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

Yongwei Yao

2024 FALL SEMESTER
GEORGIA STATE UNIVERSITY

Contents

HW Set #01, Solutions	1
HW Set #02, Solutions	3
HW Set #03, Solutions	5
HW Set #04, Solutions	7
Midterm I, Review Problems	9
Midterm I, Review Topics	10
Midterm I, Solutions	11
HW Set #05, Solutions	12
HW Set #06, Solutions	14
HW Set #07, Solutions	16
HW Set #08, Solutions	18
Midterm II, Review Problems	20
Midterm II, Review Topics	21
Extra Credit Set, Solutions—not really	22

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

$F \subseteq K \subseteq E \ldots\ldots m_{\alpha,\,F}(x) \ldots\ldots E_H = K \iff \mathrm{Gal}(E/K) = H \ldots\ldots \mathbb{C} = \overline{\mathbb{C}} \ldots\ldots [G : N(P)] = |C(P)| = n_p \equiv 1 \mod p$

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 $\mathbb{Z}[x]$?

Solution. (1) By the Rational Root Theorem, the (possible) rational roots of $f(x)$ must be from $\left\{\pm\frac{1}{1}, \pm\frac{1}{2}\right\}$. Direct computation (of $f(\pm 1)$ and $f(\pm\frac{1}{2})$) shows

$$f(1) \neq 0, \quad f(-1) \neq 0, \quad f(\tfrac{1}{2}) \neq 0, \quad f(-\tfrac{1}{2}) = 0.$$

Therefore $f(x)$ has a root $-\frac{1}{2} \in \mathbb{Q}$. (In fact, $-\frac{1}{2}$ is the only rational root of $f(x)$.)

(2) Since $\deg(f(x)) > 1$ and $f(x)$ has a root in $\mathbb{Q}$, we see $f(x)$ is not irreducible in $\mathbb{Q}[x]$.

(3) Since $f(x) \in \mathbb{Z}[x]$ is not irreducible in $\mathbb{Q}[x]$, it is not irreducible in $\mathbb{Z}[x]$. By long division, we get $f(x) = (x + \frac{1}{2})(2x^2 - 2x + 2)$ over $\mathbb{Q}$. Correspondingly, we obtain

$$f(x) = (2x + 1)(x^2 - x + 1),$$

which is a non-trivial factorization of $f(x)$ in $\mathbb{Z}[x]$.

(4) By the Rational Root Theorem, the (possible) rational roots of $g(x)$ must be from $\left\{\frac{1}{1}, -\frac{1}{1}\right\}$. However, $g(1) \neq 0$ and $g(-1) \neq 0$. So $g(x)$ has no root in $\mathbb{Q}$.

(5) In light of (4) and the fact $\deg(g(x)) = 3$, we see $g(x)$ is irreducible in $\mathbb{Q}[x]$. Moreover, because $g(x)$ is primitive, $g(x)$ is irreducible also in $\mathbb{Z}[x]$.

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.

Solution. (1) By computing $h(\overline{0})$, $h(\overline{1})$, $h(\overline{2})$, $h(\overline{3})$ and $h(\overline{4})$ directly, we see

$$h(\overline{3}) = \overline{0}.$$

(2) Since $\deg(h(x)) \geqslant 2$ and $h(x)$ has a root in $\mathbb{Z}_5$, we see $h(x)$ is not irreducible in $\mathbb{Z}_5[x]$.

(3) Dividing $h(x)$ by $x - \overline{3}$ via long division, we get $h(x) = (x - \overline{3})(x^2 + \overline{3})$. By exhaustion, we see $x^2 + \overline{3}$ has no root in $\mathbb{Z}_5$, which implies $x^2 + \overline{3}$ is irreducible in $\mathbb{Z}_5[x]$. Thus

$$h(x) = (x - \overline{3})(x^2 + \overline{3}),$$

which is a product of monic irreducible polynomials in $\mathbb{Z}_5[x]$, as required.

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) $f_3(x) = 2x^4 - 24x^3 + 48x^2 - 12x + 28$.

Proof. (1) Applying Eisenstein's Criterion with $p = 7$, we see $f_1(x)$ is irreducible in $\mathbb{Q}[x]$.

(2) Applying Eisenstein's Criterion with $p = 3$ to $f_2(x)$, we see $f_2(x)$ is irreducible in $\mathbb{Q}[x]$.

(3) As $f_3(x) = 2(x^4 - 12x^3 + 24x^2 - 6x + 14)$, it suffices to show $x^4 - 12x^3 + 24x^2 - 6x + 14$ is irreducible in $\mathbb{Q}[x]$. Applying Eisenstein's Criterion with $p = 2$ to $x^4 - 12x^3 + 24x^2 - 6x + 14$, we see $x^4 - 12x^3 + 24x^2 - 6x + 14$ is irreducible in $\mathbb{Q}[x]$. Thus $f_3(x)$ is also irreducible in $\mathbb{Q}[x]$. (Note that $f_3(x)$ is reducible in $\mathbb{Z}[x]$ though.) $\square$

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 $a_i \in \mathbb{Q}$.

Solution. (1) To find $\gcd(p(x), f(x))$, we apply the Euclidean Algorithm as follows

$$\begin{aligned} p(x) &= (\tfrac{1}{3}x^2 + \tfrac{4}{9}x - \tfrac{44}{27})f(x) + \tfrac{250}{27}, \\ f(x) &= (\tfrac{27}{250}f(x))\tfrac{250}{27} + 0. \end{aligned}$$

The monic polynomial associated with $\frac{250}{27}$ is 1. Thus $\gcd(p(x), f(x)) = 1$.

