Math 566 - Homework 9

SOLUTIONS

Prof Arturo Magidin

1. Let K be an extension field of F.

   (i) Show that $[K:F]=1$ if and only if $K=F$.

   Proof. If $K=F$, then since F is a one-dimensional vector space over itself we get that $[K:F]=1$. Conversely, if $[K:F]=1$, then every nonzero element of K spans it as an F-vector space. In particular, 1 spans K, so $K=\{f\cdot 1\mid f\in F\}=\{f\mid f\in F\}=F$. $\square$

   (ii) Show that if $[K:F]$ is prime, and L is an intermediate field (that is, $F\subseteq L\subseteq K$), then either $F=L$ or $L=K$.

   Proof. By Dedekind's Product Theorem, we have $[K:F]=[K:L][L:F]$. So $[K:L]$ divides $[K:F]$. As the latter is prime, we have either $[K:L]=1$, in which case $K=L$ by part (i); or $[K:L]=[K:F]$, in which case $[L:F]=1$ and therefore by (i) we have $L=F$. $\square$

   (iii) Show that if $u\in K$ has degree n over F, and $[K:F]$ is finite, then n divides $[K:F]$.

   Proof. We have $F\subseteq F(u)\subseteq K$. Hence $[K:F]=[K:F(u)][F(u):F]=[K:F(u)]n$. Therefore, if $[K:F]$ is finite, then so is $[K:F(u)]$, and $n\mid[K:F]$, as desired. $\square$

2. Let $p(x)=x^3-6x^2+9x+3\in\mathbb{Q}[x]$.

   (i) Show that $p(x)$ is irreducible over $\mathbb{Q}$.

   Proof. This polynomial is "Eisenstein at $p=3$". That is, it satisfies the hypotheses of Eisenstein's Irreducibility Criterion with respect to the prime $p=3$: leading coefficient is not a multiple of 3; every other coefficient *is* a multiple of 3, and the constant term is not a multiple of $3^2=9$. Therefore, $p(x)$ is irreducible over $\mathbb{Q}$. $\square$

   (ii) Let u be a root of $p(x)$, and let $K=\mathbb{Q}(u)$. Express each of the following elements of K in terms of the basis $\{1,u,u^2\}$:

   (a) u^4.

   Answer. Dividing x^4 by $p(x)$, we have:

   $$x^4=(x+6)(x^3-6x^2+9x+3)+(27x^2-57x-18),$$

   so evaluating at u we get

   $$u^4=(u+6)(u^3-6u^2+9u+3)+(27u^2-57u-18)=-18-57u+27u^2,$$

   giving the desired expression.

   Alternatively, note that $0=p(u)=u^3-6u^2+9u+3$, hence $u^3=6u^2-9u-3$. Therefore,

   $$\begin{aligned}u^4&=u(u^3)=u(6u^2-9u-3)=6u^3-9u^2-3u\\&=6(6u^2-9u-3)-9u^2-3u=36u^2-54u-18-9u^2-3u\\&=-18-57u+27u^2,\end{aligned}$$

   same answer as above.

   (b) u^5.

   Answer. Dividing x^5 by x^3-6x^2+9x+3, we have:

   $$x^5=(x^2+6x+27)(x^3-6x^2+9x+3)+(105x^2-261x-81),$$

   so evaluating at u and remembering that $u^3-6u^2+9u+3=0$, we get

   $$u^5=-81-261u+105u^2.$$

(c) $3u^5 - u^4 + 2$.

Answer. We can use the two results we just obtained:

$$\begin{aligned} 3u^5 - u^4 + 2 &= 3(105u^2 - 261u - 81) - (27u^2 - 57u - 18) + 2 \\ &= 315u^2 - 783u - 243 - 27u^2 + 57u + 18 + 2 \\ &= -223 - 726u + 288u^2. \end{aligned}$$

(d) $(u+1)^{-1}$.

