⋄ ⋄ ⋄ ⋄ MATH 8220: ABSTRACT ALGEBRA I ⋄ ⋄ ⋄ ⋄
HOMEWORK SETS AND EXAMS

Yongwei Yao

2024 FALL SEMESTER
GEORGIA STATE UNIVERSITY

Contents

Each homework set contains four (4) regular problems. When solving the problems, make sure your arguments are rigorous and complete.

Problems for extra credits are available; see the last page of this file.

There are three (3) PDF files for the homework sets and exams, one with the problems only, one with hints, and one with solutions. Links are available below.

PROBLEMS HINTS SOLUTIONS

Problem 1.1. Consider $f(x) = 2x^3 - x^2 + x + 1$, $g(x) = x^3 + 2x^2 + 3x + 1 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$.

(1) Determine whether $f(x)$ has a root in $\mathbb{Q}$.
(2) Determine whether $f(x)$ is irreducible in $\mathbb{Q}[x]$.
(3) Is $f(x)$ is irreducible in $\mathbb{Z}[x]$? If not, find a non-trivial factorization of $f(x)$ in $\mathbb{Z}[x]$.
(4) Determine whether $g(x)$ has a root in $\mathbb{Q}$.
(5) Determine whether $g(x)$ is irreducible in $\mathbb{Q}[x]$. Is $g(x)$ irreducible in $\mathbb{Z}[x]$?

Hint. This should be straightforward. Use the results covered in class.

Problem 1.2. Consider $h(x) = x^3 + \overline{2}x^2 + \overline{3}x + \overline{1} \in \mathbb{Z}_5[x]$, where $\mathbb{Z}_5 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\}$.

(1) Determine whether $h(x)$ has a root in $\mathbb{Z}_5$.
(2) Determine whether $h(x)$ is irreducible in $\mathbb{Z}_5[x]$.
(3) Write $h(x)$ as a product of *monic* irreducible polynomials in $\mathbb{Z}_5[x]$. Explain why each of the factors is irreducible.

Hint. Well, $\mathbb{Z}_5$ is a *finite* field. A monic polynomial has leading coefficient 1 by definition.

Problem 1.3. Show that each the following polynomials is irreducible in $\mathbb{Q}[x]$.

(1) $f_1(x) = 3x^4 - 7x^3 + 7x^2 + 7$.
(2) $f_2(x) = 2x^4 - 90x^3 + 63x^2 - 84x + 105$.
(3) $f_3(x) = 2x^4 - 24x^3 + 48x^2 - 12x + 28$.

Hint. Use Eisenstein's Criterion.

Problem 1.4. Consider the polynomial $p(x) = x^3 + 2x^2 - 4x + 6$, which is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion. Let $u \in \mathbb{C}$ be a (fixed) root of $p(x)$. (Such a root exists in $\mathbb{C}$. In fact, $p(x)$ has at least one root in $\mathbb{R}$ by the Intermediate Value Theorem in calculus.) Consider $\mathbb{Q}[u] = \{a_0 + a_1u + a_2u^2 \mid a_i \in \mathbb{Q}\}$, which is a ring. In fact, $\mathbb{Q}[u]$ is a field. This exercise illustrates how to find the inverse of a (typical) non-zero element in $\mathbb{Q}[u]$. (Here u is not an indeterminate, and $\mathbb{Q}[u]$ is not a polynomial ring.)

As an example, we compute the inverse of $2 + 3u$ and illustrate that it is indeed in $\mathbb{Q}[u]$. Consider the polynomial $f(x) = 3x + 2 \in \mathbb{Q}[x]$. Complete the following:

(1) Find $\gcd(p(x), f(x))$ by the Euclidean Algorithm (repeated division) for polynomials. (Note that $\gcd(p(x), f(x))$ should be 1 as $p(x) \nmid f(x)$ and $p(x)$ is irreducible in $\mathbb{Q}[x]$.)
(2) Use your work in (1) to express 1 as a linear combination of $p(x)$ and $f(x)$. That is, find $a(x),\ b(x) \in \mathbb{Q}[x]$ such that $1 = a(x)p(x) + b(x)f(x)$.
(3) Show that $b(u)f(u) = 1$, so that $(f(u))^{-1} = b(u)$. Finally, show $(2+3u)^{-1} \in \mathbb{Q}[u]$ by writing $(2+3u)^{-1}$ in the form of $a_0 + a_1u + a_2u^2$ with $a_i \in \mathbb{Q}$.

Hint. Just complete (1), (2) and (3) as instructed. In (3), just evaluate the equation derived in (2) at $x = u$. You do **not** need to prove any of the claims in the first paragraph (such as that $\mathbb{Q}[u]$ is a field, etc.). **The solution is very short actually.**

PROBLEMS HINTS SOLUTIONS

Problem 2.1. Let $F \subseteq K$ be a field extension such that $[K : F] < \infty$. Let $\alpha \in K$ and $p(x)$ be the minimal polynomial of α over F.

