Exam 1: 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) Suppose p is a prime number and set $R = \mathbf{Z}/p\mathbf{Z}$. Determine the size of the unit group of the polynomial ring $R[x]$ explicitly in terms of p. Be sure to prove your answer.*

Proof. For $R = \mathbf{Z}/p\mathbf{Z}$ (or more generally, a field), the unit group of $R[x]$ is $R^\times$, embedded as the constant polynomials. To see this, first observe that these elements are units. For the converse, suppose $f(x) \in R[x]$ with $f(x)g(x) = 1$. If f has leading term $a_n x^n$, with $a_n \neq 0$, and g has leading term $b_m x^m$, with $b_m \neq 0$, then $f(x)g(x)$ has leading term $a_n b_m x^{n+m}$. If $f(x)g(x) = 1$, then necessarily $n = m = 0$, and $a_n b_m = 1$, giving the desired conclusion.

Because R is a field with size p, it has $p - 1$ units. Thus $(R[x])^\times$ has size $p - 1$. □

Problem 2. *(20 points) The two parts of this question are not related to one another. For both parts, be sure to justify your answer.*

1. *(10 points) Give an example of a ring R that has finitely many elements, and contains at least 3 distinct ideals.*

   Proof. For example $R = \mathbf{Z}/15\mathbf{Z}$. It has 15 elements. Three ideals of R are (0), (1) and (5). These are clearly distinct, because the principal ideal generated by 5 contains just the elements $\{\overline{0}, \overline{5}, \overline{10}\}$. □

2. *(10 points) Give an example of a ring of characteristic 0 that is not a field.*

   Proof. The integers $\mathbf{Z}$ is an example. This ring (trivially) has characteristic 0, and it is not a field because, for instance, 2 is not invertible in $\mathbf{Z}$. □

Problem 3. *(20 points) Suppose R is a ring in which every ideal is principal. Let $a \in R$ be fixed, and set $I = (x-a) \subseteq R[x]$ the principal ideal of $R[x]$ generated by $x-a$. If J is an ideal of $R[x]$ that contains I, prove that J can be generated by two elements, i.e., that there exists $r_1(x), r_2(x) \in R[x]$ so that $J = (r_1(x), r_2(x))$.*

Proof. This is just like a homework question, except a bit easier. Set $J' = J \cap R$. This set is immediately seen to be an ideal of R, and is thus principal $J' = Rb$ for some $b \in R$. We claim $J = (x-a, b)$. It is clear that $(x-a, b)$ is contained in J. For the reverse inclusion, suppose $f(x) \in J$. By division with remainder, $f(x) = q(x)(x-a) + r$ for some $r \in R$. But then clearly $r \in J'$, so $r = sb$ for some $s \in R$. The result follows. $\square$

Problem 4. *(20 points) Let $R = \mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}\}$ be the ring of Gaussian integers. Suppose $I \subseteq R$ is a nonzero ideal.*

1. *(10 points) Prove that there exists a nonzero integer $n \in I$.*

   Proof. This is exactly a homework question: if $a + ib \in I$ is nonzero, then $n = a^2 + b^2 = (a - ib)(a + ib)$ is a nonzero integer in I. □

2. *(10 points) Prove that the quotient abelian group R/I has finite size.* For this question, you may assume that there exists a nonzero integer $n \in I$, regardless of whether you proved that in part (1).

   Proof. Because I is an ideal and $n \in I$, I contains $nR = \{na + inb : a, b \in \mathbf{Z}\}$. It is clear that R/nR has size n^2: For example, every coset of nR in R can be represented by an element $u + iv$ with u, v integers in $\{0, 1, 2, \ldots, n - 1\}$. Because R/I is a quotient of R/nR (as abelian groups), it too has finite size. □

Problem 5. *(20 points) Consider the map* $\varphi : \mathbf{Q}[x, y] \to \mathbf{Q}[t]$ *given by* $\varphi(f(x, y)) = f(t, t^3 + t^2 + 3)$. *Find a polynomial* $g(x, y) \in \mathbf{Q}[x, y]$ *so that* $\ker(\varphi)$ *is the principal ideal generated by* $g(x, y)$. *Be sure to prove your result.*

Proof. It is clear that $g(x, y) = y - (x^3 + x^2 + 3)$ is in $\ker(\varphi)$. We claim $\ker(\varphi)$ is generated by g. To see this, suppose $f(x, y)$ in $\ker(\varphi)$ is arbitrary. By division with remainder, thinking of g as monic in y of degree 1, we can write $f(x, y) = q(x, y)g(x, y) + r(x)$ where $r(x) \in \mathbf{Q}[x]$. Applying φ, we see $r(t) = 0$, so $r = 0$. Thus g divides f as desired. □

THIS PAGE INTENTIONALLY LEFT BLANK