MATH-UA 349: Homework 3

James Pagan, February 2024

Professor Kleiner

Contents

1 Problem 1

Proof. The following six proofs demonstrate that the *first* proofs imply the *second*:

1. **Units**: Suppose that u has a multiplicative inverse v. Then $1 = uv \in (v)$, so for all $a \in R$, we obtain $a = a1 \in (v)$. Thus $(u) = R$.

   Suppose that $(u) = R$. Then $1 \in (u)$, so there exists v such that $uv = 1$. Thus u has a multiplicative inverse.

2. **Divisors**: Suppose that $b = aq$. Then for all $bx \in (b)$, we have that $bx = aqx \in (a)$ — hence $(b) \subseteq (a)$.

   Suppose that $(b) \subseteq (a)$. Then $b \in (a)$, so there exists q such that $b = aq$.

3. **Proper Divisors**: Suppose that $b = aq$ and neither a nor q are units. Then $(b) \subseteq (a)$. If we suppose for contradiction that $(b) = (a)$, then there exists x such that $bx = a$. Hence $a = axq$; since R is an integral domain, q is a unit. Thus we conclude $(b) \subset (a)$.

   Suppose that $(b) \subset (a)$. Then $b = aq$ for some q; if q was a unit, then $a = bq^{-1}$ and $(b) = (a)$. Thus u is not a unit.

4. **Associates**: Suppose that $a = ub$ for some unit u. Then for all $ax \in (a)$, we have $ax = bux \in (b)$ — and for all $bx \in (b)$, we have $bx = au^{-1}x \in (a)$. Thus $(a) = (b)$.

   Suppose that $(a) = (b)$. Then there exists u, v such that $a = ub$ and $b = va$, so $a = uva$. Since R is an integral domain, this implies that u is a unit.

5. **Irreducible Elements**: The proof follows from Parts (1) and (2):

$$\begin{aligned} a \text{ is a nonunit} &\iff (a) \subset R \\ a \text{ has no proper divisors} &\iff \text{there does not exist } (b) \text{ such that } (a) \subset (b) \subset R. \end{aligned}$$

6. **Prime Elements**: Using Part (2), we find that

$$\begin{aligned} p \mid ab \text{ implies } p \mid a \text{ or } p \mid b &\iff (ab) \subseteq (p) \text{ implies } (a) \subseteq (p) \text{ or } (b) \subseteq (p) \\ &\iff ab \in (p) \text{ implies } a \in (p) \text{ or } b \in (p), \end{aligned}$$

   as desired.

This completes the proof. $\square$

2 Problem 2

Part (a)

Proof. Since $R \subseteq \mathbb{Z}[i]$ is a subring, the units of R are units of $\mathbb{Z}_i$ — namely, they must be among 1, i, -1, and $-i$. It is clear that only $\boxed{1 \text{ and } -1}$ are elements of R and are both units. $\square$

Part (b)

Proof. Realize that elements $a + bi\sqrt{5} \in R$ have norm squared

$$\left|a + bi\sqrt{5}\right|^2 = a^2 + 5b^2.$$

Thus if an element $x \in R$ factors into nonunits $y, z \in R$, then $|x|^2$ factors into two numbers of the form $a^2 + 5b^2 > 1$ for integers a, b. The absolute values of the required elements are as follows:

1. $|2|^2 = 4$.
2. $|3|^2 = 9$.
3. $\left|1 + i\sqrt{5}\right|^2 = 6$.
4. $\left|1 - i\sqrt{5}\right|^2 = 6$.

By listing integers of the form $a^2 + 5b^2$, we obtain that none of these factor as desired. Hence they are all irreducible. $\square$

Part (c)

Proof. Observe that the element $6 \in R$ factors into two products of irreducible elements:

$$2 \times 3 \;=\; 6 \;=\; (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

Neither of the terms on the right-hand side are adjoints with the left-hand side, since the units of R are 1 and -1. Hence R is not a Unique Factorization Domain. $\square$

3 Problem 3

$F[x_1, x_2]$ is not a principal ideal domain because the ideal

$$(x_1, x_2)$$

is not principal: otherwise since $(x_1, x_2) \neq R$ there would exist a nonunit generator that divides the polynomials x_1 and x_2, but both such elements are irreducible.