(1) Prove that if $\deg(p(x)) > \frac{1}{2}[K : F]$ then $F(\alpha) = K$.

(2) Prove that if $[K : F]$ is a prime number and $\alpha \in K \setminus F$ then $F(\alpha) = K$.

Hint. In both (1) and (2), use the relation among $[K : F]$, $[K : F(\alpha)]$ and $[F(\alpha) : F]$. Feel free to use the **fact** (an easy fact from linear algebra, in disguise) that if $F \subseteq K_1 \subseteq K_2$ is a field extension such that $[K_1 : F] = [K_2 : F] < \infty$ then $K_1 = K_2$.

Problem 2.2. Let $F \subseteq K$ be a field extension, $\omega \in K$ and $p(x) \in F[x]$. Prove that, if $p(x)$ is monic and irreducible in $F[x]$ such that $p(\omega) = 0$, then $p(x)$ is the minimal polynomial of ω over F.

Hint. Let $m(x)$ be the minimal polynomial of ω over F. Can you show $p(x) = m(x)$?

Problem 2.3. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{R}$. Show $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Hint. Here is a direct and short approach: Clearly $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. So it remains to show that both $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, which would imply $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that $(\sqrt{2} + \sqrt{3})^n$ are all in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Can you “get” both $\sqrt{2}$ and $\sqrt{3}$ from the powers of $\sqrt{2}+\sqrt{3}$? Do the algebra! (Other ways are available, and are welcome.)

Problem 2.4. Consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}(u) \subseteq \mathbb{C}$ in which $u \in \mathbb{C}$ is a (fixed) root of $p(x) = x^3 + 2x^2 - 4x + 6$ and $\mathbb{Q}(u) = \mathbb{Q}[u] = \{a_0 + a_1u + a_2u^2 \mid a_i \in \mathbb{Q}\}$; see Problem 1.4. Express $(3 - 2u + u^2)^{-1}$ in the form of $a_0 + a_1u + a_2u^2$ with $a_i \in \mathbb{Q}$.

Hint. See Problem 1.4. Here it takes more steps to complete the Euclidean Algorithm.

PROBLEMS HINTS SOLUTIONS

Problem 3.1. Prove the following **lemma**: *Let $F \subseteq K$ be a field extension, $\omega \in K$ and $p(x) \in F[x]$ such that $p(\omega) = 0$. If $p(x)$ is monic and* $\deg(p(x)) = [F(\omega) : F]$, *then $p(x)$ is the minimal polynomial of ω over F.*

Hint. Let $m(x)$ be the minimal polynomial of ω over F.

Problem 3.2. Consider the field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{3}}) \subseteq \mathbb{C}$.

(1) Show $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2+\sqrt{3}})$.
(2) Prove $\sqrt{2+\sqrt{3}} \notin \mathbb{Q}(\sqrt{3})$, so that $\mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2+\sqrt{3}})$.
(3) Determine $\left[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})\right]$ and $\left[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}\right]$.

Hint. (2) If $\sqrt{2+\sqrt{3}} \in \mathbb{Q}(\sqrt{3})$, then there would be a, $b \in \mathbb{Q}$ such that $\sqrt{2+\sqrt{3}} = a + b\sqrt{3}$.
(3) What is the minimal polynomial of $\sqrt{2+\sqrt{3}}$ over $\mathbb{Q}(\sqrt{3})$? Justify fully.

Problem 3.3. Consider $\sqrt{2+\sqrt{3}} \in \mathbb{R}$ as in Problem 3.2. Find the minimal polynomial of $\sqrt{2+\sqrt{3}}$ over $\mathbb{Q}$ **with rigorous justification**.

Hint. Do some algebra with $\sqrt{2+\sqrt{3}}$. To show the polynomial you get is indeed the minimal polynomial, you might want to use the result in Problem 3.1.

Problem 3.4. Let $\alpha \in \mathbb{R} \setminus \{0\}$ be a (fixed) real number such that $\alpha^{-1} \in \mathbb{Q}[\alpha]$. To be concrete, suppose $\alpha^{-1} = \frac{5}{6}\alpha^4 - \alpha^3 + 2\alpha^2 - 3\alpha + 4$. Show that α is algebraic over $\mathbb{Q}$ and find the minimal polynomial of α over $\mathbb{Q}$.

Hint. Include your step-by-step work and justification.

PROBLEMS HINTS SOLUTIONS

Problem 4.1. Consider $\sqrt[3]{2} + \sqrt[3]{4}$, which is algebraic over $\mathbb{Q}$.

(1) Determine $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, with justification.

(2) True or false: $\mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2})$. Please justify your claim.

Hint. Feel free to use the results we have learned (in class or in **homework**).

