Math 404 HW 1 Solutions

Problem 1.1

To find $g(x)$, we use polynomial long division:

(x-1) $\overline{)x^5 + x^4 + x^3 + x^2 + x - 5}$

Our result is that $g(x) = x^4 + 2x^3 + 3x^4 + 4x + 5$.

Problem 1.2

The short answer to this problem is theorem 6.14 plus theorem 5.10. Below is a solution that's self-contained except for recourse to theorem 4.8

We will prove (3) $\implies$ (2) $\implies$ (1) $\implies$ (3).

(3) implies (2)

Suppose $k[x]/(f)$ is a field. Let $p, q \in k[x]$ so that $pq \in (f)$. Note that this means $[pq] = 0$ in $k[x]/(f)$. To show that (f) is prime, we must show that at least one of p or q is in (f).

So suppose $p \notin (f)$. Then we have that $[p] \neq 0$ in $k[x]/(f)$, by definition of quotient rings. Since $k[x]/(f)$ is a field, there is another element $c \in k[x]/(f)$ so that $c[p] = 1$. Then we compute

$$\begin{aligned}
[q] &= 1 \cdot [q] \\
&= (c[p]) \cdot [q] \\
&= c([p] \cdot [q]) \\
&= c \cdot [pq] \\
&= c \cdot 0 \\
&= 0.
\end{aligned}$$

Thus, we have that $[q] = 0$. By definition of quotient rings, we have that $q \in (f)$. Thus, we have shown that if $pq \in (f)$ but $p \notin (f)$ then $q \in (f)$. Similar reasoning shows that if $pq \in (f)$ but $q \notin (f)$ then $p \in (f)$. Either way, at least one of p or q is in (f), so (f) is prime. □

(2) implies (1)

Suppose that $f = gh$. This means in particular that f divides gh (as $gh = 1 \cdot f$), so that $gh \in (f)$. Since (f) is prime, at least one of g or h is in (f). Say without loss of generality that $g \in (f)$. Then there is another polynomial p so that $g = fp$. Then we have

$$f = gh = fph,$$

so that $f(1 - ph) = 0$. Since f is a non-constant polynomial, we must have $1 - ph = 0$. Thus, we have that h is a unit, and so it is a constant polynomial. Thus we have shown that in any factorization of f, at least one of the terms is constant, so f is irreducible.

□

(1) implies (3)

Suppose f is irreducible. We wish to show that $k[x]/(f)$ is a field. So let a be a nonzero element of $k[x]/(f)$. By definition of quotient rings, there is some polynomial g so that $a = [g]$. Since $a \neq 0$, we must have that $g \notin (f)$, by definition of quotient rings. Since the elements of (f) are those polynomials divisible by f, we must have that f does not divide g.

Let d be the greatest common divisor of f and g. Since f is irreducible and d divides f, we have that either $d = 1$, or $d = cf$, for some nonzero constant c. However we also have that d divides g, say $g = pd$. Thus, if we had $d = cf$ then we would have

$$g = pd = pcf,$$

so that f divides g, a contradiction.

Thus, we must have that $d = 1$. By theorem 4.8 in Hungerford, there are polynomials u and v so that

$$1 = d = fu + gv.$$

Taking conjugacy classes, and recalling the definition of arithmetic of conjugacy classes we have that

$$[1] = [fu] + [g] \cdot [v].$$

Since $fu \in (f)$, we have that $[fu] = 0$, so that

$$[1] = [g] \cdot [v] = a \cdot [v].$$

Thus, we have shown that a has a multiplicative inverse. Since a was an arbitrary nonzero element of $k[x]/(f)$, this ring is a field, as desired.

□

Problem 1.3

(a) We'll present two solutions. One via the first isomorphism theorem, and the other by exhibiting homomorphisms in both directions.

First Isomorphism Theorem

We seek to get a surjective homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{C}$ with kernel equal to $(x^2 + x + 1)$, so that we may apply the first isomorphism theorem and conclude

$$\mathbb{R}[x]/(x^2 + x + 1) \cong \mathbb{C}$$

. To get φ, we just need a homomorphism $\mathbb{R} \to \mathbb{C}$ and an element $\beta \in \mathbb{C}$ so that $\beta = \varphi(x)$. We have a homomorphism $\mathbb{R} \to \mathbb{C}$ given by the standard inclusion. So now we just need a good choice for β.