4 Problem 4

Part (a)

Proof. Suppose that $\mathfrak{p}$ is a prime ideal of R, and define $\phi : R \to R/\mathfrak{p}$ by $\phi(a) = a + \mathfrak{p}$. Since the kernel of ϕ is $\mathfrak{p}$, we have that

$$\phi(ab) = 0 \implies ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p} \implies \phi(a) = 0 \text{ or } \phi(b) = 0.$$

Conversely, suppose that $R/\mathfrak{p}$ is an integral domain. Then

$$ab \in \mathfrak{p} \implies \phi(ab) = 0 \implies \phi(a) = 0 \text{ or } \phi(b) = 0 \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

This completes the proof. $\square$

Part (b)

Proof. Using the result from Problem 1, we have

$$\begin{aligned}
(p) \neq (0) \text{ is prime} &\iff p \neq (0),\ p \neq R, \text{ and } ab \in (p) \text{ implies } a \in (p) \text{ or } b \in (p) \\
&\iff p \neq 0 \text{ is not a unit, and } p \mid ab \text{ implies } p \mid a \text{ or } p \mid b \\
&\iff p \text{ is a prime element,}
\end{aligned}$$

as required. $\square$

5 Problem 5

We use elementary Number Theory. It is clear that $\gcd(ab, a+b) = 1$: using the fact that $\gcd(w, y) = 1$ implies that $\gcd(x, y) = \gcd(xw, y)$ for all x, we have

$$\begin{aligned} \gcd(a, b) = 1 &\implies \gcd(a, a+b) = 1 \text{ and } \gcd(b, a+b) = 1 \\ &\implies \gcd(ab, a+b) = 1. \end{aligned}$$

We may thus use Euler's theorem on $a+b$ modulo ab. Let $\varphi(a+b) = n$, where φ is Euler's totient function. Then

$$\begin{aligned} a^n + b^n &\equiv a^n + \tbinom{n}{1} a^{n-1} b + \cdots + \tbinom{n}{n-1} a b^{n-1} \pmod{ab} \\ &\equiv (a+b)^n \pmod{ab} \\ &\equiv 1 \pmod{ab}. \end{aligned}$$

This completes the proof.

6 Problem 6

Part (a)

Proof. Let P / Q be a rational function in $\mathbb{C}(x)$. We use strong induction on the degree of Q; clearly the cases where $\deg Q = 1$ or Q is constant are trivial.

Inductive Step: Let the hypothesis be true for $\deg Q \leq n-1$, and consider when $\deg Q = n$. There exist polynomials A, R such htat

$$\frac{P}{Q} = \frac{AQ + R}{Q} = A + \frac{R}{Q},$$

where $\deg R < \deg Q$ or R is zero. Let $Q = c(x - q_1) \cdots (x - q_n)$. Again by polynomial division, there exists a polynomials B and a constant d such that

$$\frac{R}{Q} = \frac{B(x - q_1) + d}{Q} = \frac{B}{c(x - q_2) \cdots (x - q_n)} + \frac{d}{q}.$$

Our inductive hypothesis applies to $B / c(x - q_2) \cdots (x - q_n)$; we need only demonstrate that d / Q is of the required form. If $q_1 = \cdots = q_n$, we are done; otherwise, the GCD of all $(x - q_i)$ is 1, so Bezout's Identity guarantees that there exist constants $a_1, \ldots, a_n$ such that

$$a_1(x - q_1) + \cdots + a_n(x - q_n) = 1.$$

Therefore, we have

$$\frac{d}{q} = \frac{da_1(x-q_1) + \cdots + da_n(x-q_n)}{q}.$$

Expanding this polynomial out, we get a sum of polynomials with denominator degree $n-1$; hence the inductive hypothesis applies. We conclude that $P\,/\,Q$ is expressable in the given form. $\square$