Problem 4.2. Find the minimal polynomial of $\sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

Hint. Here is a way: Write $(\sqrt[3]{2} + \sqrt[3]{4})^i$, $0 \leqslant i \leqslant 3$, as linear combinations of 1, $\sqrt[3]{2}$ and $\sqrt[3]{4}$ over $\mathbb{Q}$. Find a_0, a_1, a_2, $a_3 \in \mathbb{Q}$, not all zero, such that $\sum_{i=0}^{3} a_i(\sqrt[3]{2} + \sqrt[3]{4})^i = 0$.

Problem 4.3. Prove the following **theorem**: *For field extensions $F \subseteq K \subseteq L$, if L is algebraic over K and K is algebraic over F, then L is algebraic over F.*

Hint. Let $u \in L$. As u is algebraic over K, there exists $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x] \setminus \{0\}$ such that $p(u) = 0$. What can be said about u over $F(a_0, a_1, \ldots, a_n)$? What can be said about $[F(a_0, a_1, \ldots, a_n, u) : F]$? Show your reasoning.

Problem 4.4. Let $F \subseteq K$ be a field extension such that every irreducible polynomial in $F[x]$ remains irreducible in $K[x]$. Prove that F is algebraically closed in K (that is, prove that $F = \{u \in K \mid u \text{ is algebraic over } F\}$). (See Problem E-5 for the converse.)

Hint. It suffices to show that if $u \in K$ is algebraic over F then u must be in F. For such an element u, let $m_F(x)$ be the minimal polynomial of u over F, and $m_K(x)$ be the minimal polynomial of u over K. You might want to consider the following ingredients

- Relations between $m_F(x)$ and $m_K(x)$.
- The fact that $m_K(x)$ can be determined *explicitly* and *easily*.

Feel free to try your own approach(es), as always.

PROBLEMS HINTS SOLUTIONS

Irreducible polynomials, roots: Problems 1.1, 1.2, 1.3.

Computing products, quotients: Problems 1.4, 2.4.

Field extensions & extension degrees: Problems 2.1, 2.3, 4.1, 4.2, 4.3, 4.4.

Minimal polynomials & extension degrees: Problems 2.2, 3.1, 3.2, 3.3, 3.4, 4.1, 4.2.

Abstract problems on field extensions: Problems 2.1, 2.2, 3.1, 4.3, 4.4.

Lecture notes and textbooks: All we have covered in class.

Note: The above list is not intended to be complete. The problems in the actual test may vary in difficulty as well as in content. Going over, understanding, and digesting the problems listed above will definitely help. However, simply memorizing the solutions of the problems may not help you as much.

You are strongly encouraged to practice more problems (than the ones listed above) on your own.

Irreducible elements. Let R be a commutative ring with 1 and $0 \neq r \in R \setminus \mathrm{U}(R)$. We say r is irreducible if, for a, $b \in R$, $r = ab$ necessarily implies $a \in \mathrm{U}(R)$ or $b \in \mathrm{U}(R)$.

Irreducible polynomials over fields. Let K be a field and $f(x) \in K[x]$. Then $f(x)$ is irreducible iff $f(x) \notin K$ and $f(x)$ is not a product of polynomials in $K[x]$ of lower degrees.

Polynomials in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$.

- We say $f(x)$ is primitive iff $\gcd(a_n, \ldots, a_1, a_0) = 1$.
- The product of primitive polynomials is primitive.
- $f(x)$ reducible in $\mathbb{Q}[x] \implies f(x)$ reducible in $\mathbb{Z}[x]$. If $f(x)$ is primitive, then $\iff$.
- All rational roots of $f(x)$ are contained in $\{\frac{r}{s} : r, s \in \mathbb{Z}, r \mid a_0, s \mid a_n\}$.
- If there exists a prime $p \in \mathbb{Z}$ such that $p \nmid a_n$, $p \mid a_i$ for all $i \leqslant n-1$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. (This is Eisenstein's Criterion.)

Field extensions. Let $F \subseteq K \subseteq L$ be field extensions. Let $u \in K$.

- The extension degree of K over F, $[K : F]$, is the vector space dimension of K/F.
- We say u is algebraic over F if there exists $f(x) \in F[x] \setminus \{0\}$ such that $f(u) = 0$.
- We say that K is algebraic over F if all elements of K are algebraic over F.
- If $[K : F] < \infty$, then K is algebraic over F.
- The algebraic closure of F in K is defined as $\overline{F}^K = \{a \in K \mid a \text{ is algebraic over } F\}$, which is known to be a field. If $\overline{F}^K = F$, we say F is algebraically closed in K.
- We have $[L : F] = [L : K][K : F]$.
- If L is algebraic over K and K is algebraic over F, then L is algebraic over F.

Minimal polynomials. Let $F \subseteq K$ be a field extension and $u \in K$ algebraic over F. The minimal polynomial of u over F is the monic $m(x) \in F[x]$ of least degree such that $m(u) = 0$.

