MAT 4233 — Problem Set 4

Due Thursday 19 November 2026, at the start of the Q&A session.

This set covers the six meetings of 29 October through 17 November: rings, subrings, units and zero divisors, integral domains and fields (Li–Zhao §4.1–§4.2), ring homomorphisms, ideals and quotient rings (§4.5), principal, prime and maximal ideals (§4.7), irreducibles, primes, unique factorization domains and principal ideal domains (§5.1–§5.2), Euclidean domains (§5.3), and multiplicative norms, the Gaussian integers and Fermat's two squares theorem (§5.5, with Conrad's notes). Problem 1 was Problem 5 of Problem Set 3, unchanged; if you have already written it, it counts here.

Maximum six pages. Each problem is scored on *completeness* alone, not on correctness: **2** for a nominally complete solution, **1** for a clearly partial one, **0** for nothing submitted or for filler with no substance. Any submission containing non-human-readable content, stray characters, or unproofread AI output scores 0 for that item.

Sources. AI assistance, solution keys, collaboration and the internet are all permitted, without restriction. Include one line naming what you used. Note that at the Q&A session we name the problem you are to explain; you do not choose, so be ready on every problem on this set.

Notation. We follow Li–Zhao: a *unital ring* has a unity $1 \neq 0$, $U(R)$ is its group of units, and an *integral domain* is a commutative unital ring with no zero divisors. A ring homomorphism φ satisfies $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$; it need not send 1 to 1. $(a_1, \dots, a_k)$ is the ideal generated by $a_1, \dots, a_k$, and R/I the quotient ring. For an integer d that is not a perfect square, $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$, a subring of $\mathbb{C}$, with norm $N(a + b\sqrt{d}) = a^2 - db^2$; in particular $N(a + bi) = a^2 + b^2$ on $\mathbb{Z}[i]$. You may use that N is multiplicative, $N(\alpha\beta) = N(\alpha)N(\beta)$. A later problem may quote an earlier one.

Problem 1 (Rings, units and zero divisors)

A nonzero element a of a commutative ring R is a *zero divisor* if $ab = 0$ for some nonzero $b \in R$.

1. Show that $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{R}$ containing 1. Show that $1 + \sqrt{2}$ is a unit of $\mathbb{Z}[\sqrt{2}]$, and that its powers $(1 + \sqrt{2})^k$, $k \geq 1$, are all distinct. Conclude that $U(\mathbb{Z}[\sqrt{2}])$ is infinite.
2. Let R be a commutative ring with unity $1 \neq 0$.
   a. Prove that a unit of R is never a zero divisor.
   b. Now suppose R is also *finite*. Prove that every nonzero element of R is either a unit or a zero divisor. (*For $a \neq 0$, consider the map $R \to R$, $x \mapsto ax$. When is it injective?*)
3. Find all the units of the ring $\mathbb{Z}_4 \times \mathbb{Z}_6$ (with componentwise operations), and use part 2 to count its zero divisors without listing them.

Problem 2 (Ring homomorphisms, ideals and quotient rings)

1. Let $\varphi\colon R \to R'$ be a ring homomorphism. Prove that $\ker\varphi$ is an ideal of R. Deduce that if R is a field, then every ring homomorphism $\varphi\colon R \to R'$ is either injective or identically zero.
2. Define $\varphi\colon \mathbb{Z}[i] \to \mathbb{Z}_5$ by $\varphi(a+bi) := [a+2b]_5$. Show that φ is a surjective ring homomorphism. (*Where does* $2^2 \equiv -1 \pmod 5$ *come in?*) Show that $\ker\varphi = (2-i)$, using $5 = (2-i)(2+i)$, and conclude, naming the theorem, that $\mathbb{Z}[i]/(2-i) \cong \mathbb{Z}_5$.

Problem 3 (Principal, prime and maximal ideals)

Let R be a commutative unital ring.