(2) From the work in (1) above, we have $\frac{250}{27} = p(x) - (\frac{1}{3}x^2 + \frac{4}{9}x - \frac{44}{27})f(x)$. Therefore

$$\begin{aligned} 1 = \tfrac{27}{250} \cdot \tfrac{250}{27} &= \tfrac{27}{250}\left[p(x) - (\tfrac{1}{3}x^2 + \tfrac{4}{9}x - \tfrac{44}{27})f(x)\right] \\ &= \tfrac{27}{250}p(x) - \tfrac{27}{250}(\tfrac{1}{3}x^2 + \tfrac{4}{9}x - \tfrac{44}{27})f(x) \\ &= \tfrac{27}{250}p(x) + (-\tfrac{9}{250}x^2 - \tfrac{6}{125}x + \tfrac{22}{125})f(x). \end{aligned}$$

(3) Evaluating $1 = \frac{27}{250}p(x) + (-\frac{9}{250}x^2 - \frac{6}{125}x + \frac{22}{125})f(x)$ at $x = u$ and observing $p(u) = 0$, we see

$$1 = \tfrac{27}{250}p(u) + (-\tfrac{9}{250}u^2 - \tfrac{6}{125}u + \tfrac{22}{125})f(u) = (-\tfrac{9}{250}u^2 - \tfrac{6}{125}u + \tfrac{22}{125})(2 + 3u).$$

Thus $\boxed{(2 + 3u)^{-1} = \frac{22}{125} - \frac{6}{125}u - \frac{9}{250}u^2 \in \mathbb{Q}[u]}$, as required.

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 $F(\alpha) = K$.

Proof. (1) Note the equation $[K : F] = [K : F(\alpha)][F(\alpha) : F]$. Suppose $F(\alpha) \subsetneq K$ on the contrary. Then $[K : F(\alpha)] \geqslant 2$ and hence

$$\deg(p(x)) = [F(\alpha) : F] = \frac{[K : F]}{[K : F(\alpha)]} \leqslant \frac{1}{2}[K : F],$$

which is a contradiction.

(2) The equation $[K : F] = [K : F(\alpha)][F(\alpha) : F]$ implies that $[F(\alpha) : F]$ is a (positive) divisor of $[K : F]$. Now that $[K : F]$ is prime, we conclude that either $[F(\alpha) : F] = 1$ or $[F(\alpha) : F] = [K : F]$. Moreover, since $\alpha \notin F$, we see $F \subsetneq F(\alpha)$ and hence $[F(\alpha) : F] > 1$. Consequently, $[F(\alpha) : F] = [K : F]$, which implies $F(\alpha) = K$. □

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.

Proof. We first note that ω is algebraic over F as $p(\omega) = 0$ while $p(x) \neq 0$. Let $m(x)$ be the minimal polynomial of ω over F (so $m(x)$ is monic and is in $F[x]$). Now, as $p(\omega) = 0$, we see $m(x) \mid p(x)$ by a property about minimal polynomials. Thus $p(x) = m(x)n(x)$ for some $n(x) \in F[x]$. Now, since $p(x)$ is irreducible, either $m(x)$ or $n(x)$ is invertible. Moreover, $m(x)$ is not invertible because it is the minimal polynomial of ω over F. (In fact, $m(x)$ is irreducible.) Thus $n(x)$ must be invertible, hence $n(x) = c \in F$. Thus

$$p(x) = c \cdot m(x).$$

Finally, since both $p(x)$ and $m(x)$ are monic, we must have $c = 1$. Therefore $p(x) = m(x)$, meaning that $p(x)$ is the minimal polynomial of ω over F. □

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

Proof. **Here is a direct approach:** Direct computation shows

$$(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3},$$

which is clearly in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Thus

$$\sqrt{2} = \tfrac{1}{2}[(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})] \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$
$$\sqrt{3} = \tfrac{1}{2}[11(\sqrt{2} + \sqrt{3}) - (\sqrt{2} + \sqrt{3})^3] \in \mathbb{Q}(\sqrt{2} + \sqrt{3}),$$

showing $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Moreover, it is obvious that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Here is another approach: Note that $\sqrt{3} - \sqrt{2} = (\sqrt{2} + \sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Thus

$$\sqrt{2} = \tfrac{1}{2}[(\sqrt{2} + \sqrt{3}) - (\sqrt{2} + \sqrt{3})^{-1}] \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$
$$\sqrt{3} = \tfrac{1}{2}[(\sqrt{2} + \sqrt{3}) + (\sqrt{2} + \sqrt{3})^{-1}] \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

This shows $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Thus $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. □

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 $a_i \in \mathbb{Q}$.

Solution. (1) Dividing $(3x^2 - 2x + 1)(6x^2 - 5x + 4)$ by $p(x)$ via long division, we

Applying the Euclidean Algorithm to $p(x)$ and $f(x) = x^2 - 2x + 3$, we get

$$\begin{aligned} p(x) &= (x+4)f(x) + (x-6), \\ f(x) &= (x+4)(x-6) + 27, \\ x-6 &= \tfrac{1}{27}(x-6)\cdot 27 + 0. \end{aligned}$$

Thus $\gcd(p(x), f(x)) = 1$. To write 1 as a linear combination of $p(x)$ and $f(x)$, we have

$$\begin{aligned} 1 &= \tfrac{1}{27}\cdot 27 = \tfrac{1}{27}\left[f(x) - (x+4)(x-6)\right] \\ &= \tfrac{1}{27}\big[f(x) - (x+4)[p(x) - (x+4)f(x)]\big] \\ &= \tfrac{1}{27}\left[-(x+4)p(x) + (x^2+8x+17)f(x)\right] \\ &= -\tfrac{1}{27}(x+4)p(x) + (\tfrac{1}{27}x^2 + \tfrac{8}{27}x + \tfrac{17}{27})f(x). \end{aligned}$$

Thus

$$\begin{aligned} 1 &= -\tfrac{1}{27}(u+4)p(u) + (\tfrac{1}{27}u^2 + \tfrac{8}{27}u + \tfrac{17}{27})f(u) \\ &= (\tfrac{1}{27}u^2 + \tfrac{8}{27}u + \tfrac{17}{27})(3 - 2u + u^2). \end{aligned}$$

Hence, we obtain $\boxed{(3 - 2u + u^2)^{-1} = \tfrac{1}{27}u^2 + \tfrac{8}{27}u + \tfrac{17}{27}}$, as required.