- For $f(x) \in F(x)$, $f(u) = 0 \iff m(x) \mid f(x)$. Also, $m(x)$ is irreducible in $F[x]$.
- We have $F(u) = F[u] \cong F[x]/(m(x))$, and $[F(u) : F] = \deg(m(x))$.
- If $\deg(m(x)) = n$, then $F(u) = F[u] = \{a_0 + a_1 u + \cdots + a_{n-1} u^{n-1} \mid a_i \in F\}$.

Constructing roots. Let F be a field and $p(x) \in F[x]$ be irreducible with $\deg(p(x)) = n$. Consider $K = F[x]/(p(x))$, which is a field. Denote $\overline{f(x)} = f(x) + (p(x)) \in F[x]/(p(x))$.

- The map $h : F \to K$ defined by $h(r) = \overline{r}$ is an injective ring homomorphism.
- Identify F as a subfield of K via h, we see $\overline{x}$ is a root of $p(y) \in F[y]$.
- In fact, $p(y)$ (up to the leading coefficient) is the minimal polynomial of $\overline{x}$ over F.
- We have $[K : F] = n$ and $K = \{a_0 + a_1 \overline{x} + \cdots + a_{n-1} \overline{x}^{n-1} \mid a_i \in F\}$.

Algebraic closure. Let $F \subseteq C$ be a field extension.

- We say C is algebraically closed if one (or all) of the following holds
  - There is no proper field extension of C that is algebraic.
  - All irreducible polynomials in $C[x]$ have degree 1.
  - Every $f(x) \in C[x] \setminus C$ is a product of linear factors.
  - Every $f(x) \in C[x] \setminus C$ has (at least) one root in C.
- C is a algebraic closure of F iff C is algebraic over F and C is algebraically closed.
- Every field has an algebraic closure, and it is unique up to isomorphism.

Note: The above list is not intended to be complete.

Hints

have been withdrawn

from the site

PROBLEMS HINTS SOLUTIONS

Problem 5.1. Let $F \subseteq K_\lambda \subseteq L$ be field extensions such that each K_λ is normal over F, where $\lambda \in \Lambda \neq \varnothing$. Denote $K = \cap_{\lambda\in\Lambda} K_\lambda$. Prove that K is a normal extension of F.

Hint. Use one of the criteria for normal extension covered in class.

Problem 5.2. Let F be any field and $f(x) \in F[x]$ with $\deg(f(x)) = n > 0$. Let K be a splitting field of $f(x)$ over F. Prove $[K : F] \leqslant n!$.

Hint. One way to prove the claim is by induction. Present your proof rigorously.

Problem 5.3. Let K be a splitting field of $x^n - a$ over $\mathbb{Q}$, in which $a \in \mathbb{Q}\backslash\{0\}$ and $1 \leqslant n \in \mathbb{Z}$. Prove $K = \mathbb{Q}(u, v)$ for some $u, v \in K$. Assume $K \subseteq \mathbb{C}$ without loss of generality.

Hint. Let $u \in \mathbb{C}$ be a/any root of $x^n - a$, which exists (of course); and let $v = e^{\frac{2\pi}{n}i} \in \mathbb{C}$. What are all the roots of $x^n - a$ in $\mathbb{C}$? Can you show $K = \mathbb{Q}(u, v)$?

Problem 5.4. Let K be a splitting field of $x^6 - 2$ over $\mathbb{Q}$. Determine $[K : \mathbb{Q}]$ as follows. Assume $K \subseteq \mathbb{C}$ without loss of generality. Let $u = \sqrt[6]{2}$ and $v = e^{\frac{\pi}{3}i}$.

(1) True or false: $K = \mathbb{Q}(u, v)$. Explain why.
(2) Determine $[\mathbb{Q}(u) : \mathbb{Q}]$ with rigorous justification.
(3) Determine $[\mathbb{Q}(u, v) : \mathbb{Q}(u)]$ with rigorous justification.
(4) Find $[K : \mathbb{Q}]$. (*Feel free to find* $[K : \mathbb{Q}]$ *without going through (1)–(3).*)

Hint. (3) Note that $v = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. What is the minimal polynomial of v over $\mathbb{Q}$? Is v contained in $\mathbb{Q}(u)$? These questions should help you figure out $[\mathbb{Q}(u, v) : \mathbb{Q}(u)]$ precisely.

(4) This should follow from (1)–(3) immediately.

The main goal of this exercise is to find $[K : \mathbb{Q}]$*. If you can accomplish this via other approaches, feel free to present them. That is, you may skip parts (1)–(3), as long as you are able to find* $[K : \mathbb{Q}]$ *with rigorous justification.*

Problem 6.1. Let F be a field of characteristic $p > 0$ and $f(x) = \sum_{i=0}^{d} a_i x^i$ an irreducible polynomial in $F[x]$. Prove that the following statements are equivalent to one another.

