MATH-UA 349: Homework 4

James Pagan, February 2024

Professor Kleiner

Contents

1 Problem 1

Proof. For the first polynomial, we have that

$$\begin{aligned} x^9 - x &= x(x^8 + 1) \\ &= x(x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 28x^2 + 8x + 1) \\ &= \boxed{x(x+1)^8}. \end{aligned}$$

The second polynomial is a similar story:

$$\begin{aligned} x^9 - 1 &= (x^3 - 1)(x^6 + x^3 + 1) \\ &= \boxed{(x+1)(x^2 + x + 1)(x^6 + x^3 + 1)}. \end{aligned}$$

One can verify that $x^6 + x^3 + 1$ is irreducible through the Sieve of Eratosthenes. □

2 Problem 2

Proof. Let $p(x) = x^4 + 6x^3 + 9x + 3$. We claim that $\boxed{p \text{ generates a maximal ideal}}$ in $\mathbb{Q}[x]$.

Lemma 1. *p is irreducible in $\mathbb{Q}[x]$.*

Proof. By the Rational Root Theorem, the only possible rational roots of $p(x)$ are -3, -1, 1, and 3. A quick check verifies that none of these are roots of p — hence it has no rational roots.

By the Factor Theorem, this ensures that no polynomial of the form $(x - q)$ for $q \in \mathbb{Q}$ divides p. Since these are the prime elements of the Euclidean domain $\mathbb{Q}[x]$, we conclude that p is irreducible.

Hence p is a prime element of $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a principal ideal domain, the ideal (p) must be maximal. □

3 Problem 3

Proof. We claim that the argument of π in polar coordinates is a muliple of $\frac{\pi}{4}$.

Suppose that $\pi = a + bi = re^{i\theta}$ is a Gauss prime such that $\overline{\pi}$ and π are associates — that is, $\overline{\pi} = u\pi$ for some $u \in \{1, i, -1, -i\}$. This yields the equation

$$re^{-i\theta} = re^{i\left(\theta + \frac{n\pi}{2}\right)}$$

for some $n \in \mathbb{Z}$; equivalently, we find $-\theta = \theta + \frac{n\pi}{2}$; the solutions to this equation are of the form $\frac{4k\pi}{8}$ for $k \in \{0, \ldots, 7\}$. Hence in rectangular form, the Gauss prime π has three forms:

1. π is purely real.
2. π is purely imaginary.
3. π is on a diagonal of the complex plane — that is, π is of the form $a + ai$, $a - ai$, $-a - ai$, or $-a + ai$ for some $a \in \mathbb{Z}$.

If π is purely real, it must be a prime congruent to 3 (mod 4). If π is purely imaginary, then its associate is of the previous form. If π lies on a diagonal, it is quite clear that π is $1 + i$ or one of its associates; hence $\pi \cdot \overline{\pi} = 2$. □

4 Problem 4

Case 1: If $p \equiv 3 \pmod 4$, then p is a Gaussian prime; hence $\mathbb{Z}[i] \,/\, (p)$ is a field with p^2 elements: they have the form $a+bi$ for $a, b \in \{0, \ldots, p-1\}$. We conclude that $\boxed{\mathbb{Z}[i] \,/\, (p) \;\cong\; \mathbb{F}_{p^2}}$.

Case 2: If $p \equiv 1 \pmod 4$, then $x^2 + 1$ is not irreducible in $\mathbb{Z}_p$; hence there exist $a, b \in \mathbb{Z}_p$ such that $(x^2 + 1) = (x + a)(x + b)$. As elaborated in Case 3, we have $a \neq b$. Hence we claim $\boxed{\mathbb{Z}[i] \,/\, (p) \;\cong\; \mathbb{Z}_p[x] \,/\, (x + a) \times \mathbb{Z}_p[x] \,/\, (x + b)}$. It is easy to see that

$$\begin{aligned} \mathbb{Z}[i] \,/\, (p) &\cong \big(\mathbb{Z}[x] \,/\, (x^2 + 1)\big) \,/\, (p) \\ &= \big(\mathbb{Z}[x] \,/\, (p)\big) \,/\, (x^2 + 1) \\ &\cong \mathbb{Z}_p[x] \,/\, (x^2 + 1) \\ &= \mathbb{Z}_p[x] \,/\, (x + a)(x + b). \end{aligned}$$

Since $\mathbb{Z}_p[x]$ is a Euclidean domain, the ideals $(x + a)$ and $(x + b)$ are maximal. Hence $(x + a) + (x + b) = \mathbb{Z}_p[x]$; we conclude by the Chinese Remainder Theorem the desired

$$\mathbb{Z}[i] \,/\, (p) \;\cong\; \mathbb{Z}_p[x] \,/\, (x + a)(x + b) \;\cong\; \mathbb{Z}_p[x] \,/\, (x + a) \times \mathbb{Z}_p[x] \,/\, (x + b).$$

Case 3: We claim $p = 2$ if and only if $a = b$. This is because if $(x + a)^2 = (x + 1)$, then $a^2 = 1$ and $a + a = 0$; thus

$$0 = 0(a) = (a + a)a = a^2 + a^2 = 2.$$

The other direction is trivial since $(x+1)^2 = x^2+1$ in $\mathbb{Z}_2$. Similar logic to the above yields that $\boxed{\mathbb{Z}[i] \,/\, (2) \;\cong\; \mathbb{Z}_2[x] \,/\, (x + 1)^2}$.