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.*

Proof. Note that ω is algebraic over F as $p(\omega) = 0$ while $p(x) \neq 0$. Let $m(x)$ be the minimal polynomial of ω over F. So $m(x)$ is monic in $F[x]$ with $\deg(m(x)) = [F(\omega) : F]$. Now, as $p(\omega) = 0$, we see $m(x) \mid p(x)$ by a property of minimal polynomials. Thus $p(x) = n(x)m(x)$ for some $n(x) \in F[x]$. Now, since $\deg(p(x)) = [F(\omega) : F] = \deg(m(x))$, we see

$$\deg(n(x)) = \deg(p(x)) - \deg(m(x)) = 0.$$

This means that $n(x)$ is a non-zero constant, i.e., $n(x) = c \in F \setminus \{0\}$. Thus $p(x) = c \cdot m(x)$. Finally, since both $p(x)$ and $m(x)$ are monic, we must have $c = 1$. Therefore, we conclude $p(x) = m(x)$, proving that $p(x)$ is the minimal polynomial of ω over F. (Alternatively, the assumption on $p(x)$ implies that $p(x)$ is a minimal polynomial of ω over F. Given the uniqueness, we see that $p(x)$ is 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 $\Big[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})\Big]$ and $\Big[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}\Big]$.

Proof/Solution. (1) Clearly, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$. Also, as $\sqrt{2+\sqrt{3}} \in \mathbb{Q}(\sqrt{2+\sqrt{3}})$, we see

$$\sqrt{3} = (2+\sqrt{3}) - 2 = (\sqrt{2+\sqrt{3}})^2 - 2 \in \mathbb{Q}(\sqrt{2+\sqrt{3}}),$$

which proves $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2+\sqrt{3}})$.

(2) Suppose, on the contrary, $\sqrt{2+\sqrt{3}} \in \mathbb{Q}(\sqrt{3})$. Then $\sqrt{2+\sqrt{3}} = a + b\sqrt{3}$ for some a, $b \in \mathbb{Q}$. Hence $(a+b\sqrt{3})^2 = 2+\sqrt{3}$, which expands to

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2 + \sqrt{3},$$

which gives $a^2 + 3b^2 = 2$ and $2ab = 1$ since 1 and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$. Thus $b = (2a)^{-1}$, and then $a^2 + 3(2a)^{-2} = 2$. Clearing the denominator, we see $4a^4 + 3 = 8a^2$, or simply $4a^4 - 8a^2 + 3 = 0$. So a is a rational root of $4x^4 - 8x^2 + 3 \in \mathbb{Z}[x]$. However, the polynomial $4x^4 - 8x^2 + 3$ has no root in $\mathbb{Q}$ since none of $\pm\frac{1}{1}$, $\pm\frac{3}{1}$, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$, $\pm\frac{1}{4}$, $\pm\frac{3}{4}$ is a root. (Or, solving $4x^4 - 8x^2 + 3 = 0$ directly, we see that its roots are $\pm\sqrt{1/2}$ and $\pm\sqrt{3/2}$, none of which is rational.) So we get a contradiction. Therefore $\sqrt{2+\sqrt{3}} \notin \mathbb{Q}(\sqrt{3})$, which implies $\mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{2+\sqrt{3}})$. □

(3) Let $p(x) = x^2 - (2+\sqrt{3}) \in \mathbb{Q}(\sqrt{3})[x]$. (Here x is the indeterminate and $\mathbb{Q}(\sqrt{3})$ is the base field for coefficients.) Clearly, $p(\sqrt{2+\sqrt{3}}) = 0$. The work in (2) above shows that $p(x)$ has no root in $\mathbb{Q}(\sqrt{3})$, which implies $p(x)$ is irreducible in $\mathbb{Q}(\sqrt{3})[x]$ as $\deg(p(x)) = 2$. Thus $p(x) = x^2 - (2+\sqrt{3})$ is the the minimal polynomial of $\sqrt{2+\sqrt{3}}$ over $\mathbb{Q}(\sqrt{3})$ by Problem 2.2. Hence $\Big[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})\Big] = \deg(p(x)) = 2$ and

$$\Big[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}\Big] = \Big[\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}(\sqrt{3})\Big] \cdot \Big[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\Big] = 2 \cdot 2 = 4.$$

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**.

Solution. Denote $u = \sqrt{2+\sqrt{3}}$. Then

$$\begin{aligned} u^2 = 2+\sqrt{3} &\implies u^2 - 2 = \sqrt{3} \\ &\implies (u^2-2)^2 = (\sqrt{3})^2, \quad \text{which expands to} \quad u^4 - 4u^2 + 4 = 3 \\ &\implies u^4 - 4u^2 + 1 = 0. \end{aligned}$$

Let $p(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$, so that $p(\sqrt{2+\sqrt{3}}) = 0$. Moreover, $p(x)$ is monic with $\deg(p(x)) = 4 = [\mathbb{Q}(\sqrt{2+\sqrt{3}}) : \mathbb{Q}]$; see Problem 3.2. Thus, by Problem 3.1, we conclude that $\boxed{x^4 - 4x^2 + 1}$ is the minimal polynomial of $\sqrt{2+\sqrt{3}}$ over $\mathbb{Q}$.

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 $\mathbb{Q}$.

Proof/Solution. From $\alpha^{-1} = \frac{5}{6}\alpha^4 - \alpha^3 + 2\alpha^2 - 3\alpha + 4$, we see

$$\alpha\left(\frac{5}{6}\alpha^4 - \alpha^3 + 2\alpha^2 - 3\alpha + 4\right) = 1,$$

which simplifies to $5\alpha^5 - 6\alpha^4 + 12\alpha^3 - 18\alpha^2 + 24\alpha - 6 = 0$. Hence α is algebraic over $\mathbb{Q}$ since α is a root of $5x^5 - 6x^4 + 12x^3 - 18x^2 + 24x - 6 \in \mathbb{Q}[x] \setminus \{0\}$.

Moreover, the polynomial $5x^5 - 6x^4 + 12x^3 - 18x^2 + 24x - 6$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (with $p = 2$ or $p = 3$). Therefore, by Problem 2.2, the minimal polynomial of α over $\mathbb{Q}$ is

$$m(x) = x^5 - \tfrac{6}{5}x^4 + \tfrac{12}{5}x^3 - \tfrac{18}{5}x^2 + \tfrac{24}{5}x - \tfrac{6}{5} \in \mathbb{Q}[x].$$

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.

Solution. (1) Let $p(x)=x^3-2$, which is irreducible over $\mathbb{Q}$ satisfying $p(\sqrt[3]{2})=0$. Thus $p(x)$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ by Problem 2.2. So $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=\deg(p(x))=3$.

