

## MATH 350 (Fall 2024): Final Exam Review Session with Luc :)

Throughout these problems, let  $A$  and  $B$  be commutative rings with  $1 \neq 0$ .

### Problem 1.

- (a) Sort the following by inclusion: fields, Euclidean domains, PIDs, UFDs, and integral domains.
- (b) Give an example of a Euclidean domain that isn't a field and a UFD that isn't a PID.<sup>1</sup>
- (c) If  $A$  is an integral domain and  $B$  is a subring of  $A$ , is  $B$  also an integral domain?

### Problem 2. Let $\varphi : A \rightarrow B$ be a ring homomorphism.

- (a) Show that the restriction of  $\varphi$  to  $A^\times$ , denoted  $\varphi|_{A^\times}$ , is a group homomorphism from  $A^\times$  to  $B^\times$ .
- (b) Deduce that if  $A$  and  $B$  are isomorphic as rings, then  $A^\times$  and  $B^\times$  are isomorphic as groups.
- (c) Conclude that  $\mathbb{R}$  and  $\mathbb{C}$  are not isomorphic as rings.<sup>2</sup>

### Problem 3. Let $\varphi : A \rightarrow B$ be a ring homomorphism. Let $J$ be a subset of $B$ , and let $I := \varphi^{-1}(J)$ . Answer the following true-or-false questions with either a proof or a counterexample:

- (a) If  $A$  is a field, then  $\varphi$  is injective.
- (b) If  $J$  is a subring of  $B$ , then  $I$  is a subring of  $A$ .
- (c) If  $J$  is a subring of  $B$ , then  $\ker \varphi$  is an ideal in  $I$ .
- (d) If  $J$  is an ideal in  $B$ , then  $I$  is an ideal in  $A$ .
- (e) If  $J$  is a prime ideal in  $B$ , then  $I$  is a prime ideal in  $A$ .
- (f) If  $J$  is an ideal in  $B$  and  $B/J$  is an integral domain, then  $A/I$  is also an integral domain.
- (g) If  $J$  is a maximal ideal in  $B$ , then  $I$  is a maximal ideal in  $A$ .
- (h) If  $J$  is an ideal in  $B$  and  $B/J$  is a field, then  $A/I$  is also a field.
- (i) Write  $B\varphi(I) := \{bj \mid b \in B, j \in \varphi(I)\}$ . If  $J$  is an ideal in  $B$ , then  $B\varphi(I) \subset J$ .
- (j) If  $J$  is an ideal in  $B$ , then  $J \subset B\varphi(I)$ .

### Problem 4. Let $C$ be the ring of Cauchy sequences<sup>3</sup> of rational numbers with respect to the Euclidean metric $d(x, y) = |x - y|$ , and let $I$ be the ideal of $C$ whose elements converge to 0.

- (a) Convince yourself that  $C$  is a commutative ring. (No need for a proof here—this is just to make sure you remember the ring axioms.)
- (b) Verify that  $I$  is an ideal in  $C$ . (Hint: Cauchy sequences are bounded.)
- (c) Prove that  $C/I$  and  $\mathbb{R}$  are isomorphic as rings.<sup>4</sup> (Hint: Since  $\mathbb{Q}$  is dense in  $\mathbb{R}$  and  $\mathbb{R}$  is a complete metric space<sup>5</sup> with respect to the Euclidean metric, there is a natural surjection from  $C$  to  $\mathbb{R}$ .)
- (d) Let  $A$  be a ring with  $1 \neq 0$ , and let  $\mathbb{F}$  be a field. Show that if  $A$  and  $\mathbb{F}$  are isomorphic as rings, then  $A$  is a field.
- (e) Deduce that  $I$  is a maximal ideal of  $C$ .

<sup>1</sup>For an example of an integral domain that isn't a UFD, see Problem 5. For an example of a PID that isn't a Euclidean domain, see p. 282 of Dummit and Foote, but it isn't anything you'll need to know for the final.

<sup>2</sup>Nevertheless,  $\mathbb{R}$  and  $\mathbb{C}$  are isomorphic as groups. This is because they're isomorphic as vector spaces over  $\mathbb{Q}$ .

<sup>3</sup>A sequence  $(a_n)$  is called *Cauchy* if, for all  $\varepsilon > 0$ , there exists some  $N \in \mathbb{N}$  such that  $d(a_m - a_n) < \varepsilon$  for all  $m, n > N$ .

