MATH-UA 349: Homework 1

James Pagan

Professor Kleiner

Contents

1 Problem 1

Proof. The number $7+\sqrt[3]{2}$ is a root of the polynomial $x^3-21x^2+147x-345=(x-7)^3-2$ in $\mathbb{Z}[x]$, as verified by the following computation:

$$\begin{aligned}\left((7+\sqrt[3]{2})-7\right)^3-2 &= (\sqrt[3]{2})^3-2\\ &= 2-2\\ &= 0.\end{aligned}$$

We conclude that $7+\sqrt[3]{2}$ is algebraic. $\square$

2 Problem 2

Proof. We begin by characterzing the subring R generated by $\alpha=\frac{i}{2}$. For all $n\in\mathbb{Z}_{\geq 0}$:

1. If $n\equiv 0 \pmod 4$, then $\alpha^n=\frac{1}{2^n}$.
2. If $n\equiv 1 \pmod 4$, then $\alpha^n=\frac{i}{2^n}$.
3. If $n\equiv 2 \pmod 4$, then $\alpha^n=-\frac{1}{2^n}$.
4. If $n\equiv 3 \pmod 4$, then $\alpha^n=-\frac{i}{2^n}$.

Claim 1. *If n is an odd integer and $b+ci$ is a Gaussian integer, then $\frac{a+bi}{2^n}\in R$*

Proof. Suppose that $n\equiv 1 \pmod 4$. Then

$$\frac{b+ci}{2^n}=\frac{b}{2^n}+\frac{ci}{2^n}=-2b\left(-\frac{1}{2^{n+1}}\right)+c\left(\frac{i}{2^n}\right)=-2b\alpha^{n+1}+b\alpha^n,$$

which lies in R by closure. Similarly, $n\equiv 3 \pmod 4$ yields that

$$\frac{b+ci}{2^n}=\frac{b}{2^n}+\frac{ci}{2^n}=2b\left(\frac{1}{2^{n+1}}\right)-c\left(-\frac{i}{2^n}\right)=2b\alpha^{n+1}-b\alpha^n,$$

which also lies in R.

We now examine closure. Let z be a complex number, and define $S_n=\left\{\frac{a+bi}{2^n}\mid a,b\in\mathbb{Z}\right\}$ for odd integers n; observe that $S_n\subset R$. It is a trivial exercise in geometry that the farthest z lie away from an element of S is "half of the main diagonal" of the smallest square — more formally,

$$\min\{|z-s|\mid s\in S_n\}\leq\frac{1}{2^n}\left(\frac{\sqrt{2}}{2}\right)=\frac{\sqrt{2}}{2^{n+1}}.$$

For all $\epsilon > 0$, the Archmedian Property ensures the existence of an integer N such that $\frac{\sqrt{2}}{2^{N+1}} < \epsilon$. Then $N < n$ implies

$$\min\{|z - s| \mid s_n \in S_n\} = \frac{\sqrt{2}}{2^{n+1}} < \frac{\sqrt{2}}{2^{N+1}} < \epsilon,$$

so there exists $s \in S_n \subset R$ such that $|z - s| < \epsilon$ for all ϵ. We conclude that the subring generated by α is dense in R. $\square$

3 Problem 3

Proof. We tackle Part (c) first:

Claim 2. *A number $m \in \mathbb{Z}_n$ is a unit if and only if* $\gcd(n, m) = 1$.

Proof. Realize the following:

$$\begin{aligned} m \text{ is a unit in } \mathbb{Z}_n &\iff ma \equiv 1 \pmod{n} \text{ for some } a \in \mathbb{Z} \\ &\iff n \mid (ma - 1) \text{ for some } a \in \mathbb{Z} \\ &\iff nb = ma - 1 \text{ for some } a, b \in \mathbb{Z} \\ &\iff nb - ma = 1 \text{ for some } a, b \in \mathbb{Z} \\ &\iff \gcd(n, m) = 1. \end{aligned}$$

The last step is a direct application of Bézout's Identity.

We deduce the following answers for each part:

(a) The units are 1, 5, 7, and 11.

(b) The units are 1, 3, 5, and 7.