(2) True. Indeed, as $\sqrt[3]{2}+\sqrt[3]{4}\in\mathbb{Q}(\sqrt[3]{2})\setminus\mathbb{Q}$ and $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ (that is prime), we must have $\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{4})=\mathbb{Q}(\sqrt[3]{2})$ by Problem 2.1(2).

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

Solution. Denote $u=\sqrt[3]{2}+\sqrt[3]{4}$. By direct computation, we have

$$\begin{aligned} 1 &= 1\cdot 1 + 0\cdot\sqrt[3]{2} + 0\cdot\sqrt[3]{4} \\ u &= 0\cdot 1 + 1\cdot\sqrt[3]{2} + 1\cdot\sqrt[3]{4} \\ u^2 &= 4\cdot 1 + 2\cdot\sqrt[3]{2} + 1\cdot\sqrt[3]{4} \\ u^3 &= 6\cdot 1 + 6\cdot\sqrt[3]{2} + 6\cdot\sqrt[3]{4} \end{aligned}$$

Thus, finding $a_0,\dots,a_3$ such that $\sum_{i=0}^{3}a_iu^i=0$ is equivalent to solving the following system of linear equations

$$\begin{pmatrix} 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 6 \\ 0 & 1 & 1 & 6 \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Solving the system directly, we find a solution of

$$a_3=1,\quad a_2=0,\quad a_1=-6\quad\text{and}\quad a_0=-6,$$

which means $u^3-6u-6=0$.

Let $p(x)=x^3-6x-6\in\mathbb{Q}[x]$. Since $\deg(p(x))=3=[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2}+\sqrt[3]{4}):\mathbb{Q}]$, $p(x)$ is monic and $p(\sqrt[3]{2}+\sqrt[3]{4})=0$, we conclude that the minimal polynomial of $\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$ is $\boxed{x^3-6x-6}$ by Problem 3.1; also see Problem 2.2 as $p(x)$ is irreducible.

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.*

Proof. Let $u\in L$ be arbitrary. (It suffices to show that u is algebraic over F.)

As u is algebraic over K, there exists $p(x)\in K[x]\setminus\{0\}$ such that $p(u)=0$. (We may just as well choose $p(x)$ to be the minimal polynomial of u over K.) Say $p(x)=a_nx^n+\cdots+a_1x+a_0$ so that $a_i\in K$. Denote $K_1=F(a_0,a_1,\dots,a_n)$. As $a_i\in K$ and K is algebraic over F, all a_i are algebraic over F. Thus K_1 is a finite field extension of F, that is, $[K_1:F]<\infty$.

Now consider $K_1(u)$. Clearly, $p(x)\in K_1[x]$ and, of course, it still holds that $p(u)=0$. Thus u is algebraic over K_1 and hence $[K_1(u):K_1]<\infty$.

In summary, we see $[K_1:F]<\infty$ and $[K_1(u):K_1]<\infty$. Therefore,

$$[K_1(u):F]=[K_1(u):K_1][K_1:F]<\infty,$$

which implies that $K_1(u)$ is algebraic over F. In particular, u is algebraic over F. Thus L is algebraic over F, which completes the proof of the theorem. □

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.)

Proof. Clearly, $F \subseteq \{u \in K \mid u \text{ is algebraic over } F\}$. Conversely, let $u \in K$ be an (arbitrary) element that is algebraic over F. (It suffices to show $u \in F$.)

Let $m_F(x)$ be the minimal polynomial of u over F, and $m_K(x)$ be the minimal polynomial of u over K. Then $m_F(x)$ is monic and irreducible in $F[x]$ with $m_F(u) = 0$. By assumption, $m_F(x)$ remains irreducible in $K[x]$. (Clearly, $m_F(x)$ is still monic and satisfying $m_F(u) = 0$.) Thus $m_F(x)$ is the the minimal polynomial of u over K by Problem 2.2. Thus $m_K(x) = m_F(x) \in F[x]$.

On the other hand, since $u \in K$, the minimal polynomial of u over K is

$$m_K(x) = x - u \in K[x].$$

Now, putting it all together, we see $x - u = m_K(x) = m_F(x) \in F[x]$, which implies $u \in F$. This establishes that F is algebraically closed in K, as required. □

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.

Solutions

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.

Proof. Since K_λ is algebraic over F, for each $\lambda \in \Lambda \neq \varnothing$, we see that K is algebraic over F.

Let $p(x)$ be any irreducible polynomial in $F[x]$ such that $p(x)$ has a root in K; say $\deg(p(x)) = n$. Fix any $\lambda \in \Lambda$. Since K_λ is normal over F and $p(x)$ has a root in K_λ, $p(x)$ can be factored completely over K_λ (according to a result covered in class); say

$$p(x) = a(x - r_1)(x - r_2)\cdots(x - r_n) \qquad \text{with} \quad a \in F \setminus \{0\} \text{ and } r_i \in K_\lambda \subseteq L.$$

The roots of $p(x)$ are uniquely determined in L (up to re-ordering). Thus, the roots $r_1, r_2, \ldots, r_n \in K_\lambda$ are independent of $\lambda \in \Lambda$ (since they are *all the roots* of $p(x)$ in L). Consequently, we see $\{r_1, r_2, \ldots, r_n\} \subseteq K_\lambda$ for *all* $\lambda \in \Lambda$. This allows us to establish $\{r_1, r_2, \ldots, r_n\} \subseteq \bigcap_{\lambda\in\Lambda} K_\lambda = K$. Therefore

$$p(x) = a(x - r_1)(x - r_2)\cdots(x - r_n) \quad \text{with} \quad r_i \in K \text{ for all } i = 1, \ldots, n.$$

In summary, if a polynomial $p(x) \in F[x]$ that is irreducible over F has a root in K then $p(x)$ factors completely over K. This proves that K is a normal extension of F.

Here is another approach (sketch): Fix any algebraic closure C of L. Suppose that K is not normal over F. Then there exists an embedding $\varphi\colon K \to C$ such that $\varphi|_F = \mathrm{id}_F$ and $\varphi(K) \nsubseteq K$; so $\varphi(K) \nsubseteq K_\lambda$ for some $\lambda \in \Lambda$. Let $\psi\colon K_\lambda \to C$ be any extension of φ, which exists (details omitted). Then $\psi|_F = \mathrm{id}_F$ and $\varphi(K_\lambda) \nsubseteq K_\lambda$, which is a contradiction. (Note that C is not necessarily an algebraic closure of K_λ. But this is not an issue.) □

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 $[K : F] \leqslant n!$.

