Problem Set 9 solutions

Problem 1. Let F be a field. Recall that

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

The **prime ring** of F is the subring of F generated by 1_F, that is

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

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

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

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 $\mathrm{frac}(\mathbb{Z}) \cong \mathbb{Q}$. $\square$

Problem 2. In this problem, we will show that adjoining a finite set of elements to a field F is the same as adjoining its elements one at a time. More precisely, let L/F be a field extension, and let $a_1, \ldots, a_m \in L$. Set $L_0 = F$ and for each $1 \leqslant i \leqslant m$ define $L_i = L_{i-1}(a_i)$. Show that $F(a_1, \ldots, a_m) = L_m$.

Proof. We prove by induction that $L_i = F(a_1, \ldots, a_i)$ for all $1 \leqslant i \leqslant m$, with the case $i = m$ yielding the desired statement.

Base case: $i = 1$ follows by definition of L_1.

Inductive step: Assume $L_i = F(a_1, \ldots, a_i)$ for some $i < m$.

Then, by definition, we have $L_{i+1} = L_i(a_{i+1}) = F(a_1, \ldots, a_i)(a_{i+1})$. This implies in particular that L_{i+1} is a subfield of L and it contains F and $a_1, \ldots, a_i, a_{i+1}$. By definition of $F(a_1, \ldots, a_i, a_{i+1})$, $F(a_1, \ldots, a_i, a_{i+1})$ is contained in any subfield of L containing both F and $a_1, \ldots, a_{i+1}$, so it follows that $F(a_1, \ldots, a_i, a_{i+1}) \subseteq L_{i+1}$.

To establish the converse note that the respective definitions imply that there is a subfield containment $F(a_1, \ldots, a_i) \subseteq F(a_1, \ldots, a_i, a_{i+1})$ and also $a_{i+1} \in F(a_1, \ldots, a_i, a_{i+1})$. Therefore, since by definition any field containing $F(a_1, \ldots, a_i)$ and a_{i+1} must contain $F(a_1, \ldots, a_i)(a_{i+1})$, it follows that $L_{i+1} = F(a_1, \ldots, a_i, a_{i+1})(a_{i+1}) \subseteq F(a_1, \ldots, a_i, a_{i+1})$.

The two containments above combine to show the desired conclusion:

$$L_{i+1} = F(a_1, \ldots, a_i, a_{i+1}). \quad \square$$

Problem 3. Show that $x^3 + 3x + 2 \in \mathbb{Q}[x]$ is irreducible.

Proof. By Gauss' Lemma, it is sufficient to show that $f(x) = x^3 + 3x + 2$ is irreducible over $\mathbb{Z}$. If it were reducible, then it would be reducible over $\mathbb{Z}/(5)$. However, we claim that this polynomial has no roots modulo 5. Indeed, over $\mathbb{Z}/(5)$ we have the following:

$$\begin{aligned}
f(0) &= 2 \\
f(1) &= 1^3 + 3 + 2 = 1 \\
f(2) &= 2^3 + 6 + 2 = 16 = 1 \\
f(3) &= 3^3 + 9 + 2 = 2 + 4 + 2 = 3 \\
f(4) &= (-1)^3 - 3 + 2 = -2 = 3.
\end{aligned}$$

Since f is a polynomial of degree 3, if it factors, it would have a factor of degree 1. But since f has no roots, it must be irreducible. Since f is irreducible modulo 5, it is also irreducible over $\mathbb{Z}$, and thus over $\mathbb{Q}$. $\square$

Problem 4. In each part, determine, with justification, the degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$:

a) $\alpha = 2 + \sqrt{3}$

b) $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.

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 $\mathbb{Q} = \mathrm{frac}(\mathbb{Z})$. 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 $\mathbb{Q} = \mathrm{frac}(\mathbb{Z})$. 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 5. 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. □

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, $m_{\alpha,\mathbb{Q}} = x^4 - 4x^2 + 16$. □

Problem 6. Let R be a domain and let F be its fraction field. Show that F has the following universal property: if K is any field and $f : R \to K$ is any injective ring homomorphism, then f extends to an injective ring homomorphism $\overline{f}\colon F \to K$, so that $\overline{f}|_R = f$.