To ensure that $\ker(\varphi) \supset (x^2 + x + 1)$, we must have

$$0 = \varphi(x^2 + x + 1) = \varphi(x)^2 + \varphi(x) + 1 = \beta^2 + \beta + 1,$$

that is, we must have that β is a root of x^2+x+1. Using the quadratic formula, we can pick

$$\beta = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

So we have our desired φ with kernel containing (x^2+x+1). Moreover, the quadratic formula shows that this polynomial has no roots in $\mathbb{R}$.

Since it is of degree 2, it is irreducible over $\mathbb{R}$. By problem 2, we have that (x^2+x+1) is maximal. Since $\varphi(1) = 1 \neq 0$, we have that $\ker(\varphi)$ is a proper ideal containing the maximal ideal (x^2+x+1), so we must have $(x^2+x+1) = \ker(\varphi)$.

Thus, all that remains to be shown is that φ is surjective. To show this it suffices to show that there is some $f \in \mathbb{R}[x]$ such that $\varphi(f) = i$, as then for any $a+bi \in \mathbb{C}$ we would have $\varphi(a+bf) = a+bi$, so surjectivity would hold.

To find a polynomial mapping to i, note that any polynomial $f \in \mathbb{R}[x]$ can be written in the form $f = q(x^2+x+1)+r$ with $\deg(r) \leq 1$. Then we note

$$\varphi(f) = \varphi(q) \cdot 0 + \varphi(r) = \varphi(r).$$

Thus, if there was some element f with $\varphi(f) = i$, then we could assume without loss of generality that f is of degree 1.

That is, we are searching for real numbers a, b so that

$$\begin{aligned} i &= \varphi(a+bx) \\ &= a + b\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) \\ &= a - \frac{b}{2} + ib\frac{\sqrt{3}}{2}. \end{aligned}$$

Equating real and imaginary parts, we see that this equality holds if and only if

$$\begin{aligned} 0 &= a - \frac{b}{2} \\ 1 &= b\frac{\sqrt{3}}{2} \end{aligned}$$

Solving this system of equations shows that

$$\varphi\left(\frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}i\right) = i,$$

and by previous reasoning φ is surjective, and the result holds.

□

Second solution, Defining inverse homomorphisms

Getting a homomorphism $\psi : A := \mathbb{R}[x]/(x^2 + x + 1) \to \mathbb{C}$ is the same as giving a homomorphism $\mathbb{R} \to \mathbb{C}$ and an element $\beta \in \mathbb{C}$ so that $\beta^2 + \beta + 1 = 0$, so that $\beta = \psi(x)$.

The homomorphism $\mathbb{R} \to \mathbb{C}$ is just the standard inclusion of rings.

To find the desired β, we use the quadratic formula, and get one choice of root as

$$\beta = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

Thus we get a map $\mathbb{R}[x]/(x^2 + x + 1) \to \mathbb{C}$ sending x to β.

To define an inverse homomorphism $\lambda : \mathbb{C} \to Z$, we recall that $\mathbb{C} \cong \mathbb{R}[i]/(i^2 + 1)$, so we seek a map $\mathbb{R} \to A$ and an element $\alpha \in A$ so that $\alpha^2 + 1 = 0$ (and we define $\lambda(i) = \alpha$).

We may use the above to solve for i in terms of β and get an equality in $\mathbb{C}$

$$i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\beta$$

This motivates defining $\lambda : \mathbb{C} \to A$ by

$$\lambda(i) = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}x =: \alpha$$

Compute

$$\alpha^2 + 1 = (\frac{1}{3} + \frac{4}{3}x + \frac{4}{3}x^2) + 1 = \frac{4}{3}(1 + x + x^2) = 0$$

because $1 + x + x^2 = 0$ in A, by definition of A.

To check that λ and ψ are inverses, we just need to check that $\lambda \circ \psi(x) = x$ and $\psi \circ \lambda(i) = i$.

We compute

$$\begin{aligned}\lambda \circ \psi(x) &= \lambda\left(\frac{-1}{2} + i\frac{\sqrt{3}}{2}\right) \\ &= \frac{-1}{2} + \frac{\sqrt{3}}{2}\lambda(i) \\ &= \frac{-1}{2} + \frac{\sqrt{3}}{2}\left(\frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}x\right) \\ &= \frac{-1}{2} + \frac{1}{2} + x \\ &= x.\end{aligned}$$

The computation that $\psi \circ \lambda(i) = i$ is similar.