<sup>4</sup>This is Cantor's construction of the real numbers. Note how different it is from the construction by Dedekind cuts!

<sup>5</sup>A metric space  $X$  is called *complete* if every Cauchy sequence of elements of  $X$  converges to an element of  $X$ . A subset  $Y \subset X$  is called *dense* in  $X$  if, for all  $x \in X$ , there exists a sequence  $(y_n)$  in  $Y$  that converges to  $x$ .

**Problem 5.** Consider the commutative ring  $R := \mathbb{Z}[\sqrt{-5}]$  with norm  $N : R \rightarrow \mathbb{Z}_{\geq 0}$  defined<sup>6</sup> by  $N(a + b\sqrt{-5}) = a^2 + 5b^2$ . Note that for all  $\alpha, \beta \in R$ , we have  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

- (a) Is  $R$  an integral domain? Why or why not?
- (b) Show that if  $\lambda \in R$ , then  $\lambda \in R^\times$  if and only if  $N(\lambda) = 1$ .
- (c) Show that if  $\lambda \in R$  and  $N(\lambda) = 9$ , then  $\lambda$  is irreducible.
- (d) By considering the equalities  $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 = 3(3)$ , conclude that  $R$  is not a UFD.
- (e) Also, conclude that  $(3)$ , the ideal in  $R$  generated by 3, is not a prime ideal.

**Problem 6.** Let  $A$  be an integral domain with  $1 \neq 0$ , let  $\alpha \in A$ , and let  $(\alpha)$  be the ideal generated by  $\alpha$ . Answer the following true-or-false questions:

- (a)  $(0)$  is a prime ideal in  $A$ .
- (b) If  $(\alpha)$  is maximal, then  $(\alpha)$  is prime.
- (c) If  $(\alpha)$  is prime, then  $(\alpha)$  is maximal.
- (d) If  $(\alpha)$  is prime and  $\alpha \neq 0$ , then  $(\alpha)$  is maximal.
- (e) If  $(\alpha)$  is prime,  $\alpha \neq 0$ , and  $A$  is a PID, then  $(\alpha)$  is maximal. (*Hint: Check the following item.*)
- (f) If  $(\alpha)$  is prime, then  $\alpha$  is irreducible.
- (g) If  $\alpha$  is irreducible, then  $(\alpha)$  is prime. (*Hint: Check the previous problem.*)
- (h) If  $\alpha$  is irreducible and  $A$  is a PID, then  $(\alpha)$  is both prime and maximal.

**Problem 7.** Let's do a little number theory!<sup>7</sup> Let  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  be the totient function from HW10 #6.

- (a) Let  $m$  and  $n$  be relatively prime integers. Show that  $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$  and  $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ . (*Hint: For any nonzero integers  $a, b$ , there exist  $x, y \in \mathbb{Z}$  such that  $\gcd(a, b) = xa + yb$ .*<sup>8</sup>)
- (b) Let  $k_1, \dots, k_n$  be pairwise relatively prime integers, and let  $K := \prod_{i=1}^n k_i$  be their product. Prove that there exists a ring isomorphism

$$\mathbb{Z}/K \cong \mathbb{Z}/k_1 \times \mathbb{Z}/k_2 \times \cdots \times \mathbb{Z}/k_n.$$

(*Hint: Use induction on  $n$  and Sun Zi's theorem, which you proved in HW10 #2 as the "Chinese remainder theorem."*)

- (c) Give an example showing that (b) is false when the  $k_i$ 's aren't relatively prime.
- (d) Deduce that if  $n = \prod_{i=1}^k p_i^{\alpha_i}$  is the prime factorization of  $n$ , then there exists a group isomorphism

$$(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{\alpha_1})^\times \times (\mathbb{Z}/p_2^{\alpha_2})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k})^\times.$$

(*Hint: Use problem 1(b) on this worksheet.*)

- (e) Let  $n \in \mathbb{Z}$ . Show that  $|(\mathbb{Z}/n)^\times| = \varphi(n)$ . (*Hint: HW10 #6(a) and HW9 #6(c) might help.*)
- (f) Deduce that if  $n = \prod_{i=1}^k p_i^{\alpha_i}$  is the prime factorization of  $n$ , then  $\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i})$ .<sup>9</sup>

<sup>6</sup>This is actually the square of the *modulus* function  $|\cdot| : \mathbb{C} \rightarrow \mathbb{R}$ .

