 = \{1, i\}$ .

To conclude, observe that one obtains a basis for  $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$  over  $\mathbb{Q}$  by taking all products of elements from  $B_1$  with elements from  $B_2$ .  $\square$

3. **(15 points)** Let  $K$  and  $F$  be fields. Suppose that

- (a)  $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$  has a root  $u \in F$ , and
- (b)  $\sigma \in \text{Gal}(F/K)$ .

Show that  $\sigma(u)$  is also a root of  $f(x)$ . Justify all steps.

*Proof.* Since  $u$  is a root of  $f(x)$ , we have

$$(*) \quad f(u) = \sum_{i=0}^n a_i u^i = 0.$$

We apply  $\sigma$  to equation (\*) and compute:

$$\begin{aligned} \sigma(f(u)) &= \sigma\left(\sum_{i=0}^n a_i u^i\right) = \sigma(0) = 0 \\ \implies 0 &= \sigma\left(\sum_{i=0}^n a_i u^i\right) = \sum_{i=0}^n \sigma(a_i u^i) = \sum_{i=0}^n \sigma(a_i) \sigma(u)^i = \sum_{i=0}^n a_i \sigma(u)^i = f(\sigma(u)). \end{aligned}$$

In the second line, we used the following facts: since  $\sigma$  is a field automorphism, it is a homomorphism for both addition and multiplication; since  $\sigma \in \text{Gal}(F/K)$ , it fixes elements of  $K$  pointwise (here, it fixes the coefficients  $a_i$ ). It follows that  $\sigma(u)$  is also a root of  $f(x)$ .  $\square$

4. (26 points) Short answer.

- (a) (9 points) Identify algebraic numbers  $\alpha$  and  $\beta$  for which  $\mathbb{Q}(\alpha, \beta)$  is the splitting field of  $x^5 - 3$ . No justification required.

**Claim:** The splitting field is  $\mathbb{Q}(\zeta_5, \sqrt[5]{3})$ .

*Proof.* The roots are  $\{\sqrt[5]{3}, \zeta_5 \sqrt[5]{3}, \zeta_5^2 \sqrt[5]{3}, \zeta_5^3 \sqrt[5]{3}, \zeta_5^4 \sqrt[5]{3}\}$ . □

- (b) (8 points) Let  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ . What is  $\text{Gal}(K/\mathbb{Q})$ ? Write down two elements of the group. No justification required.

**Claim:**  $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ .

*Proof.* The field  $K$  is the splitting field of the separable polynomial  $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$ , and  $[K : \mathbb{Q}] = 8$ . Therefore,  $|\text{Gal}(K/\mathbb{Q})| = 8$ . Elements of  $\text{Gal}(K/\mathbb{Q})$  are completely determined by what they do to the generators  $\sqrt{2}, \sqrt{3}, \sqrt{5}$ . Three identifiable elements of order two in  $\text{Gal}(K/\mathbb{Q})$  are

- i.  $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}; \sigma_2$  fixes  $\sqrt{3}, \sqrt{5}$ .
- ii.  $\sigma_3 : \sqrt{3} \mapsto -\sqrt{3}; \sigma_3$  fixes  $\sqrt{2}, \sqrt{5}$ .
- iii.  $\sigma_5 : \sqrt{5} \mapsto -\sqrt{5}; \sigma_5$  fixes  $\sqrt{2}, \sqrt{3}$ .

It follows that  $\text{Gal}(K/\mathbb{Q}) \cong \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle \times \langle \sigma_5 \rangle$ . □

- (c) (9 points) Let  $\zeta_7 = e^{2\pi i/7} = \cos(2\pi/7) + i\sin(2\pi/7)$ .

- i. Use this fact to write  $\cos(2\pi/7)$  in terms of  $\zeta_7$ .

**Solution:**  $\cos(2\pi/7) = \frac{\zeta_7 + \zeta_7^{-1}}{2}$ .

- ii. What is the minimal polynomial of  $\zeta_7$ ? No justification required.

**Solution:**  $\Phi_7(x) := x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ .

- iii. Conclude that  $\cos(2\pi/7)$  is algebraic of degree at most 6. Explain your reasoning. For a challenge, compute its degree over  $\mathbb{Q}$  and generalize for  $\cos(2\pi/p)$  where  $p$  is prime.

*Proof.* Part (ii) implies that  $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ . Part (i) implies that  $\cos(2\pi/7) \in \mathbb{Q}(\zeta_7)$ . Therefore, we have  $[\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] \leq 6$ .

Now, let  $p \geq 3$  be prime. Then  $2\cos(2\pi/p) = \zeta_p + \zeta_p^{-1} \in \mathbb{Q}(\zeta_p)$ . Consider the polynomial  $f(x) = x^2 - (\zeta_p + \zeta_p^{-1})x + 1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})[x]$ . It has roots  $\zeta_p, \zeta_p^{-1} \notin \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Therefore,  $f(x)$  is irreducible in  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})[x]$ . It follows that  $[\mathbb{Q}(\zeta_p, \zeta_p + \zeta_p^{-1}) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$ . Noting that  $\mathbb{Q}(\zeta_p, \zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\zeta_p)$ , we write  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] \cdot [\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ . Hence, we conclude that  $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{p-1}{2}$ . □

5. (24 points) No justification required.