□

(b) Let $A = \mathbb{F}_3[x, y]$, let $I \trianglelefteq A = (x^3, x^2y^2, y^3)$, and let $B = A/I$. We are trying to find the size of B.

First recall that the composite homomorphism $\mathbb{F}_3 \to A \to B$ naturally makes B and $\mathbb{F}_3$-vector space. I claim that B has a basis consisting of the conjugacy classes of the following 8 elements of A:

$$1, x, x^2, y, y^2, xy, x^2y, xy^2$$

Proving this claim will solve the problem, as then B will be exactly the sset of linear combinations of these 8 elements with coefficients in F_3, of which there are $3^8 = 6{,}561$. So now we prove the claim by showing these elements span, and that they are independent.

Spanning

To prove that they span, let $b = [f]$ in B, with $f \in A$. Recall that $f \in A$ may be written in the form

$$f = \sum_{i,j \geq 0} a_{i,j} x^i y^j$$

with all the $a_{i,j} \in \mathbb{F}_3$ and all but finitely many $a_{i,j} = 0$.

Note that if $i \geq 3$ then

$$a_{i,j}x^i y^j = x^3(a_{i,j}x^{i-3}y^j) \in I.$$

Thus, for any $i \geq 3$ we may define $g = f - a_{i,j}x^i y^j$, so that $b = [f] = [g]$, but g has a zero coefficient in front of the term $x^i y^j$.

Thus, we may assume without loss of generality that f has no monomial terms with the degree of x at least 3. Similarly, we may assume without loss of generality that f has no monomial terms with the degree of y at least 3, and has zero coefficient in front of x^2y^2. This means that f is a linear combination of the desired 8 elements, and so $[f]$ is a linear combination of the desired 8 conjugacy classes.

Independence

We must show that if the conjugacy class of

$$f = a_{0,0} + a_{1,0}x + a_{2,0}x^2 + a_{0,1}y + a_{0,2}y^2 + a_{1,1}xy + a_{2,1}x^2y + a_{1,2}xy^2$$

is zero in B, then all the $a_{i,j} = 0$.

If $[f] = 0$, then in A we must have

$$f = px^3 + qy^3 + rx^2y^2$$

for some $p, q, r \in A$. But then px^3 could only have nonzero monomials of degree at least 3 in x, qy^3 could only have nonzero monomials of degree at least 3 in y, and rx^2y^2 could only have nonzero monomials of degree at least 2 in x and y. None of these monomials include the monomials of f, so this equality could only hold if both sides of the desired equality are zero. By definition of the polynomial ring, this holds if and only if all the $a_{i,j} = 0$.

□

Problem 1.4

Part (a)

To show that the polynomial $f(x) = x^5 - x^2 + 1$ is irreducible over $\mathbb{Q}[x]$. It might be tempting to try and factor this polynomial over $\mathbb{C}$; however, one of the significant results we have seen in 403 is that there is no formula for factoring a quintic (5^{th} degree polynomial). Then, we'll need to be a little more sneaky. We cannot straight away use Eisenstein's Criterion, because all of our coefficients are 1. What can we do then? (pause for suspense)

Let's recall from last quarter that we have **Gauss's Lemma** which effectively says that is a polynomial is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$. To show that f is irreducible over $\mathbb{Z}$, we will evaluate at $x+1$ and take everything mod 2. Evaluating at $x+1$, we see that

$$f(x+1) = (x+1)^5 - (x+1)^2 + 1$$

$$= (x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1) - (x^2 + 2x + 1) + 1$$

$$= x^5 + 5x^4 + 10x^3 + 9x^2 + 3x + 1$$

Now, taking mod 2, we get $x^5+1x^4+0x^3+1x^2+1x+1 = x^5+x^4+x^2+x+1$. Call this new polynomial $g(x)$.

It is important to check that there is no root in our field $\mathbb{Z}/2\mathbb{Z}$ for this new polynomial; if there was, it would be reducible because there would be a linear factor.

$$g(0) = 1 \bmod 2$$

$$g(1) = 1 \bmod 2$$

Since the top degree is 5 and there are no linear factors, **IF** g was reducible, it would have to factor into a quadratic term and a cubic term. Moreover, since g is monic and it's constant term is 1, we express this as $g(x) = (x^3 + ax^2 + bx + 1)(x^2 + cx + 1)$. This tells us the following:

$$a + c = 1 \text{ (the coefficient of } x^2 \text{ is 1)}$$

$$1 + ac + b = 0$$

$$a + b + c + 1 = 1$$

$$b + c = 1$$

You can check that these relations are true by multiplying out the two factor polynomials. These four relations simultaneously being satisfied leads us to a contradiction, and so we have shown that g is irreducible in $\mathbb{Z}/2\mathbb{Z}$.

