MATH30010: Field Theory
Homework 3: Solutions

1. Let $K$ be a field and let $F$ be a subfield (i.e. $K/F$ is an extension of fields). Let $p(x), q(x) \in F[x]$ with $q(x) \neq 0$. Prove that if $q(x)$ divides $p(x)$ over $K$, then $q(x)$ divides $p(x)$ over $F$.

[Hint: Use the ‘division algorithm’ for polynomials.]

Solution: This follows, for example, from the uniqueness of remainders (in the statement of the division algorithm). Since $p(x)$ divides $q(x)$ in $K[x]$, the remainder in $K[x]$ is 0. Now there exist $t(x), r(x) \in F[x]$ with $p(x) = t(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(q(x))$. But then $t(x), r(x) \in K[x]$ (since $F \subset K$) and hence $r(x) = 0$.

2. Let $F$ and $K$ be fields and suppose that $\phi : F \rightarrow K$ is a map satisfying

(a) $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in F$.
(b) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ for all $x, y \in F$.
(c) $\phi(1) \neq 0$.

Prove the following:

(a) $\phi(0) = 0$
(b) $\phi(1) = 1$
(c) $\phi(-x) = -\phi(x)$ for all $x \in F$.
(d) If $x \neq 0$ in $F$ then $\phi(x) \neq 0$ in $K$ and $\phi(x^{-1}) = \phi(x)^{-1}$.
(e) $\phi$ is injective: If $x \neq y$ in $F$ then $\phi(x) \neq \phi(y)$ in $K$.

Solution:

(a) $\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0)$. Subtract $\phi(0)$ from both sides to get: $0 = \phi(0)$.

(b) $\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$. Divide both sides by $\phi(1) \neq 0$ to get $1 = \phi(1)$.

(c) Let $x \in F$. $0 = \phi(0) = \phi(x + (-x)) = \phi(x) + \phi(-x) \implies -\phi(x) = \phi(-x)$.

(d) Let $x \in F$, $x \neq 0$. Then $1 = \phi(1) = \phi(x \cdot x^{-1}) = \phi(x) \cdot \phi(x^{-1})$. This shows that $\phi(x) \neq 0$ and that $\phi(x^{-1}) = \phi(x)^{-1}$ (by uniqueness of inverses, for example).

(e) Suppose that $x, y \in F$ and $\phi(x) = \phi(y)$. Then $0 = \phi(x) - \phi(y) = \phi(x) + \phi(-y) = \phi(x - y)$. It follows from (d) that $x - y = 0$. Thus $x = y$. So $\phi$ is injective.
3. (a) Prove that \( x^3 + x + 1 \) is irreducible in \( \mathbb{Q}[x] \).
(b) Prove that \( x^3 + 11x - 27x + 3 \) is irreducible in \( \mathbb{Q}[x] \).
(c) Is \( x^5 + x + 1 \) irreducible in \( \mathbb{F}_2[x] \)? Prove your assertion.
(d) Show that \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{F}_2[x] \).

Solution:

(a) Since this is a cubic, it is reducible if and only if it has roots.
By the rational root test, the only possible rational roots are \( \pm 1 \).
Since neither of these is a root, it follows that \( x^3 + x + 1 \) is irreducible over \( \mathbb{Q} \).

(b) By the rational root test, the only possible roots are \( \pm 3 \). It is straightforward to verify neither is a root. Thus the polynomial has no rational roots. Since it is cubic, it follows that it is irreducible.

(c) It is easy to see that \( x^5 + x + 1 \) has no roots in \( \mathbb{F}_2 \). Thus it has no linear factors, and hence if it is reducible it must have a quadratic irreducible factor. It is easy to see that \( x^2 + x + 1 \) is the only irreducible quadratic in \( \mathbb{F}_2[x] \). Dividing this into \( x^5 + x + 1 \) we find that \( x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1) \). So our polynomial is reducible in this case.

(d) The same opening remarks apply to this polynomial as in the last case. This time, however, we find that \( x^2 + x + 1 \) does not divide \( x^5 + x^2 + 1 \) (it goes in \( x^3 + x^2 \) times with remainder 1). Thus \( x^5 + x^2 + 1 \) has no linear or quadratic factors and so must be irreducible.