(c) The units are all $m \in \mathbb{Z}_n$ such that $\gcd(n, m) = 1$,

as desired. $\square$

4 Problem 4

Proof. Performing polynomial divison yields that

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + 2x - 2)(x^2 + x + 1) + (7x + 7).$$

If $x^4+3x^3+x^2+7x+5$ divides x^2+x+1 in $\mathbb{Z}_n$, then $7x+7$ is must be the zero polynomial — which occurs if and only if $7 \equiv 0 \pmod{n}$. The answer is $\boxed{\text{all positive } n \text{ such that } 7 \mid n}$, **with a *potential* inclusion of $n = 1$ if deemed a valid modulus**. $\square$

5 Problem 5

5.1 Part (a)

Proof. Rather routine calculations verify that $F[[x]]$ is a ring. We must first prove that $(F[[x]], +)$ is an Abelian group:

1. **Closure**: It is clear that if $f, g \in F[[x]]$, then $f + g \in F[[x]]$.
2. **Associativity**: Since F is a field, $f, g, h \in F[x]$ implies
$$\big((f+g)+h\big)(k) = \big(f(k)+g(k)\big)+h(k) = f(k)+\big(g(k)+h(k)\big) = \big(f+(g+h)\big)(k)$$
for all $k \in \mathbb{Z}_{\geq 0}$; thus $(f+g)+h = f+(g+h)$
3. **Identity**: It is easy to verify that $f(k) = 0$ is an additive identity of $F[[x]]$.
4. **Invertability**: For $f \in F[[x]]$, define $-f$ by $(-f)(k) = -f(k)$. Then
$$(-f)(k)+f(k) = -f(k)+f(k) = 0 = f(k)-f(k) = f(k)+(-f)(k)$$
for all $k \in \mathbb{Z}_{\geq 0}$; thus $-f+f = 0$.
5. **Commutativity**: See that $(f+g)(k) = f(k)+g(k) = g(k)+f(k) = (g+f)(k)$ for all $k \in \mathbb{Z}_{\geq 0}$; hence $f = g$.

The multiplicative axioms are as follows:

6. **Closure**: It is clear that if $f, g \in F[[x]]$, then $fg \in F[[x]]$.
7. **Associativity**: Observe that for all $k \in F$,
$$\begin{aligned}\big((fg)h\big)(k) &= \sum_{i+j=k}(fg)(i)h(j) = \sum_{i+j=k}\left(\sum_{a+b=i} f(a)g(b)\right)g(j) \\ &= \sum_{a+b+c=k} f(a)g(b)h(c) \\ &= \sum_{i+j=k} f(i)\left(\sum_{a+b=j} g(a)h(b)\right) = \sum_{i+j=k} f(i)(gh)(j) \\ &= \big(f(gh)\big)(k).\end{aligned}$$

Therefore, $f(gh) = fg(h)$.

8. **Identity**: Let $g(k) = 0$ if $k \neq 0$ and $g(0) = 1$. Then for all $f \in F[[x]]$, and $k \in F$,

$$(fg)(k) = \sum_{i+j=k} f(i)g(j) = f(k) = \sum_{i+k=k} g(i)f(j) = (gf)(k).$$

   We conclude that $fg = gf = f$ for all $f \in F[[x]]$, so g is a multiplicative identity.

The two distributive axioms are as follows:

9. **Left Distributivity**: For all $f, g, h \in F[[x]]$ and $k \in F$, we have

$$\begin{aligned}\big(f(g+h)\big)(k) &= \sum_{i+j=k} f(i)(g+h)(j) \\ &= \sum_{i+j=k} f(i)g(j) + \sum_{i+k=k} f(i)h(j) \\ &= (fg)(k) + (fh)(k).\end{aligned}$$

   Thus $f(g+h) = fg + fh$.

10. **Right Distributivity**: For all $f, g, h \in F[[x]]$ and $k \in F$, we have

$$\begin{aligned}\big((f+g)h\big)(k) &= \sum_{i+j=k} (f+g)(i)h(j) \\ &= \sum_{i+j=k} f(i)h(j) + \sum_{i+k=k} g(i)h(j) \\ &= (fh)(k) + (gh)(k).\end{aligned}$$

   Thus $(f+g)h = fg + gh$.