5 Problem 5

Proof. Let $n = p_1^{e_1} \cdots p_n^{e_n} q_1^{f_1} \cdots q_m^{f_m}$, where the p_i are prime integers congruent to $1 \pmod 4$ and the q_i are prime integers congruent to $3 \pmod 4$. We claim that

$$\boxed{n \text{ is a sum of squares if and only if } f_1, \ldots, f_n \text{ are even}}.$$

First, we demonstrate that if $f_1, \ldots, f_n$ are even, then n is a sum of two squares.

Lemma 2 (Brahmagupta-Diophantus Identity)**.** *Let $j, k \in \mathbb{Z}$ be sums of two squares. Then jk is a sum of two squares.*

Proof. This follows from the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

for integers a, b, c, and d. □

Since f_i is even for all i, each $q_i^{f_i}$ is a square; thus the product $q_1^{f_1} \cdots q_m^{f_m}$ is a sum of squares by Lemma 2. By Fermat's Two-Square Theorem, all the primes p_i are a sum of squares. Thus their product $p_1^{e_1} \cdots p_n^{e_n}$ is a sum of squares. Multiplying the p_i and q_i together, we obtain that n is a sum of two squares.

Next, we demonstrate that if n is a sum of two squares, then f_i are even. Suppose for contradiction that $f_{k_1}, \cdots f_{k_j}$ are odd; then

$$q_{k_1} \cdots q_{k_j} \mid n.$$

Expressing n as a product of Gaussian primes, it is easy to attain that n cannot be a square since $q_{k_1}, \ldots, q_{k_j}$ are Gaussian primes, using Euclid's Lemma. □

6 Problem 6

6.1 Part (a)

Proof. Let M be a simple R-module. Since $(M, +)$ is a simple Abelian group, it must be isomorphic to a finite cyclic group of prime order — say C_p. Hence M is generated by one element x.

Lemma 3. *M is isomorphic to a quotient of R.*

Proof. Define a mapping $f : R \to M$ by the rule $f(a) = ax$. This is an R-module homomorphism, since $a, b \in R$ implies

$$f(a+b) = (a+b)x = ax + bx = f(a) + f(b)$$
$$f(ab) = abx = a(bx) = af(b).$$

ϕ is surjective, since $f(1+\cdots+1) = x+\cdots+x$, which generates the entirety of M. Thus if we let $\mathfrak{m} = \operatorname{Ker} f$, the First Isomorphism Theorem yields the desired $R / \mathfrak{m} \cong M$.

Because the ring $R / \mathfrak{m}$ has prime order, it contains no proper nonzero ideals. Thus the quotient is a field, so $\mathfrak{m}$ is maximal. This completes the proof. □

6.2 Part (b)

Proof. Suppose $\phi : V \to V'$ is a homomorphism of simple R-modules. Then V and V' must be finite, and the submodules $\operatorname{Ker} \phi \subseteq V$ and $\operatorname{Im} \phi \subseteq V'$ must be either 0 or the module itself.

1. If $\operatorname{Ker} \phi = V$: then ϕ is the zero homomorphism.
2. If $\operatorname{Ker} \phi = 0$: then $V \cong \operatorname{Im} \phi$ by the First Isomorphism Theorem. Thus $\operatorname{Im} \phi$ is a nonzero submodule of V', so $\operatorname{Im} \phi = V'$. We conclude that $V \cong V'$.

This yields the desired result. □

7 Problem 7

7.1 Part (a)

For convenience, we denote by x_i for each $i \in \{1, \ldots, n\}$ as the canonical basis $(\delta_{ik})_{k=1}^n$ for each $i \in \{1, \ldots, n\}$, where δ is the Kronecker delta. Then the list

$$\phi(x_1), \ldots, \phi(x_n) \quad \in \quad R^n$$

is linearly independent and has length n, so it must constitute a basis of R^n. Thus for $r_1, \ldots, r_n \in R$,

$$r_1\phi(x_1) + \cdots + r_n\phi(x_n) = 0 \qquad \Longrightarrow \qquad r_1 = \cdots = r_n = 0.$$

Since the right-hand side equals $\phi(r_1x_1 + \cdots + r_nx_n)$, we conclude that ϕ has kernel 0 — thus ϕ is an isomorphism.

7.2 Part (b)

$\boxed{\text{No}}$. Consider the ring $\mathbb{Z}[x]$ and the prime ideals $(2) \subset (2, x)$. These ideals are free $\mathbb{Z}[x]$-modules; hence let $\phi : (2, x) \to (2, x)$ be the $\mathbb{Z}[x]$-module homommorphism defined by $\phi(y) = 2y$. Two observations:

1. **Injectivity**: Holds. Clearly $\operatorname{Ker} \phi = 0$, since $\mathbb{Z}[x]$ is an integral domain.
2. **Surjectivity**: Fails. ϕ maps the entirety of $(2, x)$ to (2).

Since ϕ is not an automorphism, it constitutes a counterexample to the stated claim.