- (a) (7 points) Let  $K$  and  $F$  be fields with  $F \supseteq K$ , and let  $u \in F$ . Write down what it means for  $f_{K,u}(x)$  to be the minimal polynomial of  $u$  over  $K$ . There several equivalent ways to formulate an answer.

**Solution:** The following are equivalent formulations of the definition:

- The polynomial  $f_{K,u}(x)$  is monic, irreducible in  $K[x]$ , and has  $u$  as a root.
- The polynomial  $f_{K,u}(x)$  is monic of least degree in  $K[x]$  with  $u$  as a root.
- The polynomial  $f_{K,u}(x)$  is monic with the property that if  $g(x) \in K[x]$  has  $u$  as a root, then  $f(x) \mid g(x)$ .
- The polynomial  $f_{K,u}(x) \in K[x]$  is the monic generator for the kernel of the evaluation homomorphism  $\phi_u : K[x] \rightarrow F$ ; i.e., we have  $\ker \phi_u = (f(x))$ .

- (b) (10 points) Let  $K$  and  $F$  be fields with  $F \supseteq K$ , and let  $a, b \in F$ . Identify the statement(s) which is(are) **always true**.

- i. Let  $a$  and  $b$  be algebraic over  $K$ . Then  $a + b$  is algebraic over  $K$ .

**Solution:** True. The elements of  $F$  which are algebraic over  $K$  form a field; hence they are closed under addition.

- ii. Let  $a$  and  $b$  be transcendental over  $K$ . Then  $a + b$  is transcendental over  $K$ .

**Solution:** False. Both  $\pi$  and  $-\pi$  are transcendental, but  $\pi + (-\pi) = 0$  is not. It is worth noting that there instances in which it is not known whether the sum of transcendentals is transcendental. For example, it is not known whether  $\pi + e$  is transcendental.

- iii. Let  $a$  be algebraic over  $K$ , and let  $b$  be transcendental over  $K$ . Then  $a + b$  is algebraic over  $K$ .

**Solution:** False. In fact, this is never true. Let  $c := a + b$ , and suppose that  $c$  is algebraic. Then since  $a$  is algebraic, and elements algebraic over  $K$  are closed under addition (in fact, these elements constitute a field), we have  $c - a = b$  algebraic, a contradiction.

- iv. Let  $a$  be algebraic over  $K$ , and let  $b$  be transcendental over  $K$ . Then  $a + b$  is transcendental over  $K$ .

**Solution:** True since part (c) is never true.

- (c) (7 points) Let  $K$  and  $F$  be fields with  $F \supseteq K$ , and let  $u \in F$ . Identify the statement(s) which is(are) **always true**.

- i. An element  $u \in F$  is algebraic over  $K$  if and only if  $[K(u) : K]$  is finite.

**Solution:** True.

- ii. The field  $F$  is algebraic over  $K$  if and only if  $[F : K]$  is finite.

**Solution:** False. A standard counterexample is given by

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

6. **Challenge problem:** Show that  $\text{Gal}(\mathbb{R}/\mathbb{Q}) = \langle 1 \rangle$ .

Possible steps:

- (a) Show that for all  $\sigma \in \text{Gal}(\mathbb{R}/\mathbb{Q})$ , and for all  $u > v$  in  $\mathbb{R}$ , we have  $\sigma(u) > \sigma(v)$ . (For this, use the fact that  $x > 0$  in  $\mathbb{R}$  has a square root.
- (b) Now, suppose that for some  $u \in \mathbb{R}$ ,  $\sigma(u) \neq u$ . Use the fact that  $\sigma$  fixes  $\mathbb{Q}$  to reach a contradiction.

*Proof.* Let  $\sigma \in \text{Gal}(\mathbb{R}/\mathbb{Q})$ , and suppose that  $u > 0$  in  $\mathbb{R}$ . Then there is  $x \in \mathbb{R}$  with  $x^2 = u$ . We apply  $\sigma$  to obtain  $\sigma(u) = \sigma(x^2) = \sigma(x)^2 > 0$ . Now, let  $u > v$  in  $\mathbb{R}$ . Then we have  $u - v > 0$ , so  $\sigma(u - v) = \sigma(u) - \sigma(v) > 0$ . Hence, we conclude that  $\sigma(u) > \sigma(v)$ .

Now, suppose, by way of contradiction, that for some  $u \in \mathbb{R}$ , we have  $\sigma(u) \neq u$ . Then we have either  $\sigma(u) < u$  or  $\sigma(u) > u$ .

- Suppose that  $\sigma(u) < u$ . Then there is  $x \in \mathbb{Q}$  with  $\sigma(u) < x < u$ . Since  $x \in \mathbb{Q}$  and  $\sigma \in \text{Gal}(\mathbb{R}/\mathbb{Q})$ , we find that  $\sigma(x) = x$ . Moreover, since  $x < u$ , part (a) (proved above) implies that  $x = \sigma(x) < \sigma(u)$ , which contradicts  $\sigma(u) < x$ .
- Suppose that  $\sigma(u) > u$ . The same type of argument applies. There is  $y \in \mathbb{Q}$  with  $\sigma(u) > y > u$ . The automorphism  $\sigma$  fixes  $y$  and  $y > u$  implies that  $y = \sigma(y) > \sigma(u)$ , which contradicts  $\sigma(u) > y$ .

□

**Extra scratch paper.**