Proof. Define $\overline{f}\colon F \to K$ by

$$\overline{f}\left(\frac{a}{b}\right) = f(a)f(b)^{-1}.$$

First, we claim that this map is well-defined. There are really two things to check: first, that $f(b)^{-1}$ makes sense for any element $\frac{a}{b} \in F$, and second that this doesn't depend on the choice of representatives for the class of $\frac{a}{b}$.

Given any element of F, say $\frac{a}{b}$, by definition the elements $a, b \in R$ are such that $b \neq 0$. Since f is injective, $f(b) \neq 0$, and since K is a field, we conclude that $f(b)$ has an inverse. Thus $f(a)f(b)^{-1}$ makes sense.

Moreover, if $\frac{a}{b} = \frac{c}{d}$ are nonzero, then $ad = bc$, and since f is a ring homomorphism we conclude that

$$f(a)f(d) = f(ad) = f(bc) = f(b)f(c).$$

Now since $b, d \neq 0$ by definition of F, and since f is injective, we must have $f(b), f(d) \neq 0$, and since K is a field, both have inverses. Multiplying the identity above by $f(b)^{-1}f(d)^{-1}$, we get

$$f(a)f(b)^{-1} = f(b)f(d)^{-1}.$$

Thiss shows that $\overline{f}$ is well-defined.

Moreover, $\overline{f}$ is a ring homomorphism:

- $\overline{f}(1_F) = \overline{f}(\frac{1}{1}) = f(1)f(1)^{-}1 = 1_K \cdot 1_K^{-1} = 1_K$. Since f is a ring homomorphism, $f(1_R) = 1_K$.
- Using that f is preserves sums, we see that

$$\overline{f}(\frac{a}{b} + \frac{c}{d}) = \overline{f}(\frac{ad+bc}{bd}) = f(ad+bc)f(bd)^{-1} = (f(a)f(d) + f(b)f(c))f(b)^{-1}f(d)^{-1}$$

$$= (f(a)f(b)^{-1}) + (f(c)f(d)^{-1}) = \overline{f}(\frac{a}{b}) + \overline{f}\left(\frac{c}{d}\right).$$

- Using that f is preserves multiplication, we see that

$$\overline{f}\left(\frac{a}{b}\frac{c}{d}\right) = \overline{f}\left(\frac{ac}{bd}\right) = f(ac)f(bd)^{-1}$$

$$= f(a)f(c)f(b)^{-1}f(d)^{-1} = (f(a)f(b)^{-1})(f(c)f(d)^{-1}) = \overline{f}\left(\frac{a}{b}\right)\overline{f}\left(\frac{c}{d}\right).$$

Finally, $\overline{f}$ is an extension of f: indeed, given any $r \in R$,

$$\overline{f}\left(\frac{r}{1}\right) = f(r)f(1)^{-1} = r \cdot 1_K^{-1} = r.$$

All that remains to show is that this map $\overline{f}$ is the unique ring homomorphism extending f to F. So let $g\colon F \to K$ be a ring homomorphism such that

$$g\left(\frac{r}{1}\right) = f(r).$$

Then since g preserves products, for any nonzero $b \in R$ we have

$$1_K = g(\frac{1}{1}) = g\left(\frac{b}{b}\right) = g\left(\frac{b}{1}\right) g\left(\frac{1}{b}\right) = f(b) g\left(\frac{1}{b}\right).$$

Thus

$$g\left(\frac{1}{b}\right) = f(b)^{-1}.$$

Therefore,

$$g\left(\frac{a}{b}\right) = g\left(\frac{a}{1}\right) g\left(\frac{1}{b}\right) = f(a)f(b)^{-1} = \overline{f}\left(\frac{a}{b}\right).$$

We conclude that $g = \overline{f}$. □