Therefore, $F[[x]]$ is a ring. $\square$

5.2 Part (b)

Proof. Recall that the identity function of $F[[x]]$ is 1 when $k = 0$ and 0 otherwise. If $f \in F[[x]]$ has a multiplicative inverse g, then expanding these equations across all $k \geq 0$ yields

$$\begin{aligned}
1 &= f(0)g(0) \\
0 &= f(1)g(0) + f(0)g(1) \\
0 &= f(2)g(0) + f(1)g(1) + f(0)g(1) \\
&\vdots \\
0 &= f(k)g(0) + \cdots + f(0)g(k) \\
&\vdots
\end{aligned}$$

Solving for g along each equation, we obtain a recursive formula:

$$\begin{aligned}
g(0) &= \frac{1}{f(0)} \\
g(1) &= -\frac{f(1)g(0)}{f(0)} \\
g(2) &= -\frac{f(2)g(0) + f(1)g(1)}{f(0)} \\
&\vdots \\
g(k) &= \frac{f(k)g(0) + \cdots + f(1)g(k-1)}{f(0)} \\
&\vdots
\end{aligned}$$

A straightforward induction verifies that this formula produces a multiplicative inverse. Naturally, this recursion can occur if and only if $\boxed{f(0) \neq 0}$. □

6 Problem 6

Proof. Suppose $\mathfrak{a}$ is a nonzero ideal of the Gaussian integers, and let $a + bi \in \mathfrak{a}$ for $a, b \in \mathbb{Z}$, not both equal to zero. Then

$$(a + bi)(a - bi) = a^2 + b^2 \in \mathfrak{a};$$

noting that $a^2 + b^2 \in \mathbb{Z} + > 0$ completes the proof. □

7 Problem 7

Proof. Since the operations upon F are pointwise, verifying that Φ is a homomorphism is easy: for all $f, g \in R$ and $a \in F$, we have

$$\Phi(f+g)(a) = (f+g)(a) = f(a) + g(a) = \Phi(f)(a) + \Phi(g)(a)$$
$$\Phi(fg)(a) = (fg)(a) = f(a)g(a) = \Phi(f)(a)\Phi(g)(a).$$

As for the injectivity of Φ, suppose that $\Phi(f)(a) = f(a) = 0$ for all $a \in F$. Consider f in the algebraically closed extension of F: it has more roots than its degree, since the former is finite while the latter is infinite.

We conclude that f it must be the zero polynomial in this algebraically closed extension. Thus $f = 0$ in $F[x]$ as well, so Φ is injective. $\square$

8 Problem 8

Proof. Suppose $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ is an automorphism, and let $p = a_n x^n + \cdots + a_1 x + a_0$ be any polymonial of $\mathbb{Z}[x]$, where $a_n \neq 0$. Then

$$\phi(p) = \phi(a_n x^n + \cdots + a_1 x + a_0) = a_n \phi(x)^n + \cdots + a_1 \phi(x) + a_0 \phi(1).$$

Hence, ϕ is uniquely determined by $\phi(x)$ and $\phi(1)$. **We claim the answer is as follows**: ϕ is an automorphism if and only if ϕ is an endomorphism and $\phi(x)$ is an affine function with leading coefficent 1 or -1.

Let ϕ be an automorphism. We wish to demonstrate that $\phi(x)$ is an affine function with leading coefficent 1 or -1.

Claim 3. *$\phi(x)$ is an affine function with leading coefficent 1 or -1.*

Proof. Suppose for contradiction that $\deg \phi(x) > 1$; then the degree of all nonconstant polynomials in $\phi(\mathbb{Z}[x])$ is an integer multiple of $\phi(x)$, violating the injectivity of ϕ. Hence $\phi(x)$ is an affine function of the form $bx + c$ for some $b, c \in \mathbb{Z}$.

As noted in Claim 1, $b \neq 0$. Realize that the leading term of $\phi(p)$ is the leading term of $a_n \phi(x)^n$, which is

$$a_n b^n x^n.$$

We must have that $b^n = \pm 1$ in order for ϕ to be injective; thus $b = \pm 1$.

Now, let ϕ be an endomorphism of $\mathbb{Z}[x]$ such that $\phi(x) = bx + c$, where $b \in \{-1, 1\}$ and $c \in \mathbb{Z}$. We wish to demonstrate that ϕ is an automorphism.

