FIELD THEORY HOMEWORK 2 SOLUTIONS

JC

(1) Recall that if \( p \) is a prime number then \( (p) = p\mathbb{Z} \) is a maximal ideal in \( \mathbb{Z} \), and so \( \mathbb{Z}/p\mathbb{Z} \) is a field with \( p \) elements. Recall also that for any field \( k \), the ring \( k[x] \) is a PID and hence is a UFD.

(a) Let \( E = \mathbb{Z}/2\mathbb{Z} \). Find all the irreducible polynomials of degrees 1, 2 and 3 in \( E[x] \) (you should find 2 of degree 1, 1 of degree 2 and 2 of degree 3). Exhibit factorisations into irreducibles for all the polynomials of degree 3. (Keep in mind that 1 + 1 = 0, so for example \( (x+1)^2 = x^2 + 1 \).) Polynomials of degree one are always irreducible in \( k[x] \) for \( k \) a field: here the only possibilities are \( x \) and \( x+1 \).

If a polynomial of degree two is irreducible it is the product of two polynomials of degree one, uniquely up to associates (but 1 is the only unit, so that means uniquely). \( x \times x = x^2 \), \( x \times (x+1) = x^2 + x \), \( (x+1) \times (x+1) = x^2 + 1 \). So the only irreducible of degree two is \( x^2 + x + 1 \).

Similarly a non-irreducible of degree three is a product of polynomials of smaller degree. We see that \( x^3, (x+1)^3 = x^3 + x^2 + x + 1, x^2(x+1) = x^3 + x^2, x(x^2 + x + 1) = x^3 + x^2 + x, (x+1)(x^2 + x + 1) = x^3 + 1 \) are not irreducible. That leaves \( x^3 + x + 1 \), \( x^3 + x + 1 \) as the irreducibles. Alternative proof: in \( k[x] \) a polynomial of degree three is irreducible iff it has no linear factor iff it has no root.

(b) Choose one of the polynomials of degree 3 on your list. Call it \( m \). By general theory the quotient ring \( F = E[x]/(m) \) is a field, and every element of \( F \) is of the form \( r + (m) \) for a unique polynomial \( r \) of the form \( r_0 + r_1 x + r_2 x^2 \) with \( r_i \in E \).

I choose \( m = x^3 + x + 1 \). Notice that since 1 = -1 we have \( m = x^3 - x - 1 \), that is to say that \( x^3 \) is congruent to \( x + 1 \) mod \( m \).

What is \( |F| \)?

There are two choices for each of \( r_0, r_1, r_2 \) so that \( |F| = 8 \).

Prove that \( f + f = 0 \) for all \( f \in F \).

This is easy, as \( p + p = 0 \) for all \( p \in E[x] \).

For each unit in \( F \), find its multiplicative inverse in \( F \) and its order in the group of units (that is the group formed by the set of units under multiplication). Which units (if any) are generators of the group of units of \( F^\times \)?

The units of \( F \) are the 7 non-zero elements.

Let \( a = x + (m) \), so that elements of \( F \) are of form \( r_0 + r_1 a + r_2 a^2 \) with \( r_i \in E \).

Now the powers of \( a \) are \( a^2, a^3 = a + 1, a^4 = a^2 + a, a^5 = a^3 + a^2 = a^2 + a + 1, a^6 = a^3 + a^2 + a = a + 1 + a^2 + a = a^2 + 1, a^7 = a^3 + a = a + 1 + a = 1 \).
That is to say, $a$ has order 7 in the group of units, which is therefore cyclic of order 7. So all the units other than 1 are generators, and they come in mutually inverse pairs: $a$ and $a^2 + 1$, $a^2$ and $a^3 = a^2 + a + 1$, $a^3 = a + 1$ and $a^4 = a^2 + a$.

(2) An automorphism of a ring $R$ is an isomorphism from $R$ to $R$, that is a permutation $\phi$ of the elements of $R$ which respects addition and multiplication in the sense that $\phi(a + b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

(a) Prove that for any ring $R$ and any automorphism $\phi$ of $R$, $\phi(0) = 0$ and $\phi(1) = 1$.

$b(0) + \phi(0) = \phi(0 + 0) = \phi(0)$, so that $\phi(0) = 0$. Similarly $1 \neq 0$ so $\phi(1)\phi(1) = \phi(1) \neq 0$, and so $\phi(1) = 1$.

(b) Let $k$ be a field, let $a$ be a generator for the group of units of $k$, and let $\phi$ be an automorphism of $k$. Prove that $\phi(a)$ is also a generator. Prove further that for every generator $b$ there is at most one automorphism $\phi$ such that $\phi(a) = b$.

Every nonzero element of $k$ is of form $a^n$. Let $b \in k$ be nonzero, and let $c \in b$ be such that $\phi(c) = b$ and let $n$ be such that $c = a^n$. Then $b = \phi(c) = \phi(a^n) = \phi(a)^n$, so that $\phi(a)$ is also a generator.

(c) Find all the automorphisms of the field $F$ which you constructed in the preceding question. [Note that this was the original version of the question].