Part (b)

Proof. Since $\{1, x, x^2, x^3, \ldots\}$ is a basis of $\mathbb{C}[x]$, a basis of $\mathbb{C}(x)$ is

$$\boxed{1, x, x^2, x^3, \ldots \text{ and every term } \frac{1}{(x-a)^i} \text{ for } a \in \mathbb{C} \text{ and } i \in \mathbb{Z}_{>0}}.$$

$\square$

7 Problem 7

Note: My solutions for these problems are parts, differing only at the final equation

Part (a)

Proof. Using the norm $\|a + b\omega\| = a^2 + ab + b^2$, we will divide $a + b\omega$ by $c + d\omega$. It is easy to deduce that there exist rationals r, s such that

$$\frac{a + b\omega}{c + d\omega} = r + s\omega.$$

Approximate r and s by integers: namely define $n, m \in \mathbb{Z}$ such that $|r - n| \leq 1$ and $|s - m| \leq 1$. Then we can express the above as

$$r + s\omega = (n + m\omega) + (r - n) + (s - m)\omega.$$

Expanding this out, we obtain a rather messy equation:

$$a + bi \quad = \quad (n + n\omega)(c + d\omega) \quad + \quad \big((r-n) + (s-m)\omega\big)(c + d\omega).$$

All that remains to be proven is that the right-most term has a norm less than $c + di$, which is equivalent to showing that $(r - n) + i(s - m)\sqrt{2}$ has a norm less than one:

$$\|(r-n) + (s-m)\omega\| = (r-n)^2 + (r-n)(s-m) + (s-m)^2 \leq \frac{3}{4} < 1.$$

This completes the proof. $\square$

Part (b)

Proof. Using the norm $\left\|a + bi\sqrt{2}\right\| = a^2 + 2b^2$, we will divide $a + bi\sqrt{2}$ by $c + di\sqrt{2}$. It is easy to deduce that there exist rationals r, s such that

$$\frac{a + bi\sqrt{2}}{c + di\sqrt{2}} = r + si\sqrt{2}.$$

Approximate r and s by integers: namely define $n, m \in \mathbb{Z}$ such that $|r - n| \leq 1$ and $|s - m| \leq 1$. Then we can express the above as

$$r + si\sqrt{2} = (n + mi\sqrt{2}) \;+\; (r - n) + i(s - m)\sqrt{2}.$$

Expanding this out, we obtain a rather messy equation:

$$a + bi \quad = \quad (n + ni\sqrt{2})(c + di\sqrt{2}) \quad + \quad \big((r - n) + i(s - m)\sqrt{2}\big)(c + di\sqrt{2}).$$

All that remains to be proven is that the right-most term has a norm less than $c + di$, which is equivalent to showing that $(r - n) + i(s - m)\sqrt{2}$ has a norm less than one:

$$\left\|(r - n) + i(s - m)\sqrt{2}\right\| = (r - n)^2 + 2(s - m)^2 \leq \frac{1}{4} + 2\left(\frac{1}{4}\right) = \frac{3}{4} < 1.$$

This completes the proof. □

8 Problem 8

Let $\psi_1 : \mathbb{Z}[x] \to \mathbb{F}_{c_1}[x]$ and $\psi_2 : \mathbb{Z}[x] \to \mathbb{F}_{c_2}[x]$ be the natural homomorphisms. It is clear by the properties of modular arithmetic that $\psi_1 \circ \psi_2 = \psi_2 \circ \psi_1$: hence we have

$$\phi_2 \circ \phi_1(f_1 f_2) = \phi_2(\phi_1(f_1))\phi_1(\phi_2(f_2)) = 0,$$

so $c_1 c_2$ divides every coefficent of $f_1 f_2$. It is easy to see that if c contains a prime power which is bigger (or different) than one in $c_1 c_2$, then we attain a contradiction divvying up the prime power between f_1 and f_2 in $\mathbb{F}_{p^n}$.