Math 547, Exam 2. 3/19/10. Name: ____________

- Read problems carefully. Show all work.
- No notes, calculator, or text.
- The exam is approximately 15 percent of the total grade.
- There are 100 points total. Partial credit may be given.

1. **(15 points)**

   (a) **(5 points)** Give an example of an R which is a UFD but not a PID. Exhibit an ideal $I \lhd R$ which is not principal. **No justification required. You may cite examples from homework or lecture.**

   Solution: The ring $\mathbb{Z}[x]$ is a UFD but not a PID. Then ideal $I = (2, x)$ is not principal.

   (b) **(10 points)** Let R be an integral domain, and suppose that $f(x) \in R[x]$ is a unit. Use the notion of **degree** to show that f is constant, and therefore a unit in R.

   Proof. If $f(x) \in (R[x])^{\times}$, then there exists $g(x) \in (R[x])^{\times}$ for which $f(x)g(x) = 1$. Taking degrees, since R is an integral domain, we find that

   $$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) = \deg(1) = 0.$$

   Since $f(x)$, $g(x) \neq 0$, their degrees are non-negative; the degrees sum to zero, so they must be zero. Hence, $f(x)$ is constant. $\square$

2. **(15 points)** Let $f(x) = a_n x^n + \cdots a_0 \in \mathbb{Z}[x]$.

   (a) **(5 points)** Define what the **content** of $f(x)$ is. Use a complete sentence.

   Solution: The **content** of f is the greatest common divisor of its coefficients: $C(f) = \gcd(a_0, \ldots, a_n)$.

   (b) **(5 points)** What does it mean for $f(x)$ to be **primitive**? Use a complete sentence.

   Solution: The polynomial $f(x)$ is **primitive** if and only if its content is one: $C(f) = 1$.

   (c) **(5 points)** State **Gauss' Lemma**.

   Solution: Let $f(x)$ and $g(x) \in \mathbb{Z}[x]$. Then we have

   - If $f(x)$ and $g(x)$ are primitive, then $f(x)g(x)$ is primitive.
   - The product of contents of $f(x)$ and $g(x)$ is the content of the product of $f(x)$ and $g(x)$: $C(fg) = C(f)C(g)$.

3. **(25 points)** Consider the ring $R = \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$. Define the **norm** map on R for all $r = a + b\sqrt{-6} \in R$ by $N(r) = (a + b\sqrt{-6})(a - b\sqrt{-6}) = a^2 + 6b^2$. You may assume the following facts:

   (i) For all r, $s \in R$, we have $N(rs) = N(r)N(s)$.

   (ii) $u \in R$ is a unit if and only if $N(u) = \pm 1$.

   (a) **(10 points)** The elements 2, 5, $2 + \sqrt{-6}$, and $2 - \sqrt{-6}$ are irreducible in R.
   Use the norm to show that 2 is irreducible in R.

   Proof. Suppose that $\exists x, y \in R$ with $2 = xy$. Taking norms and using fact (i), we obtain

$$4 = N(2) = N(xy) = N(x)N(y).$$

   Therefore, we see that $N(x) \in \{1, 2, 4\}$. Suppose that $N(x) = 2$. If $x = a + b\sqrt{-6}$, then we have $N(x) = a^2 + 6b^2 = 2$, which has no solution in integers a, b. Hence, we see that $N(x) \neq 2$. If $N(x) = 1$, then fact (ii) implies that $x \in R^\times$, so 2 is irreducible. If $N(x) = 4$, then $N(y) = 1$. Fact (ii) implies that $y \in R^\times$, so 2 is irreducible. $\square$

   (b) **(10 points)** The element 2 is associated to neither $2 + \sqrt{-6}$ nor to $2 - \sqrt{-6}$.
   Use the norm to show that 2 is not associated to $2 + \sqrt{-6}$.

   Proof. Suppose on the contrary that $2 \sim 2 + \sqrt{-6}$. Then there is a unit $u \in R^\times$ for which $2 = (2 + \sqrt{-6})u$. Taking norms and using facts (i) and (ii), we find that

$$4 = N(2) = N((2+\sqrt{-6})(u)) = N(2+\sqrt{-6})N(u) = \pm(2+\sqrt{-6})\cdot(2-\sqrt{-6}) = \pm 10,$$

   a contradiction. Hence, $2 \not\sim 2 + \sqrt{-6}$. Similarly one can show that $2 \not\sim 2 - \sqrt{-6}$. $\square$

   (c) **(5 points)** Explain why R is not a UFD (unique factorization domain).
   You may use the facts stated in parts (a) and (b) of this question.