Claim 4. *ϕ is injective.*

Proof. Let $p = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial in $\mathbb{Z}[x]$ of degree n such that $\phi(p) = 0$; suppose for contradiction that $n \geq 1$. Then the leading coefficent $\pm a_n x^n$ of $\phi(p)$ of must be zero; hence $a_n = 0$, which violates the degree of n.

Thus p must be constant. Since $\phi(p) = p$ for all constant polynomials (a consequence of the fact $\phi(1) = 1$), we must have $p = 0$; thus $\operatorname{Ker} \phi = 0$, so ϕ is injective.

Claim 5. *ϕ is surjective.*

Proof. We prove that for all $p \in \mathbb{Z}[x]$, there exists $s \in \mathbb{Z}[x]$ such that $\phi(s) = p$ by induction on the degree of p. For the base clase: clearly if p is constant, then $\phi(p) = p$.

For the inductive step: suppose that all polyomials of degree $n - 1$ or smaller lie within $\phi(\mathbb{Z}[x])$, and let $p = a_n x^n + \cdots + a_n x^n + a_0$, where $a_n \neq 0$. Then

$$p \pm a_n (bx + c)^n$$

is of degree $n - 1$ or smaller, where $\pm$ cancels out the leading coefficent of p, sign beng dependent on b and the parity of n. Our inductive hypothesis guarantees the existence of a polynomial $s \in \mathbb{Z}[x]$ such that

$$\phi(s) = p \pm a_n (bx + c)^n.$$

Hence, we deduce that

$$\phi(s \mp a_n x^n) = \phi(s) \mp a_n \phi(x)^n = p \pm a_n (bx + c)^n \mp a_n (bx + c)^n = p.$$

Thus all polynomials of degree n lie within $\phi(\mathbb{Z}[x])$. This completes the induction.

We conclude that ϕ is an automorphism, which implies the required result. $\square$

9 Problem 9

9.1 Part (a)

Proof. We claim that $\boxed{\mathbb{Z}[i]\,/\,(2+i)\;\cong\;\mathbb{Z}_5}$, by the isomorphism: $\phi(a+bi) = a+3b \pmod 5$. Verifying that ϕ is a homomorphism is straightforward: if $a+bi$ and $c+di$ are Gaussian integers,

$$\begin{aligned}
\phi(a+bi)+\phi(c+di) &= a+3b+c+3d \pmod 5 \\
&\equiv (a+c)+3(b+d) \pmod 5 \\
&= \phi\big(a+c+i(b+d)\big) \\
&= \phi\big((a+bi)+(c+di)\big).
\end{aligned}$$

As per the multiplicative condition,

$$\begin{aligned}
\phi(a+bi)\phi(c+di) &= (a+3b)(c+3d) \pmod 5 \\
&\equiv ac+3(ad+bc)+9bd \pmod 5 \\
&\equiv (ac-bd)+3(ad+bc) \pmod 5 \\
&= \phi\big((ac-bd)+i(ad+bc)\big) \\
&= \phi\big((a+bi)(c+di)\big).
\end{aligned}$$

It is clear that $\phi(1) = 1$, so ϕ is a homomorphism; it is surjective, as $\phi(n) = n$ for $n \in \{0,\ldots,4\}$. We need only demonstrate that ϕ is injective. Suppose that $\phi(a+bi) = 0$, which implies $a+3b \equiv 0 \pmod 5$; we wish to demonstrate that $a+bi = (2-i)z$ for a Gaussian integer z. See that

$$2a+b \equiv 2(a+3b) \cong 0 \pmod 5 \qquad \text{and} \qquad -a+2b = -1(a+3b) \cong 0 \pmod 5.$$

Then let us divide $a+bi$ by $2-i$: define

$$z = \frac{a+bi}{2-i} = \frac{(a+bi)(2-i)}{2^2-i^2} = \frac{(2a+b)+(-a+2b)i}{5}.$$

Since both the real and imaginary components of this fraction are divisible by 5, we deduce that z is a Gaussian integer. Then $a+bi$ is 0 modulo $(2+i)$, so $\operatorname{Ker}\phi = 0$. We conclude that ϕ is injective, which implies the desired isomorphism. □

9.2 Part (b)

Proof. We claim that $\boxed{\mathbb{Z}[x]\,/\,(x^2+3,5) \cong \mathbb{F}_{25}}$, the field with 25 elements; since all finite fields of the same order are isomorphic, we need only demonstrate that $\mathbb{Z}[x]\,/\,(x^2+3,5)$ is a field with 25 elements.