Proof. We prove the statement by induction on $\deg(f(x))$. In case $\deg(f(x)) = 1$, it is clear that $f(x)$ has precisely one root that is in F. Thus $K = F$ hence $[K : F] = 1 = 1!$.

Assume that the statement holds for $n = k-1 \geqslant 1$. (This means that the statement holds for the splitting fields of *any* polynomial of degree $k - 1$ over *any* field.) Let $f(x) \in F[x]$ with $\deg(f(x)) = k$. (We must show $[K : F] \leqslant k!$ in order to complete the induction.)

Since K is a splitting field of $f(x)$ over F, we have

$$f(x) = a(x - u_1)(x - u_2)\cdots(x - u_k) \qquad \text{with} \quad a \in F \setminus \{0\} \text{ and } u_i \in K$$

and $K = F(u_1, u_2, \ldots, u_k)$ by definition.

Denote $F_1 = F(u_1)$. Since $f(u_1) = 0$ and $\deg(f(x)) = k$, we see

$$(*) \qquad [F_1 : F] \leqslant k.$$

Also, as $f(x) \in F_1[x]$ and u_1 is a root of $f(x)$ in F_1, we have

$$f(x) = (x - u_1)f_1(x) \qquad \text{with} \quad f_1(x) = a(x - u_2)\cdots(x - u_k) \in F_1[x].$$

Hence $K = F_1(u_2, \ldots, u_k)$ is a splitting field of $f_1(x)$ over F_1. Now, as $\deg(f_1(x)) = k - 1$, the induction hypothesis (applied to $f_1(x)$ over the field F_1) implies

$$(**) \qquad [K : F_1] \leqslant (k - 1)!.$$

Combining $(*)$ and $(**)$, we see

$$[K : F] = [K : F_1][F_1 : F] \leqslant k!$$

as required. This concludes the induction. The proof is complete. □

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.

Proof. Let $u \in \mathbb{C}$ be a/any root of $x^n - a$ (which exists); and let $v = e^{\frac{2\pi}{n}i} \in \mathbb{C}$. Then, as $v^0, v^1, \ldots, v^{n-1}$ are the distinct roots of $x^n - 1 \in \mathbb{Q}[x]$, we see that $u, uv, \ldots, uv^{n-1}$ are distinct roots of $x^n - a$. As $x^n - a$ have at most n distinct roots in $\mathbb{C}$, we conclude that $u, uv, \ldots, uv^{n-1}$ must exhaust all the roots of $x^n - a$. Thus

$$K = \mathbb{Q}(u, uv, \ldots, uv^{n-1}).$$

Finally, note that $\mathbb{Q}(u, uv, \ldots, uv^{n-1}) = \mathbb{Q}(u, v)$. (Indeed, as $uv^t \in \mathbb{Q}(u, v)$ for all $t \in \mathbb{Z}$, we get $\mathbb{Q}(u, uv, \ldots, uv^{n-1}) \subseteq \mathbb{Q}(u, v)$. Conversely, as both u and $v = u^{-1}(uv)$ are in $\mathbb{Q}(u, uv, \ldots, uv^{n-1})$, we see $\mathbb{Q}(u, uv, \ldots, uv^{n-1}) \supseteq \mathbb{Q}(u, v)$.) Therefore $K = \mathbb{Q}(u, v)$ as required. (**In fact**, there exists $w \in K$ such that $K = \mathbb{Q}(w)$. Stay tuned.) □

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).*)

Solution. (1) It is true that $K = \mathbb{Q}(u, v)$, as this has been just shown in Problem 5.3.

(2) As $u^6 - 2 = 0$ while $x^6 - 2$ is monic and irreducible over $\mathbb{Q}$ (by Eisenstein's Criterion with $p = 2$), we see $x^6 - 2$ is the minimal polynomial of u over $\mathbb{Q}$ (cf. Problem 2.2). Hence

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg(x^6 - 2) = 6.$$

(3) Note that $v = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $v^{-1} = e^{-\frac{\pi}{3}i} = \frac{1}{2} - \frac{\sqrt{3}}{2}i$. (Indeed, for all $z \in \mathbb{C}$ with $|z| = 1$, $z^{-1} = \overline{z}$, the conjugate of z.) Consequently, we see

$$v + v^{-1} = 1 \qquad \text{which implies} \qquad v^2 - v + 1 = 0.$$

So the minimal polynomial of v over $\mathbb{Q}(u)$ has degree at most 2; hence

$$(\dagger) \qquad [\mathbb{Q}(u, v) : \mathbb{Q}(u)] \leqslant 2.$$

Moreover, as $v \notin \mathbb{R}$ while $\mathbb{Q}(u) \subseteq \mathbb{R}$, we see $v \notin \mathbb{Q}(u)$; hence

$$(\ddagger) \qquad [\mathbb{Q}(u, v) : \mathbb{Q}(u)] \geqslant 2.$$

Combining (†) and (‡), we see $[\mathbb{Q}(u, v) : \mathbb{Q}(u)] = 2$.

(4) Putting (1), (2) and (3) together, we see

$$[K : \mathbb{Q}] = [\mathbb{Q}(u, v) : \mathbb{Q}] = [\mathbb{Q}(u, v) : \mathbb{Q}(u)][\mathbb{Q}(u) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

In summary, $[K : \mathbb{Q}] = 12$. The solution is now complete.

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 $g(x) \in F[x]$.

Proof. (1) $\Rightarrow$ (2): This is clear.

(2) $\Rightarrow$ (3): Suppose that $f(x)$ has a multiple root in an extension field of F. Then

$$f'(x) = 0, \quad \text{that is,} \quad da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + 2a_2 x + a_1 = 0.$$

Thus $ia_i = 0$, which implies $p \mid i$ or $a_i = 0$, for $1 \leqslant i \leqslant d$. Note that $p \mid 0$. Hence $a_i = 0$ for all $0 \leqslant i \leqslant d$ such that $p \nmid i$.

