Problem set

1. Suppose $E$ is a finite integral domain of characteristic $p$. Let $F_p : E \to E, F_p(x) := x^p$. Prove that $F_p$ is a ring isomorphism. (Long ago in class we proved that $F_p$ is a ring homomorphism in any ring of characteristic $p$ when $p$ is prime. Go over your notes and rewrite that part of the argument as well. Notice that you have to argue why $p$ is prime and why $F_p$ is a bijection.)

Proof. Since $E$ is finite ring, characteristic of $E$ cannot be 0 (otherwise $\{1, 1 + 1, \ldots \}$ is infinite set in $E$). Moreover, since $E$ is a domain, we have seen in class that characteristic $p$ has to be a prime number.

Note that using binomial theorem

$$F_p(x + y) = (x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p = F_p(x) + F_p(y)$$

, since $p$ divides $\binom{p}{r}$ for $0 < r < p$. Moreover, since $E$ is commutative $F_p(xy) = x^py^p = F_p(x)$ for all $x, y \in E$. Thus $F_p$ is a ring homomorphism.

Note that $\ker(F_p) \subset E$ is an ideal since $F_p$ is a ring homomorphism. However the only possible ideals in a field $E$ (finite integral domain is a field) are $\{0\}$ or $E$. Since $F_p(1) = 1$, we get that $\ker(F_p) = \{0\}$ thus $F_p$ is injective. Since $E$ is finite, $F_p$ is bijective hence an isomorphism.

2. (a) Prove that the minimal polynomial of $\alpha = \sqrt{1 + \sqrt{3}}$ is $f(x) = x^4 - 2x^2 - 2$.

Proof. Note that $\alpha^2 - 1 = \sqrt{3}$, hence $(\alpha^2 - 1)^2 = 3$ which simplifies to $f(\alpha) = 0$. To show that $f(x)$ is the minimal polynomial satisfying $f(\alpha) = 0$, we need to show $f(x)$ is irreducible. We obtain this by applying Eisenstein’s criterion for prime $p = 2$.

(b) Prove that $\mathbb{Q}[\alpha] := \{c_0 + \cdots + c_3\alpha^3 | c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$ is a subring of $\mathbb{C}$. 

1
3. Suppose \( E \) is an isomorphism theorem.

(a) Prove that \( \ker \alpha \) that \( \alpha \) is a (non-zero) constant as polynomial. Hence \( \ker \phi \) no zeros. Moreover \( f \) Let \( g(x) = f(x) + r(x) \) where \( \deg(f) > \deg(r) \).

We apply it in our situation by noting that any polynomial in \( \alpha \) (call it \( g(\alpha) \)), \( g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \) since \( f(\alpha) = 0 \), where degree of \( r(x) \) is less than 3. That is to say \( g(\alpha) = r(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \in Q[\alpha] \).

Multiplication or addition in \( Q[\alpha] \) is a polynomial in \( \alpha \) hence by above argument it can be represented by elements in \( Q \).

(c) Prove that \( Q[x]/\langle f(x) \rangle \cong Q[\alpha] \).

Proof. Let \( \phi_\alpha : Q[x] \to C \) be the evaluation homomorphism which takes any polynomial \( g(x) \) to \( g(\alpha) \in C \). Observe that from previous problem we note that image of \( \phi_\alpha \) is \( Q[\alpha] \).

Moreover we know that \( Ker(\phi_\alpha) = \langle f(x) \rangle \), so the required result follows from the first isomorphism theorem.

(d) Write \( \alpha^{-1} \) in term of \( c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \) with \( c_i \in Q \).

Proof. Observe that \( f(\alpha) = \alpha^4 - 2\alpha^2 - 2 = 0 \), thus by dividing \( \alpha \), we obtain \( \alpha^3 - 2\alpha - 2 \alpha^{-1} = 0 \) which implies

\[
\alpha^{-1} = \frac{\alpha^3 - 2\alpha}{2}.
\]

(e) Write \( (1 + \alpha)^{-1} \) in the form \( c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \) with \( c_i \in Q \).