(1) All roots of $f(x)$ in all splitting fields of $f(x)$ over F are multiple.
(2) $f(x)$ has a multiple root in some extension field of F.
(3) $a_i = 0$ for all $0 \leqslant i \leqslant d$ such that $p \nmid i$.
(4) $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Hint. Use the theorems proved in class concerning $f'(x)$. Given $\operatorname{char}(F) = p > 0$, $a \in F$ and $n \in \mathbb{Z}$, we have $na = 0_F \iff p \mid n$ or $a = 0_F$. The proof is not long at all.

Problem 6.2. Let F be a field of characteristic $p > 0$. Consider $f(x) = x^{p^n} - a$ where $0 \leqslant n \in \mathbb{Z}$ and $a \in F$. (Here x^{p^n} stands for $x^{(p^n)}$.) Let K be a splitting field of $f(x)$ over F. Prove that $x^{p^n} - a$ has precisely one root, with multiplicity p^n, in K.

Hint. There exists $u \in K$ such that $f(u) = 0$. Now, given this u, can you factor $f(x)$ completely over K? Make use of the assumption that K has a prime characteristic p.

Problem 6.3. Let F be a field of characteristic 0, $r \in F$ and $f(x) \in F[x] \setminus F$. Let $m \in \mathbb{N}$. Prove that the following statements are equivalent to each other:

(1) r is a root of $f(x)$ with multiplicity m.
(2) $f(r) = 0$ and r is a root of $f'(x)$ of multiplicity $m - 1$.

(We agree that r is a root of $f'(x)$ of multiplicity 0 if and only if $f'(r) \neq 0$.)

Hint. All should be straightforward, relying on basic definitions and $\operatorname{char}(F) = 0$.

Problem 6.4. Let F be a field of characteristic 0, $r \in F$ and $f(x) \in F[x] \setminus F$. Let $m \in \mathbb{N}$. Prove that the following statements are equivalent to each other:

(1) r is a root of $f(x)$ with multiplicity m.
(2) $f^{(i)}(r) = 0$ for all $i = 0, 1, \ldots, m - 1$ and $f^{(m)}(r) \neq 0$.

(Here $f^{(0)}(x) = f(x)$ and, recursively, $f^{(n+1)}(x) = (f^{(n)}(x))'$ for all $n \geqslant 0$; so $f^{(1)} = f'(x)$.)

Hint. You might want to use Problem 6.3. One way to present your proof is by induction on m. Present your proof rigorously.

PROBLEMS HINTS SOLUTIONS

Problem 7.1. Let F be a field of characteristic $p > 0$ (hence p is prime) and let $a \in F$. Prove that $x^p - a$ either factors completely in $F[x]$ or is irreducible in $F[x]$.

Hint. Fix an extension field K of F such that $x^p - a$ has a root, say r, in K. Let $m(x)$ be the minimial polynomial of r over F and examine the relations between $m(x)$ and $x^p - a$. Other approaches are available and are (of course) welcome.

Problem 7.2. Let $F \subseteq K$ be an extension of fields of characteristic $p > 0$ (hence p is prime). Define $E = \{a \in K \mid a^{p^n} \in F \text{ for some integer } n \geqslant 0\}$. Determine whether the following statements are **true or false**, with **justifications**.

(1) $F \subseteq E \subseteq K$.

(2) E is a field (under the operations of $(K, +, \cdot)$), that is, E is a subfield of K.

Hint. All should be straightforward. For (2), you might want to review one of the subfield criteria (i.e., subring criteria plus every non-zero element being invertible). Make use of the assumption that $\operatorname{char}(K) = p > 0$.

Problem 7.3. Let F be a fields of prime characteristic $p > 0$. Prove (1) $\Rightarrow$ (2).

(1) All algebraic field extensions of F are separable over F.

(2) $F = \{u^p \mid u \in F\}$.

Hint. Feel free to use what we have proved in class or in homework.

Problem 7.4. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$, all subfields of $\mathbb{C}$.

(1) True or false: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is a Galois extension. Show your justification.

(2) True or false: $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ is a Galois extension. Show your justification.

(3) True or false: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is a Galois extension. Show your justification.

Hint. All should be straightforward. Recall that a field extension $F \subseteq K$ is Galois if it is both normal and separable.

PROBLEMS HINTS SOLUTIONS

Problem 8.1. Consider the Galois extension $\mathbb{Q} \subseteq E$ where $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have seen in class that $\operatorname{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ where σ_i are determined by

$$e = \sigma_1 : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto \sqrt{3}; \qquad \sigma_3 : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto \sqrt{3};$$
$$\sigma_2 : \sqrt{2} \mapsto \sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}; \qquad \sigma_4 : \sqrt{2} \mapsto -\sqrt{2},\ \sqrt{3} \mapsto -\sqrt{3}.$$

(1) Compute $\sigma_2(1 - 2\sqrt{2} + 3\sqrt{3} - 4\sqrt{6})$.
(2) Let $H = \{\sigma_1, \sigma_4\}$. Find $u \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $E_H = \mathbb{Q}(u)$.
(3) Let $K = \mathbb{Q}(5\sqrt{2} + 8\sqrt{3})$. Determine $\operatorname{Gal}(E/K)$.
(4) Prove $\mathbb{Q}(5\sqrt{2} + 8\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Compare with Problem 2.3.)