(3) $\Rightarrow$ (4): Assume $a_i = 0$ for all $0 \leqslant i \leqslant d$ with $p \nmid i$. Then $f(x)$ can be written as

$$f(x) = a_0 + a_p x^p + a_{2p}x^{2p} + \cdots + a_{(s-1)p}x^{(s-1)p} + a_{sp}x^{sp} \quad \text{for some } s \in \mathbb{Z} \text{ with } s \geqslant 1.$$

Let $g(x) = a_0 + a_p x + a_{2p}x^2 + \cdots + a_{(s-1)p}x^{s-1} + a_{sp}x^s \in F[x]$. It is clear that $f(x) = g(x^p)$.

(4) $\Rightarrow$ (1): Suppose $f(x) = g(x^p)$ with $g(x) = c_s x^s + \cdots + c_1 x + c_0 \in F[x]$. Thus

$$f(x) = g(x^p) = c_s x^{sp} + c_{s-1}x^{(s-1)p} + \cdots + c_2 x^{2p} + c_1 x^p + c_0.$$

It is routine (and easy) to see $f'(x) = 0$ as $\mathrm{char}(F) = p$. (Or by chain rule, $f'(x) = g'(x^p)(x^p)' = g'(x^p)(px^{p-1}) = 0$.) Now, for every root r of $f(x)$ in any field extension of F,

$$f(r) = 0 = f'(r).$$

Consequently all roots of $f(x)$, in *all extension fields* of F, are multiple. □

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.

Proof. As K is a splitting field of $f(x)$ over F, there exists (at least) one root of $f(x)$ in K; that is, there exists $u \in K$ such that $f(u) = 0$, which gives

$$u^{p^n} = a.$$

Now, due to prime characteristic p, we have

$$f(x) = x^{p^n} - a = x^{p^n} - u^{p^n} = (x-u)^{p^n}.$$

This shows that u is the only root of $x^{p^n} - a$ in K, with multiplicity p^n. □

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 $f'(r) \neq 0$.)

Proof. (1) $\Rightarrow$ (2): Assume that r is a root of $f(x)$ of multiplicity m. By definition,

$$f(x) = (x-r)^m g(x) \quad \text{with} \quad g(r) \neq 0.$$

Thus, we have $f(r) = (r-r)^m g(r) = 0$. Moreover, we see

$$\begin{aligned} f'(x) &= [(x-r)^m g(x)]' \\ &= m(x-r)^{m-1} g(x) + (x-r)^m g'(x) \\ &= (x-r)^{m-1}[mg(x) + (x-r)g'(x)], \end{aligned}$$

with $mg(r) + (r-r)g'(r) = mg(r) \neq 0$, since $m \neq 0_{\mathbb{Z}}$, $g(r) \neq 0_F$ and $\mathrm{char}(F) = 0$. This proves that r is a root of $f'(x)$ of multiplicity $m-1$.

(2) $\Rightarrow$ (1): Assume that $f(r) = 0$ and r is a root of $f'(x)$ of multiplicity $m-1$. Since $f(r) = 0$, we see that r is a root of $f(x)$, say of multiplicity $s \geqslant 1$. By (1) $\Rightarrow$ (2) above (which has been established), we see that r is a root of $f'(x)$ of multiplicity $s-1$. Note that the multiplicity of r as a root of $f'(x)$ is uniquely determined (as $F[x]$ is a UFD). Thus $s-1 = m-1$, which yields $s = m$, meaning that r is a root of $f(x)$ with multiplicity m. This completes the proof. $\square$

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 $f^{(1)} = f'(x)$.)

Proof. We proceed by induction on m. The case where $m = 1$ has been proved in class (and is also proved in Problem 6.3 above).

Let $k \geqslant 1$ be an integer and suppose that the equivalence (1) $\Leftrightarrow$ (2) holds for $m = k$. (Stated explicitly, the induction hypothesis says that, for *every* polynomial $g(x) \in F[x] \setminus F$, r is a root of $g(x)$ of multiplicity k if and only if $g^{(i)}(r) = 0$ for all $i = 0, \ldots, k-1$ and $g^{(k)}(r) \neq 0$. This is labeled $(*)$.) Now we have

$$\begin{aligned} &r \text{ is a root of } f(x) \text{ of multiplicity } k+1 \\ &\overset{6.3}{\Longleftrightarrow} \ f(r) = 0 \text{ and } r \text{ is a root of } f'(x) \text{ of multiplicity } k \\ &\overset{(*)}{\Longleftrightarrow} \ f^{(i)}(r) = 0 \text{ for all } i = 0, 1, \ldots, k \text{ and } f^{(k+1)}(r) \neq 0. \end{aligned}$$

So the desired equivalence holds for $m = k+1$. By induction, the desired equivalence (1) $\Leftrightarrow$ (2) holds for all $m \in \mathbb{N}$. The proof is now complete. $\square$

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 $F[x]$.

Proof. Write $x^p - a = p_1(x) \cdots p_n(x)$ with each $p_i(x)$ monic and irreducible in $F[x]$. Also, let C be an algebraic closure of F, so that $x^p - a$ has a root $r \in C$. Consequently,

$$(\dagger) \qquad p_1(x) \cdots p_n(x) = x^p - a = x^p - r^p = (x - r)^p \in C[x].$$

In particular, r is a root of $p_i(x)$ for all $i = 1 \ldots, n$. (In fact, it follows from (†) that each $p_i(x)$ is a power of $x - r$, since $C[x]$ is a UFD.)

By Problem 2.2, each $p_i(x)$ is the (unique) minimial polynomial of r over F. Thus, by the uniqueness of minimal polynomial, we see $p_1(x) = \cdots = p_n(x)$. Consequently,

$$x^p - a = p_1(x) \cdots p_n(x) = m(x) \cdots m(x) = m(x)^n$$

in which $m(x)$ denotes the minimial polynomial of r over F. Thus $p = n \deg(m(x))$.

As p is prime, we get $\deg(m(x)) \in \{1, p\}$. If $\deg(m(x)) = 1$, then $x^p - a$ factors completely in $F[x]$; If $\deg(m(x)) = p$, then $x^p - a = m(x)$, which is irreducible in $F[x]$. □

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.

Solution/Proof. (1) True. Indeed, the inclusion $E \subseteq K$ is clear by the construction of E. For $F \subseteq E$, observe that every $a \in F$ satisfies $a^{p^0} \in F$, which yields $a \in E$.