Consider the polynomial $x^3 + x + 1$. A little thought shows that any automorphism must permute its roots. The roots are $a$ (obviously), $a^2$ because $a^0 + a^2 + 1 = a^2 + 1 + a^2 + 1 = 0$, and $a^3$ because $a^{12} + a^4 + 1 = a^5 + a^4 + 1 = a^2 + a + a^2 + a + 1 + 1 = 0$.

If $\phi(a) = a$ then $\phi(a^n) = a^n$ for all $n$, so there is at most one such $\phi$. Similarly there is at most one $\phi$ with $\phi(a) = a^2$ or $a^4$. One cancheck that these are all automorphisms.

(3) Let $a = 2^{1/3}$, the real cube root of 2. It is a fact (proved a bit later in the course) that the minimal polynomial of $a$ over $\mathbb{Q}$ is $x^3 - 2$. By results from class every element of $\mathbb{Q}(a)$ is of form $q_0 + q_1 a + q_2 a^2$ for unique rational numbers $q_0, q_1, q_2$.

Prove that $\sqrt[3]{2} \notin \mathbb{Q}(a)$.

The minimal polynomial of $\sqrt[3]{2}$ is $x^2 - 2$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2$. On the other hand $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. By the theorem on multiplicativity of degree, it is not possible that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(a)$, otherwise we would have $3 = 2 \times [\mathbb{Q}(a) : \mathbb{Q}(\sqrt[3]{2})]$. Note: this is much more efficient than a proof by direct calculation.

Express the multiplicative inverses of the elements $a, 1 + a, 1 + a + a^2$ in the form $q_0 + q_1 a + q_2 a^2$.

This amounts to an exercise in Euclid’s algorithm: we compute for appropriate polynomials $p$ some polynomials $A, B$ such that $Ap + B(x^3 - 2) = \gcd(p, x^3 - 2) = 1$, then we are basically done.

$x^3 - 2 = xx^2 + (-2)$, so $l = (x^2/2)x - (1/2)(x^3 - 2)$, so $l = (a^2/2)a$ and $a^{-1} = a^2/2$.

$x^3 - 2 = (1 + x)(x^2 - x + 1) - 1$, so $(1 + a)(a^2 - a + 1) = 1$, $(a + 1)^{-1} = a^2 - a + 1$.
The Fundamental Theorem of Algebra states that every complex polynomial of degree greater than zero has a complex root, which implies (think about it!) that the only irreducible polynomials in \( \mathbb{C}[x] \) are the linear ones.

(a) If \( z = a + bi \) \((a, b \text{ real})\) is a complex number then the complex conjugate \( \bar{z} \) of \( z \) is given by \( \bar{z} = a - bi \). The map \( z \mapsto \bar{z} \) is easily seen to be an automorphism of \( \mathbb{C} \).

Define a map \( f \mapsto \bar{f} \) from \( \mathbb{C}[x] \) to \( \mathbb{C}[x] \) as follows: if \( f = \sum_{i=0}^{n} a_i x^i \) then \( \bar{f} = \sum_{i=0}^{n} \bar{a_i} x^i \). Prove that \( f \mapsto \bar{f} \) is an automorphism of the ring \( \mathbb{C}[x] \).

This is routine, since the ring operations in the polynomial ring are defined in terms of the ring operations in \( \mathbb{C} \).

(b) Which elements \( f \) of \( \mathbb{C}[x] \) have \( f = \bar{f} \)?

Easily, \( f = \bar{f} \) if and only if \( f \in \mathbb{R}[x] \).

(c) Prove that \( ff \in \mathbb{R}[x] \) for all \( f \in \mathbb{C}[x] \).

\( \overline{ff} = ff \).

(d) Let \( g \in \mathbb{R}[x] \) be a monic irreducible in \( \mathbb{R}[x] \). Prove that \( g \) is linear or quadratic. Hint: start by proving that if \( x - a \) divides \( g \) in \( \mathbb{C}[x] \) then \( x - \bar{a} \) also divides \( g \) in \( \mathbb{C}[x] \).

If \( g = (x - a)h \) then \( g = \bar{g} = (x - a)\bar{h} = (x - \bar{a})h \), so that \( x - a \) also divides \( g \).

By the FTOA, \( g \) is a product of linear factors in the ring of complex polynomials. Let \( x - a \) be one of them, so that \( x - a \) divides \( g \) in \( \mathbb{C}[x] \), say \( g = (x - a)q \) for some \( q \in \mathbb{C}[x] \).

Suppose \( a \) is real, and consider the division algorithm: since \( \mathbb{R} \) is a subfield of \( \mathbb{C} \), all coefficients of \( q \) are real. So \( x - a \) divides \( g \) in \( \mathbb{R}[x] \), and so \( g \) is an associate of \( x - a \) in \( \mathbb{R}[x] \).

If \( a \) is not real, \( g \) is divisible in \( \mathbb{C}[x] \) by the real quadratic polynomial \((x - a)(x - \bar{a})\). But the division algorithm tells us that this polynomial divides \( g \) in \( \mathbb{R}[x] \), so as before \( g \) is an associate of \((x - a)(x - \bar{a})\) in \( \mathbb{R}[x] \).