Our proof will utilize the equivalent notation $\mathbb{Z}[x]\,/\,(x^2+3,5) = \mathbb{Z}_5[x]\,/\,(x^2+3)$.

Naturally, the elements of $\mathbb{Z}_5[x]\,/\,(x^2+3)$ are the 25 polynomials of the form $ax+b$, for $a, b \in \{0, \dots, 4\}$; this is because if $\deg p \geq 2$, there exist polynomials q and r with integer coefficents (ensured since x^2+3 is monic) such that

$$p = (x^2+3)q + r$$

where r is zero or $\deg r < 2$. Hence $p \equiv r \pmod{x^2+3}$, and r is of the aforementioned form $ax+b$. Hence the commutative ring $\mathbb{Z}_5[x]\,/\,(x^2+5)$ has order 25.

Claim 6. *Every nonzero polynomial in* $\mathbb{Z}_5[x]\,/\,(x^2+3)$ *is a multiplicative unit.*

Proof. The nonzero constant polynomials $1, 2, 3, 4$ are units by Problem 3. Now, consider ax for $a \neq 0$; since $x^2 \equiv 2 \pmod{x^2+3}$, we have that

$$(ax)(3a^{-1}x) \equiv (aa^{-1})3x^2 \equiv 3x^2 \equiv 6 \equiv 1 \pmod{x^2+3}.$$

where a^{-1} denotes the modular inverse of a; thus ax is a unit. Now, consider $ax+b$ for $a, b \neq 0$; define n as the multiplicative inverse of $2-(a^{-1}b)^2$ (since squares modulo 5 are congruent to 0, 1, or 4, this quantity is never zero and is thus a unit). Then

$$\begin{aligned}(ax+b)\Big(n(a^{-1}x - a^{-2}b)\Big) &\equiv n(ax+b)(a^{-1}x - a^{-2}b) \pmod{x^2+3} \\ &\equiv n(x^2 - a^{-2}b^2) \pmod{x^2+3} \\ &\equiv n(2-(a^{-1}b)^2) \pmod{x^2+3} \\ &\equiv 1 \pmod{x^2+3}.\end{aligned}$$

Thus every nonzero polynomial in $\mathbb{Z}_5[x]\,/\,(x^2+3)$ is a unit.

We conclude that $\mathbb{Z}_5[x]\,/\,(x^2+3)$ is a field with 25 elements, so it is isomorphic to $\mathbb{F}_{25}$. □

10 Problem 10

Proof. Suppose for contradiction that $\phi : \mathbb{Z}[x]\,/\,(2x^2+7) \to \mathbb{Z}[x]\,/\,(x^2+7)$ is an isomorphism. Observe that $(2x^2+7)$ and (x^2+7) are prime ideals of $\mathbb{Z}[x]$, so both quotient rings are integral domains. Since $\phi(n) = n$ for all constant polynomials n, we have

$$\begin{aligned}\phi(0) = 0 &\implies \phi(x^2+7) = 2x^2+7 \\ &\implies \phi(x^2) + \phi(7) = 2x^2+7 \\ &\implies \phi(x)^2 + 7 = 2x^2+7.\end{aligned}$$

We deduce that $\phi(x)^2 = 2x^2$. Let $\phi(x) = ax + b$ for integers a, b; then

$$2x^2 = (ax+b)^2 = a^2x^2 + 2abx + b^2.$$

We must have that $2abx = 0$; thus $a = 0$ or $b = 0$. If $a = 0$, then $\phi(x)$ is a constant; the image of ϕ consists of constant polynomials, violating the injectivity of ϕ. Thus $b = 0$ and $\phi(x) = ax$. This leaves us with the equation

$$2x^2 = a^2x^2 \implies (2 - a^2)x^2 = 0.$$

Then $2 - a^2 = 0$; however, no integer a satisfies this equation. Any possibility of the value $\phi(x)$ leads to a contradiction, so $\boxed{\text{the rings are not isomorphic}}$. $\square$