Answer. Let \( g(y) = f(y - 1) = (y - 1)^4 - 2(y - 1)^2 - 2 = y^4 - 4y^3 + 4y^2 - 3 \), and note that \( g(\alpha + 1) = f(\alpha) = 0 \). Thus by the same procedure as before, \( y^3 - 4y^2 + 4y - \frac{3}{y} = 0 \) for \( y = \alpha + 1 \), which implies

\[
(\alpha + 1)^{-1} = \frac{(\alpha + 1)^3 - 4(\alpha + 1)^2 + 4(\alpha + 1)}{3}
\]

3. Suppose \( E \) is a finite field that contains \( Z_3 \) as a subring. Suppose there is \( \alpha \in E \) such that \( \alpha^3 - \alpha + 1 = 0 \). Let \( \phi_\alpha : Z_3[x] \to E \) be the map of evaluation at \( \alpha \).

(a) Prove that \( \ker \phi_\alpha = \langle x^3 - x + 1 \rangle \).

Proof. Note that \( Z_3 \) is a field hence \( Z_3[x] \) is a principal ideal domain (PID) and \( \phi_\alpha \) is a homomorphism. Thus \( \ker \phi_\alpha = \langle g(x) \rangle \) for some \( g(x) \in Z_3[x] \).

Let \( f(x) := x^3 - x + 1 \). Note that \( f(x) \) is irreducible since it degree 3 polynomial with no zeros. Moreover \( \phi_\alpha(f(x)) = f(\alpha) = 0 \), thus \( f(x) \in \ker \phi_\alpha = \langle g(x) \rangle \), which implies \( f(x) = g(x)h(x) \). Since \( f(x) \) is irreducible and \( g(x) \) is not a constant polynomial, \( h(x) \) is a (non-zero) constant as polynomial. Hence \( \ker \phi_\alpha = \langle f(x) \rangle \).
(b) Prove that \( \text{Im} \phi_\alpha = \{ c_0 + c_1 \alpha + c_2 \alpha^2 | c_0, c_1, c_2 \in \mathbb{Z}_3 \} \).

Proof. Note that image of \( \phi_\alpha \) consists of all polynomials in \( \alpha \) (i.e \( g(\alpha) \in E \) where \( g(x) \in \mathbb{Z}_3[x] \)). We have seen that euclidean algorithm for polynomials over any field, thus for any polynomial \( g(x) \in \mathbb{Z}_3[x] \), there exists polynomials \( q(x), r(x) \in \mathbb{Z}_3[x] \) such that \( g(x) = q(x)f(x) + r(x) \) where \( 3 \deg(f) > \deg(r) \). Applying this to our situation, we see that \( g(\alpha) = r(\alpha) = c_0 + c_1 \alpha + c_2 \alpha^2 \), where \( c_i \in \mathbb{Z}_3 \).

(c) Let us denote the image of \( \phi_\alpha \) by \( \mathbb{Z}_3[\alpha] \). Prove that \( \mathbb{Z}_3 \) is a finite field with 27 elements.

Proof. Note that \( c_0 + c_1 \alpha + c_2 \alpha^2 = 0 \) implies \( c_0 = c_1 = c_2 = 0 \) because \( f(x) = x^3 - x + 1 \) is the minimal polynomial satisfying \( f(\alpha) = 0 \). Thus \( c_0 + c_1 \alpha + c_2 \alpha^2 = b_0 + b_1 \alpha + b_2 \alpha^2 \) implies \( c_i = b_i \) for all \( i \). Hence by using part (b) we conclude that \( \mathbb{Z}_3[\alpha] \) is in set theoretic bijection with \( \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \) given by \( (c_0 + c_1 \alpha + c_2 \alpha^2) \mapsto (c_0, c_1, c_2) \). Thus there are precisely \( 3^3 = 27 \) elements in \( \mathbb{Z}_3[\alpha] \).

Note that \( \mathbb{Z}_3[\alpha] \) is a subring of the field \( E \) (since it is the image of a homomorphism), thus \( \mathbb{Z}_3[\alpha] \) is an integral domain. Since any finite integral domain is a field, we conclude \( \mathbb{Z}_3[\alpha] \) is a field. \( \square \)

4. Suppose \( I \) and \( J \) are two ideals of a commutative ring \( R \).

(a) Prove that \( I \cap J \) is an ideal of \( R \).