Answer. We express a constant in the form $p(x)(x+1) + q(x)(x^3 - 6x^2 + 9x + 3)$. We do this via long division. Dividing $x^3 - 6x^2 + 9x + 3$ by $x + 1$, we get

$$x^3 - 6x^2 + 9x + 3 = (x+1)(x^2 - 7x + 16) - 13.$$

After a rearrangement, we get:

$$\begin{aligned} 13 &= (x+1)(x^2 - 7x + 16) - (x^3 - 6x^2 + 9x + 3) \\ 1 &= \frac{1}{13}(x+1)(x^2 - 7x + 16) - \frac{1}{13}(x^3 - 6x^2 + 9x + 3). \end{aligned}$$

Evaluating at u, and recalling that $u^3 - 6u^2 + 9u + 3 = 0$, we get

$$1 = (u+1)\left(\frac{1}{13}(u^2 - 7u + 16)\right) - \frac{1}{13}(u^3 - 6u^2 + 9u + 3) = (u+1)\left(\frac{1}{13}u^2 - \frac{7}{13}u + \frac{16}{13}\right).$$

Therefore, $(u+1)^{-1} = \frac{16}{13} - \frac{7}{13}u + \frac{1}{13}u^2$. $\Box$

3. Let K be an extension of F, and let $u \in K$. Show that if $[F(u) : F]$ is finite and odd, then $F(u^2) = F(u)$.

Proof. Since $u^2 \in F(u)$, we have $F(u^2) \subseteq F(u)$. Thus, we have

$$[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F].$$

Note that $F(u) = F(u^2)(u)$; and that u satisfies a polynomial of degree 2 in $F(u^2)[x]$, namely $x^2 - u^2$. That means that $[F(u^2)(u) : F(u^2)] \leq 2$.

However, it cannot equal 2, because it must also divide $[F(u) : F]$, which is odd. Therefore, $[F(u^2)(u) : F(u^2)] = 1$, and therefore $F(u) = F(u^2)(u) = F(u^2)$, as required. $\Box$

Alternative proof. It is clear that $F(u^2) \subseteq F(u)$. Let $f(x)$ be the monic irreducible polynomial of u over F; write

$$f(x) = x^{2n+1} + a_{2n}x^{2n} + \cdots + a_1x + a_0, \qquad a_i \in F.$$

Evaluating at u, we have:

$$\begin{aligned} &u^{2n+1} + a_{2n}u^{2n} + \cdots + a_1u + a_0 = 0 \\ &u^{2n+1} + a_{2n-1}u^{2n-1} + \cdots + a_1u = -\left(a_{2n}u^{2n} + a_{2n-2}u^{2n-2} + \cdots + a_2u^2 + a_0\right) \\ &u\left(u^{2n} + a_{2n-1}u^{2n-2} + \cdots + a_1\right) = -\left(a_{2n}u^{2n} + a_{2n-2}u^{2n-2} + \cdots + a_2u^2 + a_0\right). \end{aligned}$$

Since $f(x)$ is the monic irreducible of u, the expression

$$u^{2n} + a_{2n-1}u^{2n-2} + \cdots + a_1$$

does not equal 0. Therefore,

$$u = -\frac{a_{2n}u^{2n} + \cdots + a_2u^2 + a_0}{u^{2n} + a_{2n-1}u^{2n-2} + \cdots + a_1} \in F(u^2).$$

This proves that $F(u) \subseteq F(u^2)$, yielding equality. $\Box$

4. Let E and F be field extensions of $\mathbb{Q}$. Prove that if $\sigma\colon E \to F$ is a nonzero field homomorphism, then $\sigma(q) = q$ for all $q \in \mathbb{Q}$.

   Proof. A field homomorphism $\sigma\colon E \to F$ must send 1_E to an element satisfying $e^2 = e$; this means that $e^2 - e = e(e - 1_F) = 0$. That means that either $e = 0$ (in which case σ sends everything to 0), or else $e = 1_F$. Since we are assuming that σ is not the zero map, it follows that $\sigma(1_E) = 1_F$.

   Here, $1_E = 1 = 1_F$ the rational number 1. We also know that $\sigma(0) = 0$. If k is a natural number and $\sigma(k) = k$, then $\sigma(k+1) = \sigma(k) + \sigma(1) = k + 1$. By induction, $\sigma(n) = n$ for all natural numbers n.

   Since σ is in particular a group homomorphism, if $n > 0$ is an integer, then $\sigma(-n) = -\sigma(n) = -n$, so σ fixes every integer.