Hint. For (2), first determine E_H and, then, u should be clear. For (4), the fundamental theorem of Galois theory says $K = E_{\operatorname{Gal}(E/K)}$; So we might want to examine $E_{\operatorname{Gal}(E/K)}$.

Problem 8.2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\operatorname{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ be as in Problem 8.1.

(1) Determine the group structure of $\operatorname{Gal}(E/\mathbb{Q})$. Explain why.
(2) Find *all* (proper and improper) subgroups of $\operatorname{Gal}(E/\mathbb{Q})$ explicitly.
(3) Find *all* intermediate fields K between $\mathbb{Q}$ and E explicitly, including $\mathbb{Q}$ and K.

Hint. For (1), compute σ_i^2 for all $\sigma_i \in \operatorname{Gal}(E/\mathbb{Q})$. For (3), the fundamental theorem of Galois theory says that there is an one-one correspondence between the subgroups and the intermediate fields. **No justification is necessary for (2) and (3)**.

Problem 8.3. Consider the Galois group of $x^4 - 2$ over $\mathbb{Q}$, $\operatorname{Gal}(E/\mathbb{Q})$ where $E = \mathbb{Q}(\sqrt[4]{2}, i)$. It can be shown that $\operatorname{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_8\}$ in which σ_i are determined by

$$i \overset{\sigma_1}{\mapsto} i,\ \sqrt[4]{2} \overset{\sigma_1}{\mapsto} \sqrt[4]{2}; \quad i \overset{\sigma_3}{\mapsto} i,\ \sqrt[4]{2} \overset{\sigma_3}{\mapsto} -\sqrt[4]{2}; \quad i \overset{\sigma_5}{\mapsto} -i,\ \sqrt[4]{2} \overset{\sigma_5}{\mapsto} \sqrt[4]{2}; \quad i \overset{\sigma_7}{\mapsto} -i,\ \sqrt[4]{2} \overset{\sigma_7}{\mapsto} -\sqrt[4]{2};$$
$$i \overset{\sigma_2}{\mapsto} i,\ \sqrt[4]{2} \overset{\sigma_2}{\mapsto} \sqrt[4]{2}\, i; \quad i \overset{\sigma_4}{\mapsto} i,\ \sqrt[4]{2} \overset{\sigma_4}{\mapsto} -\sqrt[4]{2}\, i; \quad i \overset{\sigma_6}{\mapsto} -i,\ \sqrt[4]{2} \overset{\sigma_6}{\mapsto} \sqrt[4]{2}\, i; \quad i \overset{\sigma_8}{\mapsto} -i,\ \sqrt[4]{2} \overset{\sigma_8}{\mapsto} -\sqrt[4]{2}\, i.$$

(1) Let $H = \{\sigma_1, \sigma_8\}$. Find $u \in \mathbb{Q}(\sqrt[4]{2}, i)$ such that $E_H = \mathbb{Q}(u)$.
(2) Let $K = \mathbb{Q}(\sqrt[4]{2} + i)$. Determine $\operatorname{Gal}(E/K)$.
(3) Prove $\mathbb{Q}(\sqrt[4]{2} + i) = \mathbb{Q}(\sqrt[4]{2}, i)$. (Compare with Problem 2.3 and Problem 8.1.)

Hint. See the hint for Problem 8.1.

Problem 8.4. Let $G = \{e, a, b, c\}$ be a group of order 4 that is not cyclic (or equivalently, $a^2 = b^2 = c^2 = e$). (Such G is unique up to isomorphism, called the *Klein four-group.*) Let $V = \operatorname{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ as in Problem Problem 8.1.

(1) Let H be any group. Prove that H must be abelian if $x^2 = e$ for all $x \in H$.
(2) Complete the multiplication table (a.k.a. the *Cayley table*) of G. No need to justify.

$\cdot$	e	a	b	c
e				
a				
b				
c				

(3) True or false: $G \cong V$. **If it is true**, construct a group isomorphism explicitly.

Hint. This involves group theory. By default, e stands for the identity element of G.

Materials covered earlier: Homework Sets 1, 2, 3, 4; Exam I.

Splitting fields, normal extensions: Problems 5.1, 5.2, 5.3, 5.4, 7.4.

Simple roots, multiple roots, separable extensions: Problems 6.1, 6.2, 6.3, 6.4, 7.3.

Fields of characteristic $p > 0$: Problems 6.1, 6.2, 7.1, 7.2, 7.3.

Galois extensions, fundamental theorem of Galois theory: Problems 7.4, 8.1, 8.2, 8.3.

Group theory: Problems 8.4.

Lecture notes and textbooks: All we have covered.