<sup>7</sup>This problem is actually closely related to the *classification of finitely generated abelian groups*, which you should look up if you plan on taking Math 370 (and you should, because I'll be one of the ULAs for it next semester :). I suggest Section 5.2 of Dummit and Foote as a reference.

<sup>8</sup>This is actually a consequence of the fact that  $\mathbb{Z}$  is a Euclidean domain. I highly suggest referring to p. 5 of Dummit and Foote for details!

<sup>9</sup>In other words, the totient function is a multiplicative function!

**Problem 8.** In class, you showed that if  $\mathbb{F}$  is a field, then the polynomial ring  $\mathbb{F}[x]$  is a Euclidean domain. Prove a strengthened version of the converse: if  $A$  is a commutative ring and  $A[x]$  is a PID, then  $A$  is a field. (*Hint: Check Problems 1(c) and 6(e) from earlier.*)

These next few problems (along with Problem 4(c) from earlier) use the *first isomorphism theorem for rings*, which you proved in HW9 #2.

**Problem 9.** Let  $\mathbb{C}[x, y, z]$  be the ring of polynomials in three variables with complex coefficients, and let  $(xz - y)$  be the ideal generated by  $xz - y$ . Show there exists a ring isomorphism

$$\mathbb{C}[x, y, z]/(xz - y) \cong \mathbb{C}[x, z].$$

**Problem 10.** In this problem, we prove the *second isomorphism theorem for rings*. Let  $S$  be a subring of  $A$ , and let  $I$  be an ideal in  $A$ .

- (a) Show that  $S + I$  is a subring of  $A$ .
- (b) Show that  $S \cap I$  is an ideal in  $S$ .
- (c) Prove that there exists a ring isomorphism

$$S/(S \cap I) \cong (S + I)/I.$$

**Problem 11.** Now, we prove the *third isomorphism theorem for rings*. Let  $I \subset J$  be ideals in  $A$ .

- (a) Show that  $J/I$  is an ideal of  $A/I$ .
- (b) Prove that there exists a ring isomorphism

$$(A/I)/(J/I) \cong A/J.$$

- (c) Deduce that  $J$  is prime (resp. maximal) in  $A$  if and only if  $J/I$  is prime (resp. maximal) in  $A/I$ .

**Problem 12.** In class, you showed that  $\mathbb{Z}[i]$  is a Euclidean domain with norm  $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$  given by  $N(a + bi) = a^2 + b^2$ . Let  $d = 1 + 2i$ . Apply the Euclidean algorithm to express  $8 + 7i$  in the form  $qd + r$  for some  $q, r \in \mathbb{Z}[i]$  such that  $N(r) \leq N(d)/2$ .

**Problem 13.** More true-or-false questions!

- (a) For all  $n \geq 2$ , the symmetric group  $S_n$  is generated by transpositions.
- (b) The alternating group  $A_3$  is cyclic.
- (c)  $A_n$  is a normal subgroup of  $S_n$  for all  $n \geq 2$ .

**Problem 14.** In this problem, we consider a certain element of  $S_5$ . Let  $X = \{1, 2, 3, 4, 5\}$ . Define  $g : X \rightarrow X$  by  $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 5$  and  $f : X \rightarrow X$  by  $1 \mapsto 5, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 4, 5 \mapsto 3$ , and define  $\varphi : X \rightarrow X := g \circ f$ .

- (a) Write the inversion set of  $\varphi$ .
- (b) Is  $\varphi$  an element of  $A_5$ ?
- (c) Decompose  $\varphi$  into a sequence of transpositions.

**Problem 15.** *This problem is just for fun!* How many continuous ring automorphisms are there from  $\mathbb{R}$  to  $\mathbb{R}$ ? from  $\mathbb{C}$  to  $\mathbb{C}$ ? (*Hint 1: How many ring homomorphisms are there from  $\mathbb{Q}$  to  $\mathbb{R}$ ? from  $\mathbb{Q}$  to  $\mathbb{C}$ ?*) (*Hint 2:  $\mathbb{Q}$  is a dense subset of  $\mathbb{R}$ , and  $\mathbb{Q}[i]$  is a dense subset of  $\mathbb{C}$ .*)

**You're doing great! Good luck on the final—you've got this! :)**