4. (a) Let \( F \) be a field and let \( q(x) \in F[x] \) be irreducible. Suppose that \( f(x), g(x) \in F[x] \) and that \( q(x)|f(x)g(x) \). Prove that \( q(x)|f(x) \) or \( q(x)|g(x) \) (this includes the possibility that \( q(x) \) divides both).
[Hint: Suppose \( q(x) \nmid f(x) \). Then there exist \( s(x), t(x) \in F[x] \) with \( 1 = q(x)s(x) + f(x)t(x) \). Use this to prove that \( q(x)|g(x). \)]

(b) Give an example of a field \( F \) and three polynomials \( q(x), f(x), g(x) \in F[x] \) such that \( q(x)|f(x)g(x) \) but \( q(x) \nmid f(x) \) and \( q(x) \nmid g(x) \).

Solution:

(a) By assumption, we have \( f(x)g(x) = q(x)h(x) \) for some \( h(x) \in F[x] \).
Suppose \( q(x) \nmid f(x) \). Then there exist \( s(x), t(x) \in F[x] \) with
\[ 1 = q(x)s(x) + f(x)t(x). \] Then

\[
g(x) = g(x) \cdot 1 = g(x)[q(x)s(x) + f(x)t(x)]
= g(x)q(x)s(x) + f(x)q(x)t(x)
= q(x)g(x)s(x) + q(x)h(x)t(x)
= q(x)[g(x)s(x) + h(x)t(x)]
\]

which shows that \( q(x) \) divides \( g(x) \).

(b) Take, for example, \( F = \mathbb{Q}, f(x) = x + 1, g(x) = x - 1 \) and \( q(x) = x^2 - 1 \).

5. Construct a field with 16 elements. Explain how you know that it is a field.

**Solution:** If \( q(x) \) is an irreducible degree 4 polynomial in \( \mathbb{F}_2[x] \), then the field \( K = \mathbb{F}_2(q(x)) \) will have 16 elements. So we just need to find an irreducible quartic over \( \mathbb{F}_2 \). An example is \( q(x) = x^4 + x^3 + x^2 + x + 1 \). It has no roots in \( \mathbb{F}_2 \), hence no linear factors. Thus if it factored it would have to be a product of two irreducible quadratic factors. The only irreducible quadratic in \( \mathbb{F}_2[x] \) is \( x^2 + x + 1 \) and \( (x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq q(x) \). So \( q(x) \) is irreducible.

6. Let \( q(x) = x^3 - 2 \in \mathbb{F}_7[x] \). Find the inverse of \( 1 + \theta + \theta^2 \) in \( K = \mathbb{F}_7(q(x)) \).

**Solution:** Division shows that \( x^3 + 5 = (x + 6)(x^2 + x + 1) + 6 \) in \( \mathbb{F}_7[x] \). Thus \( 1 = -6 = (x + 6)(x^2 + x + 1) - (x^3 + 5) \). It follows that \( 1 = (\theta + 6)(\theta^2 + \theta + 1) \) in \( K \).

7. Show that \( q(x) = x^3 + x + 1 \) is irreducible in \( \mathbb{F}_5[x] \). Let \( K \) be the field \( \mathbb{F}_5(q(x)) \). Find the inverse of the element \( 1 + \theta^2 \) in \( K \).

**Solution:** Division shows that \( x^3 + x + 1 = x(x^2 + 1) + 1 \) in \( \mathbb{F}_5[x] \). Thus \( 1 = (x^3 + x + 1) - x(x^2 + 1) \). It follows that \( 1 = -\theta(1 + \theta^2) \) in \( K \).

8. (a) Find a quartic polynomial with integer coefficients which has \( \sqrt{2} + \sqrt{-2} \) as a root.

(b) Find a quartic polynomial with integer coefficients which has \( \sqrt{2} + \sqrt{3} \) as a root.

**Solution:**

(a) Let \( a = \sqrt{2} + \sqrt{-2} \). Then \( a^2 = 2\sqrt{-4} \). Thus \( a^4 = -16 \). So \( a \) is a root of \( x^2 + 16 \).
(b) Let \( b = \sqrt{2 + \sqrt{3}} \). Then \( b^2 = 2 + \sqrt{3}; b^2 - 2 = \sqrt{3} \). So \( (b^2 - 2)^2 = 3 \); i.e. \( b^4 - 4b^2 + 4 = 3 \) and thus \( b^4 - 4b^2 + 1 = 0 \). So \( b \) is a root of \( x^4 - 4x^2 + 1 \in \mathbb{Z}[x] \).