(2) True. To prove it, let us first note that $E \neq \varnothing$ because $\varnothing \neq F \subseteq E$. (This also shows $1_K = 1_F \in E$.) Next, let $a, b \in E$. There exist non-negative integers m, n such that

$$a^{p^m} \in F \quad \text{and} \quad b^{p^n} \in F.$$

Let $t = \max\{m, n\}$ (or choose any $t \geqslant \max\{m, n\}$). By the Frobenius, we see

$$\begin{aligned} (a - b)^{p^t} &= a^{p^t} - b^{p^t} = (a^{p^m})^{p^{t-m}} - (b^{p^n})^{p^{t-n}} \in F, \\ (ab)^{p^t} &= a^{p^t} b^{p^t} = (a^{p^m})^{p^{t-m}} (b^{p^n})^{p^{t-n}} \in F, \\ (a^{-1})^{p^m} &= (a^{p^m})^{-1} \in F \quad \text{if} \quad a \neq 0, \end{aligned}$$

which implies $a - b \in E$, $ab \in E$, and $a^{-1} \in E$ if $a \neq 0$. Given $E \subseteq K$, this shows that E is a subfield of K. □

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

(1) All algebraic field extensions of F are separable over F.
(2) $F = \{u^p \mid u \in F\}$.

Proof. Suppose $F \neq \{u^p \mid u \in F\}$. This necessarily means $\{u^p \mid u \in F\} \subsetneq F$, so there exists $a \in F$ such that $a \notin \{u^p \mid u \in F\}$. Consider the following polynomial

$$p(x) = x^p - a \in F[x].$$

By the assumption above, $p(x)$ has no roots in F and, hence, $p(x)$ does not factor completely over F. By Problem 7.1, we conclude that $p(x)$ is irreducible over F. Let K be a splitting

field of $p(x) = x^p - a$ over F, so that there exists $r \in K$ such that r is a root of $p(x)$, which simply means $r^p = a$. Thus, in $K[x]$, we have

$$p(x) = x^p - a = x^p - r^p = (x - r)^p.$$

Moreover, $p(x)$ is the minimal polynomial of r over F; see Problem 2.2. Therefore, the element r is not separable over F, because r is a multiple root of its minimal polynomial over F (namely $p(x)$). Altogether, we get an algebraic field extension $F \subseteq K$ such that K is not separable over F. This completes the proof. □

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.

Solution/Proof. (1) True. The field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is separable since $\mathrm{char}(\mathbb{Q}) = 0$. Also, $\mathbb{Q}(\sqrt{2})$ is normal over $\mathbb{Q}$ since $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$ is a splitting field of $x^2 - 2$ over $\mathbb{Q}$. Therefore $\mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$.

(2) True. The field extension $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ is separable since $\mathrm{char}(\mathbb{Q}(\sqrt{2})) = 0$. Also, as $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2})$ is a splitting field of $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$, we see that $\mathbb{Q}(\sqrt[4]{2})$ is normal over $\mathbb{Q}(\sqrt{2})$. In conclusion, $\mathbb{Q}(\sqrt[4]{2})$ is Galois over $\mathbb{Q}(\sqrt{2})$.

(3) False. Indeed, consider $x^4 - 2$, which is irreducible in $\mathbb{Q}[x]$ (by Eisenstein's criterion). Clearly, $x^4 - 2$ has roots $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$. But $\mathbb{Q}(\sqrt[4]{2})$ does not contain the other roots $\pm\sqrt[4]{2}\, i$ of $x^4 - 2$, since $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$. Thus $\mathbb{Q}(\sqrt[4]{2})$ is not normal, hence not Galois, over $\mathbb{Q}$. □

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 $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ 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 $\mathrm{Gal}(E/K)$.
(4) Prove $\mathbb{Q}(5\sqrt{2} + 8\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. (Compare with Problem 2.3.)

Solution/Proof. (1) It is straightforward to see

$$\sigma_2(1 - 2\sqrt{2} + 3\sqrt{3} - 4\sqrt{6}) = 1 - 2\sqrt{2} - 3\sqrt{3} + 4\sqrt{6}.$$

(2) By inspection (details skipped), we see $E_H = \{a + b\sqrt{6} \,|\, a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$.

(3) By definition (and also because $5\sqrt{2} + 8\sqrt{3}$ generates K over $\mathbb{Q}$), $\sigma_i \in \mathrm{Gal}(E/K)$ if and only if $\sigma_i(5\sqrt{2} + 8\sqrt{3}) = 5\sqrt{2} + 8\sqrt{3}$. Direct checking reveals (details skipped)

$$\sigma_1(5\sqrt{2} + 8\sqrt{3}) = 5\sqrt{2} + 8\sqrt{3} \quad \text{while} \quad \sigma_i(5\sqrt{2} + 8\sqrt{3}) \neq 5\sqrt{2} + 8\sqrt{3} \text{ for all } i = 2, 3, 4.$$

That is, **only** σ_1 keeps $5\sqrt{2} + 8\sqrt{3}$ fixed. Thus $\mathrm{Gal}(E/K) = \{\sigma_1\}$.

(4) By the fundamental theorem of Galois theory, $K = E_{\mathrm{Gal}(E/K)}$. Since $\mathrm{Gal}(E/K) = \{\sigma_1\}$, we must have $K = E_{\{\sigma_1\}}$, the fixed field of $\{\sigma_1\}$. On the other hand, direct calculation reveals that $E_{\{\sigma_1\}} = E$. (Indeed, σ_1 is the identity map on E, so *every* element of E is fixed by σ_1.) Thus $K = E$, which verifies $\mathbb{Q}(5\sqrt{2} + 8\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. □

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

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

Solution. (1) The Galois group $\mathrm{Gal}(E/\mathbb{Q})$ has order 4. And direct computing shows

$$\sigma_i^2(\sqrt{2}) = \sqrt{2} \quad \text{and} \quad \sigma_i^2(\sqrt{3}) = \sqrt{3} \qquad \text{for all} \qquad i = 1, 2, 3, 4.$$

That is, $\sigma_i^2 = \sigma_1$ for all i. Thus $\mathrm{Gal}(E/\mathbb{Q})$ is the Klein four-group (cf. Problem 8.4).