Proof. Let \( a, b \in I \cap J \) and \( r \in R \), then \( a, b \in I \) and \( a, b \in J \). Since \( I \) and \( J \) are ideals, \( (a + b), ar \) are both in \( I \) and \( J \), hence \( (a + b), ar \in I \cap J \). Thus \( I \cap J \) is an ideal. \( \square \)

(b) Let \( I + J := \{ x + y | x \in I, y \in J \} \). Prove that \( I + J \) is an ideal of \( R \).

Proof. Let \( a = (x + y), b = (x' + y') \in I + J \) and \( r \in R \), then \( a + b = (x + x') + (y + y') \in I + J \) and \( ar = (xr + yr) \in I + J \). Hence \( I + J \) is an ideal. \( \square \)

5. Suppose \( R \) is a unital commutative ring and \( x_1, \ldots, x_n \in R \).

(a) Let \( I = Rx_1 + Rx_2 + \cdots + Rx_n = \{ r_1 x_1 + \cdots + r_n x_n \} \), where \( Rx_i = \langle x_i \rangle \). Prove that \( I \) is an ideal.

Proof. The proof is nearly same as the proof of part (b) of the previous problem. \( \square \)

(b) Prove that the ideal \( I \) is the smallest ideal that contains \( x_1, \ldots, x_n \).

Proof. Note that \( I \) contains \( x_1, \ldots, x_n \) so we need to show that for any ideal \( J \subset R \) containing \( x_1, \ldots, x_n \) we have \( I \subset J \). Any element \( a \in I \) can be written as \( a = r_1 x_1 + \cdots + r_n x_n \), we need to show that \( a \in J \). This follows since \( x_i \in J \) and \( r_i \in R \), we get \( r_i x_i \in J \) and hence \( \sum_{i=1}^{n} r_i x_i = a \in J \) since \( J \) is an ideal. \( \square \)
6. Let $I := \langle 2, x \rangle = \{2f(x) + xg(x) : f, g \in \mathbb{Z}[x] \}$. Prove that $I$ is not a principal ideal. Deduce that $\mathbb{Z}[x]$ is not a PID.

**Proof.** Suppose $I = \langle h(x) \rangle$ for some $h(x) \in \mathbb{Z}[x]$. Note that $2 = h(x)q(x)$ and $x = h(x)r(x)$ for some $q(x), r(x) \in \mathbb{Z}[x]$ because $2, x \in I$. We use $2 = h(x)q(x)$ to conclude that $\deg h(x) = 0$ as polynomial, thus $h(x) = c$ where $c|2$. Moreover since $r(1) = cr(1)$, evaluating this equation at $x = 1$, we get $1 = cr(1)$ where $c \in \mathbb{Z}$, thus $c = \pm 1$.

Although since $c \in I$, there exists $f(x), g(x) \in \mathbb{Z}[x]$ such that $c = 2f(x) + xg(x)$. Evaluating this equation at $x = 0$ we get $c = 2f(0) + 0g(0) = 2f(0)$, since $c = \pm 1$ and $f(0) \in \mathbb{Z}$, we get a contradiction. \hfill \square

7. Suppose $E$ is a finite field that contains $\mathbb{Z}_p$ as a subring. Suppose $a \in \mathbb{Z}_p^\times$. Suppose there is $\alpha \in E$ such that $\alpha^p - \alpha + a = 0$.

(a) Prove that $\alpha + 1, \alpha + 2, \ldots, \alpha + (p - 1)$ are zeroes of $g(x) = x^p - x + a$.