Therefore, $f(x)$ is irreducible in $\mathbb{Z}$, and by applying Gauss's Lemma, irreducible over $\mathbb{Q}$.

Note: I use the terminology "irreducible *over* $\mathbb{Q}$" and "irreducible *in* $\mathbb{Q}[x]$" interchangeably.

Part (b)

We aim to factor $f(x) = x^5 - x \in \mathbb{F}_5[x]$ into irreducibles. For this problem, we will need to recognize that $\mathbb{F}_5$ is the field with 5 elements, factor f with coefficients in this field, and demonstrate that each factor is irreducible in this field.

We begin with $x^5 - x = 0$. Pulling out an x term, we get $(x^4 - 1)x = 0$. Then, we concentrate on the 4^{th} degree term, which we can factor as $(x^2 + 1)(x^2 - 1)$. First we look at the $x^2 - 1$ term: $x^2 - 1 = (x + 1)(x - 1)$. Then, our current factorization is $(x^2 + 1)(x + 1)(x - 1)x$.

Because we are in $\mathbb{F}_5$, $2^2 + 1 = 0$, so $(x - 2)$ divides $(x^2 + 1)$. Using polynomial long division, we get that $(x - 2)(x - 3) = x^2 + 1$. Now, because we have factored the polynomial into linear terms, we have an irreducible factorization: $(x-2)(x-3))(x+1)(x-1)x$. Note that -1 is not an element of our field, so we need to recall that $-1 \cong 4$ in $\mathbb{F}_5$, and so our final factorization is $(x - 2)(x - 3))(x - 1)(x - 4)x$.

Problem 1.5

Part (a)

To find the solutions to $f(x) = x^3 - 3x + 2 = 0$, we will use **Cardano's Formula**.

Given $x^3 - 3x + 2 = 0$, we let $x = \frac{y+1}{y}$ so that this cubic becomes $y^6 + 2y^3 + 1 = (y^3)2 + 2(y^3) + 1 = 0$. Using the quadratic formula with

respect to the quantity y^3, we have that the roots of this quadratic are $y^3 = \frac{-2\pm\sqrt{4-4}}{2} = -1$. If this step is confusing, you can re-label y^3 as z in the above equation, and then it'll look more like a quadratic you're used to.

This gives

$$y = -1$$
$$y = e^{\frac{i\pi}{3}} = \frac{1}{2} \pm \frac{i\sqrt{3}}{2}$$

Now, we plug each y value into our equation $x = y + \frac{1}{y}$, and get the following:

For $y = -1$, $x = -2$.
For $y = e^{\frac{i\pi}{3}} = \frac{1}{2} + \frac{i\sqrt{3}}{2}$, we get that $x = 1$.
For $y = e^{\frac{i\pi}{3}} = \frac{1}{2} - \frac{i\sqrt{3}}{2}$, we get again that $x = 1$.
Then, the roots are $-2, 1$.

Part (b)

$x^3 + 3x - 36 = 0$. Which solutions are real? rational?

Following the calculation from part (a), we use the substitution that $x = y + \frac{1}{y}$. Then $x^3 + 3x - 36 = 0$ becomes $y^6 - 36y^3 - 1$, which we can re-write at $(y^3)^2 - 36y^3 - 1 = 0$. Then, we apply the quadratic formula to this equation, regarding y^3 as our variable. This gives us

$$y^3 = \frac{36 \pm \sqrt{36^2 + 4}}{2}$$
$$= 18 \pm \sqrt{325}$$
$$= 18 \pm 5\sqrt{13}$$

Thus, $y = \sqrt[3]{18 \pm 5\sqrt{13}}$. Now, we recall our initial substitution of $x = y + \frac{1}{y}$. In solving for x for each of our y values, we get that:
For $y = \sqrt[3]{18 + 5\sqrt{13}}$, $x = 3$.
For $y = \sqrt[3]{18 - 5\sqrt{13}}$, $x = \frac{-1}{2}i(\sqrt{39} - 3i)$.
For $y = \sqrt[3]{18 - 5\sqrt{13}}$, $x = \frac{1}{2}i(\sqrt{39} + 3i)$.

The only one of these roots that is rational is $x = 3$.