   Proof. Part (a) asserts that 2, 5, $2 + \sqrt{-6}$, and $2 - \sqrt{-6}$ are irreducible in R;
   part (b) asserts that 2 is associated to neither $2 + \sqrt{-6}$ nor to $2 - \sqrt{-6}$. Therefore,

$$2 \cdot 5 = 10 = (2 + \sqrt{-6}) \cdot (2 - \sqrt{-6})$$

   gives distinct factorizations into irreducibles in R. $\square$

4. **(20 points)** Let $F \subseteq E$ be fields, and let $r \in E$. Recall that the **evaluation homomorphism** at r is $\phi_r : F[x] \to E$ defined for all $f(x) \in F[x]$ by $\phi_r(f(x)) = f(r)$.

   (a) **(5 points)** Explain why there exists a polynomial $f(x) \in F[x]$ such that $\ker\phi_r = (f(x)) \triangleleft F[x]$.

   (What kind of ring is $F[x]$?)

   Proof. Since F is a field, the ring $F[x]$ is a PID. Hence, the ideal $\ker\phi_r$ is prinicipal: there exists $f(x) \in F[x]$ with $\ker\phi_r = (f(x)) \triangleleft F[x]$. □

   (b) **(10 points)** Assume that there exists a polynomial $f(x) \in F[x]$ for which $\ker\phi_r = (f(x)) \triangleleft F[x]$. Show that $f(x)$ is **irreducible** in $F[x]$.

   (Observe that the image is an integral domain.)

   Proof. By the Fundamental Ring Homomorphism Theorem, we find that

   $$F[x]/(f(x)) \cong \mathrm{Im}\phi_r \subseteq E.$$

   Now, $\mathrm{Im}\phi_r$ is a subring of a field, so it is an integral domain. It follows that the ideal $(f(x))$ is prime; hence, $f(x)$ is prime in $F[x]$. Since $F[x]$ is a PID, the polynomial $f(x)$ is irreducible in $F[x]$. □

   (c) **(5 points)** Assume the results of parts (a) and (b), namely that there exists $f(x)$, irreducible in $F[x]$, for which $\ker\phi_r = (f(x))$. Explain why $F[x]/(f(x))$ is a field.

   (You can get full credit without doing part (a) nor part (b) correctly.)

   Proof. Since $f(x)$ is irreducible in $F[x]$, a PID, the ideal $(f(x)) \triangleleft F[x]$ is maximal. Hence, $F[x]/(f(x))$ is a field. □

5. **(25 points)** Determine whether the following polynomials are irreducible.
The method you use may depend on the **degree**.

(a) **(9 points)** Determine whether $f(x) = x^3 + x - 3 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$.
Justify your answer.

Claim: The polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Since $\deg(f(x)) = 3$, it follows that $f(x)$ is reducible in $\mathbb{Q}[x]$ if and only if it has a root in $\mathbb{Q}$. Therefore, it suffices to check for roots in $\mathbb{Q}$. By the Rational Root Theorem, the possible rational roots are ± 1, ± 3. Since $f(-3) = -33$, $f(-1) = -5$, $f(1) = -1$, and $f(3) = 27$, none of which are zero, we conclude that $f(x)$ has no rational roots; hence, it is irreducible in $\mathbb{Q}[x]$. Since it is primitive, it is also irreducible in $\mathbb{Z}[x]$. □

(b) **(9 points)** Determine whether $f(x) = x^3 + x - 3 \in \mathbb{Z}_5[x]$ is irreducible in $\mathbb{Z}_5[x]$.
Justify your answer.

Claim: The polynomial $f(x)$ is reducible in $\mathbb{Z}_5[x]$.

Proof. Since $\deg(f(x)) = 3$, it follows that $f(x)$ is reducible in $\mathbb{Z}_5[x]$ if and only if it has a root in $\mathbb{Z}_5$. Therefore, it suffices to check for roots in $\mathbb{Z}_5$. We test as follows; $f(0) \equiv -3 \equiv 2 \pmod{5}$, $f(1) \equiv -1 \equiv 4 \pmod{5}$, $f(2) \equiv 2 \pmod{5}$, $f(3) \equiv 2 \pmod{5}$, $f(4) \equiv 0 \pmod{5}$. Now, since $x \equiv 4 \pmod{5}$ is a root, $f(x)$ is reducible in $\mathbb{Z}_5[x]$. □

(c) **(7 points)** Show that $2x^5 - 6x^3 + 9x^2 - 15 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$

Proof. The polynomial is 3-Eisenstein; hence it is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion. Since $f(x)$ is primitive, it is irreducible in $\mathbb{Z}[x]$. □

6. **Challenge problem:** You can attempt the challenge problem if and only if you have completed the regular portion of the exam.

   Let R be an integral domain which satisfies the **descending chain condition**: whenever

   $$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m \supseteq \cdots$$

   is a descending chain of ideals in R, there exists $N \geq 1$ in $\mathbb{Z}$ such that $\forall n \geq N$, we have $I_N = I_n$. I.e., every descending ideal chain stabilizes. Show that R is a field.

Extra scratch paper.