   Finally, if a and b are integers, $b \neq 0$, then

   $$\sigma\left(\frac{a}{b}\right) = \sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1} = \frac{a}{b},$$

   so $\sigma(q) = q$ for all $q \in \mathbb{Q}$, as claimed. $\square$

5. Let $F = \mathbb{Q}(\sqrt{2})$.

   (i) Show that $x^2 - 3 \in F[x]$ is irreducible.

   Proof. It is enough to show that $x^2 - 3$ has no root in F. Assume to the contrary that it does. An element of F is of the form $p + q\sqrt{2}$ with $p, q \in \mathbb{Q}$, so we would have rational numbers p and q such that

   $$(p^2 + 2q^2) + 2pq\sqrt{2} = (p + q\sqrt{2})^2 = 3.$$

   Since $\{1, \sqrt{2}\}$ is a basis for F over $\mathbb{Q}$, we must have $2pq = 0$ and $p^2 + 2q^2 = 3$. Since $2pq = 0$, either $p = 0$ or $q = 0$. If $p = 0$, then $2q^2 = 3$. Writing $q = \frac{a}{b}$ with $\gcd(a, b) = 1$, we have that $2a^2 = 3b^2$. the power of 3 that divides the left hand side is even (since 3 must divide a), but the power of 3 that divides the right hand side is 1 (since $3 \nmid \gcd(a, b)$. So this is impossible. Hence $p \neq 0$, which means $q = 0$. Then $p^2 = 3$. But $x^2 - 3$ is irreducible over $\mathbb{Q}$, so there are no rationals p such that $p^2 = 3$. So this is also impossible. We conclude that $x^2 - 3$ is irreducible in $F[x]$. $\square$

   (ii) Show that every element of $F(\sqrt{3})$ can be written uniquely in the form

   $$a_0 + a_2\sqrt{2} + a_3\sqrt{3} + a_6\sqrt{6}, \qquad a_i \in \mathbb{Q}.$$

   Hint: Note that $\{1, \sqrt{3}\}$ is a basis for $F(\sqrt{3})$ over F, and that $\{1, \sqrt{2}\}$ is a basis for F over $\mathbb{Q}$.

   Proof. A basis for $F(\sqrt{3})$ over F is $\{1, \sqrt{3}\}$ (since we just proved that the monic irreducible of $\sqrt{3}$ over F is $x^2 - 3$). A basis for $F = \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$, because the monic irreducible of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. As in the proof of Dedekind's Product Theorem, we conclude that the set of pairwise products is a basis for $\mathbb{F}(\sqrt{3})$ over $\mathbb{Q}$; these pairwise products are 1, $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{2}\sqrt{3} = \sqrt{6}$. This proves the result. $\square$

   (iii) Define $\sigma\colon F(\sqrt{3}) \to F(\sqrt{3})$ by

   $$\sigma(a_0 + a_2\sqrt{2} + a_3\sqrt{3} + a_6\sqrt{6}) = a_0 - a_2\sqrt{2} + a_3\sqrt{3} - a_6\sqrt{6}.$$

   Prove that σ is an isomorphism of $F(\sqrt{3})$ to itself which does not restrict to the identity on F.

Proof. This is certainly a nonzero $\mathbb{Q}$-linear transformation from $F(\sqrt{3})$ to itself, so it is an additive automorphism that is $\mathbb{Q}$-homogeneous. We just need to show that it is multiplicative. We have:

$$\begin{aligned}
&\left(a_0 + a_2\sqrt{2} + a_3\sqrt{3} + a_6\sqrt{6}\right)\left(b_0 + b_2\sqrt{2} + b_3\sqrt{3} + b_6\sqrt{6}\right) \\
&\quad = (a_0b_0 + 2a_2b_2 + 3a_3b_3 + 7a_6b_6) \\
&\qquad + (a_0b_2 + a_2b_0 + 3a_3b_6 + 3a_6b_3)\sqrt{2} \\
&\qquad + (a_0b_3 + a_3b_0 + 2a_2b_6 + 2a_6b_2)\sqrt{3} \\
&\qquad + (a_0b_6 + a_6b_0 + a_2b_3 + a_3b_2)\sqrt{6}, \\
&\left(a_0 - a_2\sqrt{2} + a_3\sqrt{3} - a_6\sqrt{6}\right)\left(b_0 - b_2\sqrt{2} + b_3\sqrt{3} - b_6\sqrt{6}\right) \\
&\quad = (a_0b_0 + 2a_2b_2 + 3a_3b_3 + 7a_6b_6) \\
&\qquad + (-a_0b_2 - a_2b_0 - 3a_3b_6 - 3a_6b_3)\sqrt{2} \\
&\qquad + (a_0b_3 + a_3b_0 + 2a_2b_6 + 2a_6b_2)\sqrt{3} \\
&\qquad + (-a_0b_6 - a_6b_0 - a_2b_3 - a_3b_2)\sqrt{6} \\
&\quad = (a_0b_0 + 2a_2b_2 + 3a_3b_3 + 7a_6b_6) \\
&\qquad - (a_0b_2 + a_2b_0 + 3a_3b_6 + 3a_6b_3)\sqrt{2} \\
&\qquad + (a_0b_3 + a_3b_0 + 2a_2b_6 + 2a_6b_2)\sqrt{3} \\
&\qquad - (a_0b_6 + a_6b_0 + a_2b_3 + a_3b_2)\sqrt{6}.
\end{aligned}$$

Thus, $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, which proves that σ is indeed a field isomorphism.
Now note that $\sqrt{2} \in F$, but $\sigma(\sqrt{2}) \neq \sqrt{2}$, and we are done. $\square$

6. Show that there is an isomorphism from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(\sqrt{2}+1)$ that restricts to the identity on $\mathbb{Q}$, even though $\sqrt{2}$ and $\sqrt{2}+1$ do not satisfy the same monic irreducible over $\mathbb{Q}$.

   Proof. Simply note that $\mathbb{Q}(\sqrt{2}+1) = \mathbb{Q}(\sqrt{2})$, so that the isomorphism is simply the identity map on the set. Alternatively, we define $\sigma\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}+1)$ by

$$\sigma(p + q\sqrt{2}) = (p - q) + q(\sqrt{2}+1),$$

   where $p, q \in \mathbb{Q}$.

   The monic irreducible ov $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. The monic irreducible of $\sqrt{2}+1$ over $\mathbb{Q}$ is

$$(x-1)^2 - 2 = x^2 - 2x + 1 - 2 = x^2 - 2x - 1. \qquad \square$$

7. Let $\sigma\colon \mathbb{R} \to \mathbb{R}$ be a field automorphism.

   (i) Prove that σ must send positive reals to positive reals.

   Proof. Note that a real number is nonnegative if and only if it is a square. Since σ is multiplicative, $\sigma(r^2) = \sigma(r)^2$, so σ sends squares to squares. Since it sends 0 to 0, it follows that σ sends nonzero squares to nonzero squares, so σ sends positive reals to positive reals. The inverse has the same property, so $\sigma(r) > 0$ if and only if $r > 0$. $\square$

   (ii) Prove that if $a, b \in \mathbb{R}$ and $a < b$, then $\sigma(a) < \sigma(b)$.

   Proof. We have:

$$a < b \iff 0 < b - a$$

$$
\begin{aligned}
&\iff \sigma(0) < \sigma(b-a) \\
&\iff 0 < \sigma(b) - \sigma(a) \\
&\iff \sigma(a) < \sigma(b). \quad \square
\end{aligned}
$$

(iii) Show that if $q \in \mathbb{Q}$, then $\sigma(q) = q$.

Proof. This follows from Problem 4, taking $E = F = \mathbb{R}$. $\square$

(iv) Show that $\sigma(r) = r$ for every $r \in \mathbb{R}$.

Proof. By (ii) and (iii), if $q \in \mathbb{Q}$, then $q < r \iff q < \sigma(r)$.

If $r < \sigma(r)$, then let $q \in \mathbb{Q}$, $r < q < \sigma(r)$. Then $r < q$ implies $\sigma(r) < \sigma(q) = q$, which contradicts the choice of q to lie between r and $\sigma(r)$.

If $\sigma(r) < r$, then let $q \in \mathbb{Q}$ with $\sigma(r) < q < r$. Then $q < r$, so $q = \sigma(q) < \sigma(r)$, again contradicting the choice of q.

Thus, we have that $r \not< \sigma(r)$ and $r \not> \sigma(r)$. By trichotomy, $r = \sigma(r)$, as desired.