Note: The above list is not intended to be complete. The problems in the actual test may vary in difficulty as well as in content. Going over, understanding, and digesting the problems listed above will definitely help. However, simply memorizing the solutions of the problems may not help you as much.

You are strongly encouraged to practice more problems (than the ones listed above) on your own.

Splitting fields. Let $F \subseteq K$ be a field extension and $f(x) \in F[x] \backslash F$. We say K is a splitting field of $f(x)$ over F iff $f(x) = a(x - r_1) \cdots (x - r_m)$ with $r_i \in K$ and $K = F(r_1, \ldots, r_m)$.

Normal extensions. Let $F \subseteq K$ be a field extension. We say K is a normal over F iff K is a splitting field of $\{f_i(x) \in F[x] \setminus F\}_{i \in \Lambda}$, a family of polynomials in $F[x]$.

An algebraic field extension $F \subseteq K$ is normal if and only if every irreducible polynomial in $F[x]$ that has a root in K can be factored completely over K if and only if ⟨omitted⟩.

Fields of prime characteristic $p > 0$, finite fields. Let F be a field.

- If $\operatorname{char}(F) = p > 0$, then $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ for all $a, b \in F$ and all $n \in \mathbb{N}$.
- Every finite field F has prime characteristic $p > 0$ and hence $|F| = p^n$ for some $n \geqslant 1$.
- For every prime number p and every $n \geqslant 1$, there is a field F such that $|F| = p^n$.

Separable extensions. Let $F \subseteq K \subseteq L$ be algebraic field extensions. Let $u \in K$.

- Given $f(x) \in F[x]$, u is a multiple root of $f(x)$ iff $f(u) = 0 = f'(u)$.
- A irreducible polynomial $p(x)$ over F has a multiple root in $\overline{F}$ iff $p'(x) = 0$.
- [Definition] We say u is separable over F iff u is a simple root of its minimal polynomial over F (iff the minimal polynomial of u over F has no multiple roots).
- [Definition] We say K is separable over F iff all elements of K are separable over F.
- If u is separable over F, then $F(u)$ is separable over F.
- L is separable over F if and only if L is separable over K and K is separable over F.
- The separable closure of F in L is $\{u \in L \mid u \text{ is separable over } F\}$, which is a field.
- If $[K : F] < \infty$ and K is separable over F, then there is $a \in K$ such that $K = F(a)$.
- We say F is perfect if every algebraic field extension of F is separable.

Automorphisms. Let $F \subseteq E$ be a (finite) field extension.

- An F-automorphism of E is an isomorphism $h : E \to E$ satisfying $h(a) = a, \forall\, a \in F$.
- All F-automorphisms of E form a group under composition, denoted $\operatorname{Aut}(E/F)$.
- For $H \subseteq \operatorname{Aut}(E/F)$, the fixed field of H is $E_H = \{u \in E \,|\, h(u) = u \text{ for all } h \in H\}$.
- $|\operatorname{Aut}(E/F)| \leqslant [E : F]$. For $H \leqslant \operatorname{Aut}(E/F)$, $H = \operatorname{Aut}(E/E_H)$ and $|H| = [E : E_H]$.

Galois extensions. Let $F \subseteq E$ be a finite field extension. We say E is Galois over F iff E is normal and separable over F iff $|\operatorname{Aut}(E/F)| = [E : F]$ iff $F = E_{\operatorname{Aut}(E/F)}$. When $F \subseteq E$ is Galois, we denote $\operatorname{Aut}(E/F) = \operatorname{Gal}(E/F)$, called the Galois group of E over F.

The fundamental theorem of Galois theory. Let $F \subseteq E$ be a Galois extension. Then, for any intermediate field K (so $F \subseteq K \subseteq E$) and for any $H \leqslant \operatorname{Gal}(E/F)$, we have

- $K = E_{\operatorname{Gal}(E/K)}$ and $[E : K] = |\operatorname{Gal}(E/K)|$. (Note that E is Galois over K.)
- $H = \operatorname{Gal}(E/E_H)$, $|H| = [E : E_H]$ and $|\operatorname{Gal}(E/F)|/|H| = [E_H : F]$.
- K is Galois over F iff K is normal over F iff $\operatorname{Gal}(E/K) \trianglelefteq \operatorname{Gal}(E/F)$.
- If K is normal (hence Galois) over F, then $\operatorname{Gal}(K/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.

Group theory. Groups, subgroups, normal subgroups, group homomorphisms, quotient groups, Lagrange's theorem, isomorphism theorems of homomorphisms, etcetera.

Note: The above list is not intended to be complete.

Hints

have been withdrawn

from the site

PROBLEMS HINTS SOLUTIONS

Problem 9.1. Let G be a group, X be a G-set, and $x,\ y \in X$. Using elementary arguments, prove that the following statements, (1)–(4), are equivalent:

(1) $Gx = Gy$;
(2) $x \in Gy$;
(3) $y \in Gx$;
(4) $Gx \cap Gy \neq \varnothing$.

