Problem Set 9

Due Thursday, April 2

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Let F be a field. Recall that

$$a1_F = \underbrace{1 + \cdots + 1}_{a \text{ times}}.$$

The **prime field** of F is the subfield of F generated by 1_F, that is

$$K = \mathrm{Frac}\left(\{\mathrm{k1_F} \mid \mathrm{k} \in \mathbb{Z}\}\right).$$

Show that the prime field of F is isomorphic to exactly one of the fields $\mathbb{Q}$ or $\mathbb{Z}/p$ for some prime integer p.

Proof. Consider the map

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\psi} & F \\ a & \longmapsto & a1_F \end{array}.$$

This map is a ring homomorphism:

- $\psi(1) = 1_F$ by definition;
- $\phi(a+b) = (a+b)1_F = a1_F + b1_F = \psi(a) + \psi(b)$;
- $\phi(a+b) = (a+b)1_F = a1_F + b1_F = \psi(a) + \psi(b)$

Moreover, the image of ψ is the prime subring of R, which is

$$\{k1_F \mid k \in \mathbb{Z}\}.$$

Thus the prime subring of F is the fraction field of $\mathrm{im}(\psi)$.

Suppose that ψ has a nontrivial kernel. Since $\mathbb{Z}$ is a PID, there exists a positive integer n such that $\ker(\psi) = (n)$. We claim that such n must in fact be prime. If n is not prime, then we can find positive integers $a > 1$ and $b > 1$ such that $n = ab$. Then

$$0 = \psi(n) = \psi(ab) = \psi(a)\psi(b) = (a1_F) \cdot (b1_F).$$

Since F is a field, we must have $a1_F = 0$ or $b1_F = 0$. But this implies either $a \in \ker(\psi) = (n)$ or $b \in \ker(\psi)$, while $a, b < n$, which is a contradiction. Therefore, n must be prime, and we will write $p = n$.

By the First Isomorphism Theorem, the prime ring of F is isomorphic to $\mathbb{Z}/\ker(\psi) = \mathbb{Z}/(p)$. Thus the prime field of F is isomorphic to the fraction field of $\mathbb{Z}/p$, but since $\mathbb{Z}/p$ is a field, its fraction field is itself. Thus the prime field of F is $\mathbb{Z}/(p)$.

On the other hand, if ψ is injective, then again by the First Isomorphism Theorem the prime ring of F is isomorphic to $\mathbb{Z}$, so the prime field of F is isomorphic to $\text{frac}(\mathbb{Z}) \cong \mathbb{Q}$. □

Problem 2. In each part, determine, with justification, the degree of the given field extension.

a) $[\mathbb{Q}(2+\sqrt{3}) : \mathbb{Q}]$.

b) $[\mathbb{Q}(1+\sqrt[3]{2}+\sqrt[3]{4}) : \mathbb{Q}]$.

Proof. a) We claim that for $\alpha = 2+\sqrt{3}$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

First, we claim that $x^2 - 3 \in \mathbb{Q}[x]$ is irreducible. By Gauss' Lemma, it is sufficient to check that it is irreducible over $\mathbb{Z}$, since $\mathbb{Q} = \text{frac}(\mathbb{Z})$. Now we can use Eisenstein's criterion with the prime ideal (2), which applies since all the coefficients of degree up to 1 are in (3), the constant coefficient is not in $(3)^2$, and the degree 2 coefficient is not in (3). We conclude that $x^2 - 3$ is irreducible over $\mathbb{Z}$, and thus over $\mathbb{Q}$ as well.

Since $\alpha \in \mathbb{R}$ we may consider the subfield $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Similarly we may also consider $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$. Since $\mathbb{Q}(\sqrt{3})$ contains $\mathbb{Q}$ and $\sqrt{3}$ it follows by definition of $\mathbb{Q}(\alpha)$ that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{3})$. Since $\sqrt{3}$ is a root of the polynomial $x^2 - 3 \in \mathbb{Q}[x]$ and this polynomial is irreducible, it follows that $m_{\sqrt{3},\mathbb{Q}} = x^2 - 3$ and consequently $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.

By the degree formula, $2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$, which implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{1, 2\}$. But $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$ if and only if $\mathbb{Q}(\alpha) = \mathbb{Q}$, which is false as $\alpha \notin \mathbb{Q}$. So it must be the case that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

b) For $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$, we claim that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

First, we claim that $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible. By Gauss' Lemma, it is sufficient to check that it is irreducible over $\mathbb{Z}$, since $\mathbb{Q} = \text{frac}(\mathbb{Z})$. Now we can use Eisenstein's criterion with the prime ideal (2), which applies since all the coefficients of degree up to 2 are in (2), the constant coefficient is not in $(2)^2$, and the degree 3 coefficient is not in (2). We conclude that $x^3 - 2$ is irreducible over $\mathbb{Z}$, and thus over $\mathbb{Q}$ as well.

Since $\beta \in \mathbb{R}$, we may consider the subfield $\mathbb{Q}(\beta) \subseteq \mathbb{R}$. Similarly we may also consider $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Since $\mathbb{Q}(\sqrt[3]{2})$ contains $\mathbb{Q}$ and the elements $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2 = \sqrt[3]{4}$, it follows by definition of $\mathbb{Q}(\beta)$ that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt[3]{2})$. Since $\sqrt[3]{2}$ is a root of the polynomial $x^3 - 2 \in \mathbb{Q}[x]$ and this polynomial is irreducible, it follows that $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ and consequently $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

By the degree formula,

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}],$$

which implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \{1, 3\}$. But $[\mathbb{Q}(\beta) : \mathbb{Q}] = 1$ if and only if $\mathbb{Q}(\beta) = \mathbb{Q}$, but we will show that $\beta \notin \mathbb{Q}$. Suppose, by contradiction, that $\beta \in \mathbb{Q}$, so that $q(x) = x^2 + x + (1 - \beta) \in \mathbb{Q}[x]$. Note that $\sqrt[3]{2}$ is a root of q, but we have shown that the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ has degree 2, so this is a contradiction. We conclude that $[\mathbb{Q}(\beta) : \mathbb{Q}] \neq 1$, and thus $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.
□

Problem 3. Consider the two field extensions $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{3})$ and $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt[3]{2})$.

a) Show that $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{3})$ has degree 4.