(2) There are *precisely* five subgroups of $\mathrm{Gal}(E/\mathbb{Q})$, which are listed as follows

$$H_1 = \{\sigma_1\}, \quad H_2 = \{\sigma_1, \sigma_2\}, \quad H_3 = \{\sigma_1, \sigma_3\}, \quad H_4 = \{\sigma_1, \sigma_4\}, \quad H_5 = \mathrm{Gal}(E/\mathbb{Q}).$$

(3) By the fundamental theorem of Galois theory, the intermediate fields must be the fixed fields E_{H_i}, $1 \leqslant i \leqslant 5$, *precisely*. Studying each E_{H_i} directly (details skipped), we see

$$E_{H_1} = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad E_{H_2} = \mathbb{Q}(\sqrt{2}), \quad E_{H_3} = \mathbb{Q}(\sqrt{3}), \quad E_{H_4} = \mathbb{Q}(\sqrt{6}), \quad E_{H_5} = \mathbb{Q}.$$

So there are *precisely* five intermediate fields: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Problem 8.3. Consider the Galois group of $x^4 - 2$ over $\mathbb{Q}$, $\mathrm{Gal}(E/\mathbb{Q})$ where $E = \mathbb{Q}(\sqrt[4]{2}, i)$. It can be shown that $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_8\}$ 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 $\mathrm{Gal}(E/K)$.
(3) Prove $\mathbb{Q}(\sqrt[4]{2} + i) = \mathbb{Q}(\sqrt[4]{2}, i)$. (Compare with Problem 2.3 and Problem 8.1.)

Solution/Proof. (1) For $w = c_1 + c_2\, i + c_3\sqrt[4]{2} + c_4\sqrt[4]{2}\, i + c_5\sqrt{2} + c_6\sqrt{2}\, i + c_7\sqrt[4]{8} + c_8\sqrt[4]{8}\, i \in \mathbb{Q}(\sqrt[4]{2}, i)$ with $c_j \in \mathbb{Q}$, we have (with some details skipped in $\overset{*}{\iff}$)

$$\begin{aligned} w \in E_H &\iff \sigma_1(w) = w \text{ and } \sigma_8(w) = w \iff \sigma_8(w) = w \\ &\overset{*}{\iff} c_2 = c_5 = 0, c_3 = -c_4 \text{ and } c_7 = c_8 \\ &\iff c_1 + c_3(\sqrt[4]{2} - \sqrt[4]{2}\, i) + c_4\sqrt{2}\, i + c_7(\sqrt[4]{8} + \sqrt[4]{8}\, i). \end{aligned}$$

Consequently, we obtain $E_H = \{a + b(\sqrt[4]{2} - \sqrt[4]{2}\, i) + c\sqrt{2}\, i + d(\sqrt[4]{8} + \sqrt[4]{8}\, i) \mid a, b, c, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt[4]{2} - \sqrt[4]{2}\, i)$, noting that $-\frac{1}{2}(\sqrt[4]{2} - \sqrt[4]{2}\, i)^2 = \sqrt{2}\, i$ and $-\frac{1}{2}(\sqrt[4]{2} - \sqrt[4]{2}\, i)^3 = \sqrt[4]{8} + \sqrt[4]{8}\, i$.

(2) By definition (and because $\sqrt[4]{2} + i$ generates K over $\mathbb{Q}$), we have $\sigma_j \in \mathrm{Gal}(E/K)$ if and only if $\sigma_j(\sqrt[4]{2} + i) = \sqrt[4]{2} + i$. Direct checking reveals (details skipped) that

$$\sigma_1(\sqrt[4]{2} + i) = \sqrt[4]{2} + i \quad \text{while} \quad \sigma_j(\sqrt[4]{2} + i) \neq \sqrt[4]{2} + i \text{ for all } j = 2, 3, \ldots, 8.$$

That is, **only** σ_1 keeps $\sqrt[4]{2} + i$ fixed. Thus $\mathrm{Gal}(E/K) = \{\sigma_1\}$.

(3) By the fundamental theorem of Galois theory, $K = E_{\mathrm{Gal}(E/K)} = E_{\{\sigma_1\}}$. Moreover, from direct inspection, we see that the fixed field of $\{\sigma_1\}$ is $E_{\{\sigma_1\}} = E$, since σ_1 is the identity map on E. Thus $K = E$, which completes the proof that $\mathbb{Q}(\sqrt[4]{2} + i) = \mathbb{Q}(\sqrt[4]{2}, i)$. □

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 $V = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ 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	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

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

Proof/Solution. (1) Indeed, $xy = xey = x(xy)^2y = x^2yxy^2 = eyxe = yx$ for all $x, y \in H$. □

(2) See the completed multiplication table (a.k.a. the *Cayley table*) of G above. (Note that G is abelian by (1).)

(3) It is **true** that $G \cong V$. For example, there is an isomorphism $h\colon G \to V$ defined by

$$h(e) = \sigma_1, \qquad h(a) = \sigma_2, \qquad h(b) = \sigma_3, \qquad h(c) = \sigma_4.$$

(It is routine to verify that $h(xy) = h(x)h(y)$ for all $x, y \in G$.)

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 $\mathrm{char}(F) = p > 0$, 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 $\mathrm{Aut}(E/F)$.
- For $H \subseteq \mathrm{Aut}(E/F)$, the fixed field of H is $E_H = \{u \in E \mid h(u) = u \text{ for all } h \in H\}$.
- $|\mathrm{Aut}(E/F)| \leqslant [E : F]$. For $H \leqslant \mathrm{Aut}(E/F)$, $H = \mathrm{Aut}(E/E_H)$ 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 $|\mathrm{Aut}(E/F)| = [E : F]$ iff $F = E_{\mathrm{Aut}(E/F)}$. When $F \subseteq E$ is Galois, we denote $\mathrm{Aut}(E/F) = \mathrm{Gal}(E/F)$, 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 $H \leqslant \mathrm{Gal}(E/F)$, we have

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

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.

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.)

$F \subseteq K \subseteq E \ldots\ldots m_{\alpha,\,F}(x) \ldots\ldots E_H = K \iff \mathrm{Gal}(E/K) = H \ldots\ldots \mathbb{C} = \overline{\mathbb{C}} \ldots\ldots [G : N(P)] = |C(P)| = n_p \equiv 1 \mod p$