Exam 2: Math 100B, Winter 2023

You have 50 minutes.

You are not permitted to use calculators, books, or notes.

YOU MUST SHOW ALL YOUR WORK TO RECEIVE CREDIT.

Name ______________________________

"I have adhered to UCSD policies on academic integrity while completing this examination."

Signature ______________________________

There are 5 problems; each problem is worth 20 points.

Good luck!

Problem 1. *(20 points) This problem has two parts.*

1. *(10 points) Suppose F is a field, and $f(x) \in F[x]$ factorizes into irreducibles as $f(x) = p_1(x)^{e_1} \cdots p_m(x)^{e_m}$. That is, each $p_j(x) \in F[x]$ is irreducible, each e_j is a positive integer, and $p_i(x)$ shares no common factor with $p_j(x)$ if $i \neq j$. Set $R_j = F[x]/(p_j(x)^{e_j})$. Prove that $F[x]/(f(x))$ is isomorphic to $R_1 \times \cdots \times R_m$.*

   Proof. This was a question on the practice worksheet. Set $I_j = (p_j(x)^{e_j}) \subseteq F[x]$. Then if $j \neq k$, $I_j + I_k = (1)$, because p_j and p_k have no common factor. Thus the CRT applies, and the result follows. □

2. *(10 points) Give an example of a polynomial $f(x) \in \mathbf{R}[x]$ such that $\mathbf{R}[x]/(f(x))$ is isomorphic to $\mathbf{C} \times \mathbf{C}$. Be sure to prove your claims. (For this problem, you may use the result of the first part, regardless of whether you proved it.)*

Proof. You could take, for example, $f(x) = (x^2+1)(x^2+2)$. These polynomials are relatively prime (indeed, $(x^2+2) - (x^2+1) = 1$), so part one of the problem applies to give $\mathbf{R}[x]/(f(x)) \simeq \mathbf{R}[x]/(x^2+1) \times \mathbf{R}[x]/(x^2+2)$. But now, if $b, c \in \mathbf{R}$ such that $b^2 - 4c < 0$, then $\mathbf{R}[x]/(x^2+bx+c)$ is isomorphic to $\mathbf{C}$ via the map that sends x to $(-b+\sqrt{b^2-4c})/2$: This map is easily seen to be surjective. There are many ways to see it is injective; one way is to observe that it is injective because x^2+bx+c is irreducible, and thus $\mathbf{R}[x]/(x^2+bx+c)$ is a field. (This was also explained again on the practice problems.)

Hence $\mathbf{R}[x]/(x^2+1) \simeq \mathbf{C}$ and $\mathbf{R}[x]/(x^2+2) \simeq \mathbf{C}$ so the problem follows. □

Problem 2. *(20 points) Give an example of an integral domain R, and a nonzero element $a \in R$, such that a is irreducible but not prime. Be sure to prove your claims.*

Proof. (This is very closely related to Problem 1a in the Discussion Section worksheet from Week 6). Let $R = \mathbf{Z}[\sqrt{-3}]$. Then $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$. We claim 2 is irreducible but not prime. Indeed, 2 is irreducible because if $2 = xy$, then $4 = |x|^2|y|^2$. But if $x = a + b\sqrt{-3}$, $|x|^2 = a^2 + 3b^2$. But $a^2 + 3b^2$ is never equal to 2, so $|x|^2 = 1$ or $|y|^2 = 1$, in which case x or y is a unit. If 2 were prime, then 2 would divide one of $1+\sqrt{-3}$ or $1-\sqrt{-3}$, but it clearly does not divide either in the ring R. □

Problem 3. *(20 points) Give an example of a unique factorization domain R, and two nonzero elements $a, b \in R$ such that*

- *the greatest common divisor of a and b is 1,*
- *the element 1 is **not** expressible in the form $ra + sb$, $r, s \in R$.*

Be sure to prove your claims.

Proof. For example, we could take $R = \mathbf{C}[x, y]$, $a = x$ and $b = y$. Then no nonconstant polynomial divides both x and y, so their gcd is 1. On the other hand, $rx + sy$ always has constant term 0, so $1 \neq rs + xy$ for any $r, s \in R$. $\square$

Problem 4. *(20 points) Suppose $f(x) \in \mathbf{Z}[x]$ and $g(x) \in \mathbf{Z}[x]$ are monic polynomials of positive degree. Let $I = (f(x), g(x))$ be the ideal in $\mathbf{Z}[x]$ generated by $f(x)$ and $g(x)$, and set $R = \mathbf{Z}[x]/I$. Recall that we say that $f(x)$ and $g(x)$ have a common factor in $\mathbf{Q}[x]$ if there exists a nonconstant polynomial $h(x) \in \mathbf{Q}[x]$ such that $h(x)$ divides both $f(x)$ and $g(x)$ in $\mathbf{Q}[x]$.*

1. *(10 points) Suppose $f(x)$ and $g(x)$ have a common factor in $\mathbf{Q}[x]$. Prove that, in this case, R has infinitely many elements.*

   Proof. (The two parts of this problem are closely related to Problem 5 of Homework 6). Observe that there are no integers in the ideal I, because if there were, $f(x)$ and $g(x)$ would have gcd equal to 1 in $\mathbf{Q}[x]$. Consequently, the map $\mathbf{Z} \to R$ is injective, so R has infinitely many elements. □

2. *(10 points) Suppose $f(x)$ and $g(x)$ do not have a common factor in $\mathbf{Q}[x]$. Now prove that R has finitely many elements.*

   Proof. In this case, there is a nonzero integer $N \in I$, as one sees by clearing denominators in the equality $r(x)f(x) + s(x)g(x) = 1$ in $\mathbf{Q}[x]$. Set $J = (N, f(x))$. Then $J \subseteq I$, so $\mathbf{Z}[x]/J$ surjects onto $\mathbf{Z}[x]/I$. But $\mathbf{Z}[x]/J = (\mathbf{Z}/N\mathbf{Z}[)x]/(\overline{f}(x))$ has size $N^{deg(f)}$ because $f(x)$ is monic. Thus $\mathbf{Z}[x]/J$ has finite size, so $R = \mathbf{Z}[x]/I$ does as well. □

Problem 5. *(20 points) Suppose p is a prime number, and a, b are integers such that $a^2 + b^2 = p$. Prove that the quotient ring $\mathbf{Z}[i]/(a + ib)$ is a field.*

Proof. (This is essentially Problem 2a of the Week 6 discussion worksheet.) Set $z = a + ib$. If $z = xy$, then $p = a^2 + b^2 = |z|^2 = |x|^2|y|^2$. Consequently, $|x|^2 = 1$ or $|y|^2 = 1$, so x or y is a unit. Thus z is irreducible. Because $\mathbf{Z}[x]$ is a PID, (z) is maximal and thus $\mathbf{Z}[i]/(a + ib)$ is a field. (In fact, it is the field with p elements.) $\square$

THIS PAGE INTENTIONALLY LEFT BLANK