Proof. We have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(i, \sqrt{3})$. The degree of $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})$ is 2 since the minimal polynomial of $\sqrt{3}$ is $x^2 - 3$. The degree of $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(i, \sqrt{3})$ is at most two since i is a root of $x^2 + 1$. On the other hand, this is a proper extension, since $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ and $i \notin \mathbb{R}$. Thus $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(i, \sqrt{3})$ has degree exactly 2. By the degree formula, we conclude that

$$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4. \quad \square$$

b) Show that $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt[3]{2})$ has degree 6.

Proof. We have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(i, \sqrt[3]{2})$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ (which we justified in Problem 4). As before, $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(i, \sqrt[3]{2})$ is a proper extension of degree at most 2 and hence has degree exactly 2. By the degree formula,

$$[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 3 = 6. \quad \square$$

c) Find a primitive element γ for the extension $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{3})$.

Proof. Let $\gamma = \sqrt{3} + i$. Since $\gamma \in \mathbb{Q}(i, \sqrt{3})$, we have $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(i, \sqrt{3})$. Note that

$$\begin{aligned} \gamma^2 &= 2 + 2\sqrt{3}i \\ \gamma^3 &= 8i \\ \gamma^4 &= -8 + 8\sqrt{3}i. \end{aligned}$$

Thus $i = \frac{1}{8}\gamma^3 \in \mathbb{Q}(\gamma)$ and $\sqrt{3} = \gamma - \frac{1}{8}\gamma^3 \in \mathbb{Q}(\gamma)$. We conclude that $\mathbb{Q}(\gamma) = \mathbb{Q}(i, \sqrt{3})$ and thus γ is a primitive element. $\square$

d) Find $m_{\gamma,\mathbb{Q}}(x)$.

Proof. Note that

$$\gamma^4 - 4\gamma^2 + 16 = -8 + 8\sqrt{3}i - 4(2 + 2\sqrt{3}i) + 16 = 0.$$

Since $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}] = 4$, we know the minimal polynomial of γ over $\mathbb{Q}$ must have degree 4. Therefore, $m_{\alpha,\mathbb{Q}} = x^4 - 4x^2 + 16$. $\square$

Problem 4. Let $K \subseteq L$ be a finite extension of fields and assume $f(x)$ is a polynomial with coefficients in K that is irreducible in the ring $K[x]$.

a) Prove $f(x)$ remains irreducible when regarded as an element of the ring $L[x]$ provided $[L : K]$ is relatively prime to the degree of $f(x)$.

Proof. Let $\overline{F}$ be an algebraic closure of F and let $L = K(\alpha)$ where α is a root of $f(x)$ in L. Then $[L : F] = [L : K][K : F] = [L : K] \cdot n = e \cdot n$, where e is the degree of $m_{\alpha,K}(x)$. We also have $[L : F] = [L : F(\alpha)][F(\alpha) : F] = [L : F(\alpha)] \cdot d$. Since $\gcd(d, n) = 1$, it follows that $d \mid e$. But since α is a root of $f(x)$, $m_{\alpha,K}$ must divide $f(x)$ in $K[x]$. Since they have the same degree, it must be that $m_{\alpha,K}(x) = cf(x)$ for some nonzero constant c. Since $m_{\alpha,K}(x)$ is irreducible in $K[x]$, then $f(x)$ is irreducible in $K[x]$. $\square$

b) Give an explicit example with justification showing that the statement in part a) would become false if we omitted the assumption that $[L : K]$ is relatively prime to the degree of $f(x)$.

Proof. Take $F = \mathbb{R}$, $K = \mathbb{C}$ and $f(x) = x^2 + 1$. The polynomial f is irreducible over $\mathbb{R}$, since it has no roots over $\mathbb{R}$ and it has degree 2, while f factors as $f = (x + i)(x - i)$ over $\mathbb{C}$. On the other hand, $[\mathbb{C} : \mathbb{R}] = 2 < \infty$. □

Problem 5. Let p be a prime integer and let $F = \mathbb{Q}(i)$. Use the theory of field extensions to show that the polynomial $x^3 - p$ is irreducible in $F[x]$.

Proof. Let $q(x) = x^3 - p \in \mathbb{Q}[x] \subseteq F[x]$. Note that q is also a polynomial in $\mathbb{Z}[x]$. Since p is a prime integer, Eisenstein's Criterion applies to q with the prime ideal (p): p divides all the coefficients of q of degree up to 2, p does not divide the coefficient of degree 3, and $p^2 \nmid -p$. Therefore, q is irreducible over $\mathbb{Z}$, and thus by Gauss' Criterion we conclude that q is irreducible over $\mathbb{Q}$.

On the other hand, $i \notin \mathbb{Q}$, since i is not even a real number. Thus the polynomial $x^2 + 1$, which has degree 2 and roots i and $-i$ over $\mathbb{C}$, must be irreducible over $\mathbb{Q}$. We conclude that $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$, so $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Since $(2, 3) = 1$, by Problem 4 we conclude that q is irreducible over $\mathbb{Q}(i)$. □