Hint. All should follow from the definition of G-sets. Note that $Gx = \{g * x \mid g \in G\}$.

Problem 9.2. Let $S_3 = \{f_1,\ f_2,\ f_3,\ f_4,\ f_5,\ f_6\} = X$, in which

$$f_1 = (1) = e, \quad f_2 = (1\ \ 2), \quad f_3 = (1\ \ 3), \quad f_4 = (2\ \ 3), \quad f_5 = (1\ \ 2\ \ 3), \quad f_6 = (1\ \ 3\ \ 2).$$

Consider the action of S_3 on X by conjugation (i.e., $g * x = gxg^{-1}$ for all $g \in G$ and $x \in X$).

(1) For each $i = 1, \ldots, 6$, determine $C(f_i)$ and $N(f_i)$ explicitly. (Skip the details.)
(2) Does the results in (1) verify the equalities $|C(f_i)| = [S_3 : N(f_i)]$ for all $i = 1, \ldots, 6$?
(3) Verify that X is a disjoint union of the distinct conjugate classes (i.e., orbits).

Hint. (1) You don't need to show the details—answers are enough.
(2) & (3) Don't quote the theorems. Instead, verify the relevant theorems on S_3 directly.

Problem 9.3. Let $S_3 = \{f_1, \ldots, f_6\}$ be as in Problem 9.2 and $Y = \{H \mid H \leqslant S_3\}$. Consider the action of S_3 on Y by conjugation (i.e., $g * H = gHg^{-1}$ for all $g \in G$ and $H \in Y$).

(1) Determine all elements of Y explicitly. (Skip the details.)
(2) Let $H_1 = \{f_1,\ f_2\}$. Determine $C(H_1)$ and $N(H_1)$ explicitly. (Skip the details.)
(3) Let $H_2 = \{f_1,\ f_5,\ f_6\}$. Determine $C(H_2)$ and $N(H_2)$ explicitly. (Skip the details.)
(4) List all the distinct orbits (i.e., conjugate classes) in Y explicitly. (Skip the details.)

Hint. Don't miss the trivial subgroups of S_3. You may present your answers directly.

Problem 9.4. Let G be a finite group with $|G| = n$ and p a prime number such that $p \mid n$. Write $n = p^r m$ with $p \nmid m$. Let H be a Sylow p-subgroup of G (so that $|H| = p^r$). Let K be any subgroup of G such that $|K| = p^s$ for some integer s. Denote $L = K \cap N(H)$.

(1) True or false: (a) $L \leqslant N(H)$; (b) $H \trianglelefteq N(H)$; (c) $LH \leqslant N(H)$; (d) $LH \leqslant G$.
(2) Prove $L \subseteq H$. (Hence $L \leqslant H$.)

Hint. (1) If $B \leqslant A$, $C \leqslant A$ and $D \trianglelefteq A$, then $B \cap C \leqslant A$ and $BD \leqslant A$. No need to justify.
(2) Suppose $L \nsubseteq H$. Now, what can be said about $|L|/|L \cap H|$ and, hence, about $|LH|$? Do you see a contradiction?

PROBLEMS HINTS SOLUTIONS

You must solve a problem **completely and correctly** in order to get the extra credit. You may attempt a problem for as many times as you wish by 12/06.

The points you get here will be added to the total score from the homework assignments.

Each ★ represents a correct solution submitted.

Problem E-1 (3 points)**.** Let D be an integral domain (not necessarily commutative) and R a subring of D such that R is non-zero with unity 1_R. Prove that 1_R is the unity of D. (Thus, if R is a field, then D is naturally a vector space over R.)

Problem E-2 (3 points)**.** Let D be a commutative integral domain and F a subring of D such that F is a field and D has finite dimension as a vector space over F (cf. Problem E-1). Prove that D is a field.

Problem E-3 (3 points)**.** Let D be an integral domain and F a subring of D such that F is a field and D has finite dimension as a vector space over F (cf. Problem E-1). Prove that D is a division ring.

Problem E-4 (3 points)**.** Let $F \subseteq K$ be a field extension and $u \in K$ such that $[F(u) : F]$ is finite and odd. Prove $F(u) = F(u^2)$.

Problem E-5 (3 points)**. Prove or disprove**: If $F \subseteq K$ is a field extension such that F is algebraically closed in K, then every irreducible polynomial in $F[x]$ is irreducible in $K[x]$. (This is the converse of Problem 4.4.)

Problem E-6 (3 points)**.** Let F be a field with $\operatorname{char}(F) = p > 0$ and let C be an algebraic closure of F. Assume that F is separably closed in C. **Prove or disprove**: Every monic irreducible polynomial in $F[x]$ is of the form $x^{p^n} - a$ for some integer $n \geqslant 0$ and $a \in F$.

PROBLEMS HINTS SOLUTIONS