**Proof.** Note that since characteristic of $E$ is $p$, $(\alpha + \beta)^p = \alpha^p + \beta^p$ for all $\alpha, \beta \in E$. Thus

$$(\alpha + i)^p - (\alpha + i) + a = \alpha^p - \alpha + a + i^p - i = 0,$$

since $\alpha^p - \alpha + a = 0$ and by Fermat’s little theorem $i^p - i = 0$ for $i \in \{0, 1, \ldots, p - 1\}$. Thus $\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + (p - 1)$ are zeroes of $g(x) = x^p - x + a$. \hfill \square

(b) Prove that in $E[x]$ we have

$$x^p - x + a = (x - \alpha)(x - \alpha + 1) \ldots (x - \alpha + p - 1).$$

**Proof.** By using generalized factor theorem $h(x) := (x - \alpha)(x - \alpha + 1) \ldots (x - \alpha + p - 1)$ divides $g(x) = x^p - x + a$ since $\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + (p - 1)$ are distinct zeros of $g(x)$. Observe that $\deg h(x) = \deg g(x)$, thus $g(x) = ch(x)$, and since leading term of both $g(x)$ and $h(x)$ are 1, we get $g(x) = h(x)$ as required. \hfill \square

(c) Suppose $f(x)$ is a (monic) divisor of $g(x) = x^p - x + a$. Argue why $f(x) = (x - \alpha - i_1) \ldots (x - \alpha - i_d)$ for some $i_1, \ldots, i_d \in \mathbb{Z}_p$.

**Proof.** We can write $g(x) = f(x)t(x)$ for some polynomial $t(x) \in E[x]$. Since $g(\alpha + i) = 0$ for $i \in \{0, 1, \ldots, p - 1\}$, for each $i$, either $f(\alpha + i) = 0$ or $t(\alpha + i) = 0$. Let $S = \{i \mathbb{Z}_p : f(\alpha + i) = 0\}$ and $T = \{i \in \mathbb{Z}_p : t(\alpha + i) = 0\}$, thus $S \cup T = \{0, 1, \ldots, p - 1\}$.

By generalized factor theorem,

$$q_1(x)\prod_{i \in S}(x - \alpha - i) = f(x)$$

$$q_2(x)\prod_{i \in T}(x - \alpha - i) = t(x)$$
and we have $\deg f(x) = |S| + \deg q_1(x)$ and $\deg t(x) = |T| \deg q_2(x)$. We also know $\deg f(x) + \deg t(x) = \deg g(x) = p$, we get $|S| + |T| + \deg q_1(x) + \deg q_2(x) = p = |S \cup T|$ which is only possible when $\deg q_i = 0$ for $i = 1, 2$ and $S \cap T = \{\}$. In particular we get $f(x) = \prod_{i \in S}(x - \alpha - i)$ as required.

(d) Show that coefficient of $x^{d-1}$ of $f$ is $-(d\alpha + i_1 + \cdots + i_d)$.

Proof. We have $f(x) = (x - \alpha - i_1) \cdots (x - \alpha - i_d)$, simply by expanding the polynomial we see that coefficient of $x^{d-1}$ is $-(\alpha + i_1) - \cdots - (\alpha + i_d) = -(d\alpha + i_1 + \cdots + i_d)$.

(e) Suppose $f(x) \in \mathbb{Z}_p[x]$ is a divisor of $x^p - x + a$ and $0 < \deg f < p$. Prove that $\alpha \in \mathbb{Z}_p$.

Proof. Note that $f(x) \in \mathbb{Z}_p[x]$ implies that coefficient of $x^{d-1}$ is in $\mathbb{Z}_p$. Thus by part (b), $d\alpha + i_1 + \cdots + i_d \in \mathbb{Z}_p$ which implies $\alpha \in \mathbb{Z}_p$ since $i_1, \ldots, i_d \in \mathbb{Z}_p$ and $0 \neq d \in \mathbb{Z}_p$ (we have used that fact that $\mathbb{Z}_p$ is a field).

(f) Use previous part and Fermat’s little theorem to get a contradiction, and deduce that $x^p - x + a$ is irreducible.

Proof. Suppose $f(x)$ is a divisor of $x^p - x + a$ such that $0 < \deg f < p$, then by previous part $\alpha \in \mathbb{Z}_p$. By Fermat’s theorem, we know $\alpha^p - \alpha = 0$ which is a contradiction because $\alpha$ is a zero of $x^p - x + a$ (that is $\alpha^p - \alpha + a = 0$) and $a \in \mathbb{Z}^\times$.