1. Let M be a proper ideal of R. Prove directly from the definitions that M is maximal if and only if, for every $a \in R \setminus M$, there is some $r \in R$ with $ra - 1 \in M$. Deduce that M is maximal if and only if R/M is a field.
2. Show that $\mathbb{Z}_3[X]/(X^2+1)$ is a field with 9 elements, but that $\mathbb{Z}_5[X]/(X^2+1)$ is not even an integral domain: exhibit two nonzero elements of it whose product is zero.
3. Show that (3) is a maximal ideal of $\mathbb{Z}[i]$, in three steps: $\mathbb{Z}[i]/(3)$ has exactly 9 elements; it has no zero divisors (*if* $3 \mid \alpha\beta$*, apply* N*, and use that a square is* 0 *or* 1 *modulo* 3); and Problem 1(2) finishes the job. By contrast, show that (5) is not even a prime ideal of $\mathbb{Z}[i]$.

Problem 4 (Irreducibles, primes, UFDs and PIDs)

1. Let D be an integral domain. Prove that every prime of D is irreducible. Then suppose that D is a principal ideal domain, and prove that for p irreducible, (p) is a maximal ideal; deduce that every irreducible of D is prime.
2. In $\mathbb{Z}[\sqrt{-3}]$, show that $U(\mathbb{Z}[\sqrt{-3}]) = \{\pm 1\}$, that no element has norm 2, and hence that 2, $1+\sqrt{-3}$ and $1-\sqrt{-3}$ are irreducible. Use the two factorizations

   $$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$$

   to show that $\mathbb{Z}[\sqrt{-3}]$ is not a unique factorization domain, and that 2 is irreducible but not prime. Conclude, naming the theorem, that $\mathbb{Z}[\sqrt{-3}]$ is not a principal ideal domain.
3. Exhibit the failure explicitly: show that the ideal $I = (2, 1+\sqrt{-3})$ of $\mathbb{Z}[\sqrt{-3}]$ is not principal. (*Every* $a+b\sqrt{-3} \in I$ *has* $a \equiv b \pmod 2$*. If* $I = (\delta)$*, what can* $N(\delta)$ *be?*)

Problem 5 (Euclidean domains)

1. Prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with Euclidean norm $N(a+b\sqrt{-2}) = a^2+2b^2$, following the proof for $\mathbb{Z}[i]$ (Li–Zhao Thm 5.33). Explain exactly where the same argument breaks down for $\mathbb{Z}[\sqrt{-3}]$, as it must by Problem 4.
2. In $\mathbb{Q}[X]$, use the Euclidean algorithm to find a greatest common divisor $d(X)$ of

$$f(X) = X^4 + X^3 + 3X^2 + 2X + 2 \qquad \text{and} \qquad g(X) = X^4 - X,$$

and write $d = \lambda f + \mu g$ with $\lambda, \mu \in \mathbb{Q}[X]$.

Problem 6 (The Gaussian integers and sums of two squares)

1. Let p be a prime number, and suppose that $p \mid n^2+1$ for some integer n. Prove that p is not irreducible in $\mathbb{Z}[i]$. ($n^2+1 = (n+i)(n-i)$. *Does p divide either factor? What does Problem 4(1) say?*) Deduce that $p = a^2+b^2$ for some integers a, b. (Such an n exists exactly when $p = 2$ or $p \equiv 1 \pmod 4$; you may quote this from the lecture.)
2. Since $12^2+1 = 145 = 5 \cdot 29$, part 1 applies to $p = 29$ with $n = 12$. Make it effective: run the Euclidean algorithm in $\mathbb{Z}[i]$ on 29 and $12+i$, and read off a, b with $29 = a^2+b^2$ from the greatest common divisor.
3. Write $493 = 17 \cdot 29$ as a sum of two squares in two genuinely different ways, by multiplying Gaussian integer factors of 17 and of 29. (*Compare* $(4+i)(5+2i)$ *with* $(4+i)(5-2i)$.)