MATH 4281 Final Exam **Name:** _____

Question 1. True of False . . . . . 10 points

Mark each of the following "T" (if true) of "F" (if false).

1 pts (a) **T** $\mathbb{Z}$ is a principal ideal domain.

1 pts (b) **T** $\mathbb{Z}_2[x]$ is a principal ideal domain.

1 pts (c) **F** A ring F is a field if every nonzero element in F has multiplicative inverse.

1 pts (d) **T** Every subring of an integral domain is an integral domain.

1 pts (e) **F** Every subring of a field is a field.

1 pts (f) **F** Every irreducible element is a prime element.

1 pts (g) **T** There are infinitely many subrings of $\mathbb{R}$ which contains $\mathbb{Q}$.

1 pts (h) **F** There are infinitely many subrings of $\mathbb{C}$ which contains $\mathbb{R}$.

1 pts (i) **F** If D is an integral domain and $I \subsetneq D$ is a proper ideal of D, then D/I is an integral domain.

1 pts (j) **T** If F is a field and $I \subsetneq F$ is a proper ideal of F, then F/I is a field.

Question 2. Ideals of a polynomial ring ..... 10 points

3 pts (a) Suppose that we are given a field F and a fixed element $\alpha \in F$. Define

$$I := \{f(x) \in F[x] \mid f(\alpha) = 0\}.$$

Show that I is an ideal of $F[x]$ generated by $x - \alpha \in F[x]$.

3 pts (b) Find an example such that F is a field, $I \subset F[x, y]$ is an ideal, but I is not principal. Explain why your example satisfies the given conditions.

4 pts (c) Define

$$I := \{f(x) \in \mathbb{R}[x] \mid f(i + 1) = 0\}$$

where $i \in \mathbb{C}$ is a square root of -1. Show that I is a principal ideal of $\mathbb{R}[x]$ and find $g(x) \in \mathbb{R}[x]$ such that $I = (g(x))$.

Answer. (a) Since I is the kernel of an F-algebra homomorphism $\phi_\alpha : F[x] \to F : f(x) \mapsto f(\alpha)$, I is an ideal of $F[x]$. SInce $\phi_\alpha(x-\alpha) = 0$, $x-\alpha \in I$, thus $(x-\alpha) \subset I$. Since $x - \alpha$ is irreducible, $(x - \alpha)$ is a maximal ideal. But $\phi_\alpha(1) \neq 0$, thus $I \neq F[x]$. Thus $(x - \alpha) = I$.

(b) Let $I = (x, y) \subset \mathbb{C}[x, y]$, an ideal generated by $\{x, y\}$. If I were principal, then there exists $f = f(x, y) \in \mathbb{C}[x, y]$ such that $I = (f)$. Since $I \neq \mathbb{C}[x, y]$, f is not a unit. Then since $f|x$ and $f|y$, there exists $u, v \in \mathbb{C}^\times$ such that $f = ux = vy$. But this is impossible.

(c) We claim that $I = (x^2 - 2x + 2)$. Since I is the kernel of an $\mathbb{R}$-algebra homomorphism $\phi : \mathbb{R}[x] \to \mathbb{C} : f(x) \mapsto f(i + 1)$, I is an ideal of $\mathbb{R}[x]$. Also since $\phi(x^2-2x+2) = 0$, $x^2-2x+2 \in I$, thus $(x^2-2x+2) \subset I$. Note that x^2-2x+2 is irreducible in $\mathbb{R}[x]$, since it cannot be a product of two linear polynomials. (x^2-2x+2 does not have a root in $\mathbb{R}$.) Thus $(x^2 - 2x + 2)$ is a maximal ideal of $\mathbb{R}[x]$. Since $\phi(1) \neq 0$, $I \neq \mathbb{R}[x]$, thus it follows that $(x^2 - 2x + 2) = I$.

Question 3. Greatest common divisor . . . . . 15 points

Recall the definition of greatest common divisor (gcd). In the following questions, you are not required, but allowed, to use the following fact: for any $a, b \in \mathbb{Z}$ such that $(a, b) \neq (0, 0)$,

$$\gcd(a, b) = c \quad \Leftrightarrow \quad c \geq 0 \text{ and } (a) + (b) = (c).$$

3 pts (a) For $a, b \in \mathbb{Z}$, if $a > 0$ and $a|b$, then show that $\gcd(a, b) = a$.

3 pts (b) If $a \neq 0$, then show that $\gcd(a, b) = \gcd(a, b + xa)$ for any $x \in \mathbb{Z}$.

3 pts (c) Let p be a positive prime number. Then show that $\gcd(a, p)$ equals 1 or p.

3 pts (d) If $c \neq 0$ and $\gcd(ab, c) = 1$, then show that $\gcd(a, c) = \gcd(b, c) = 1$.

3 pts (e) If $ra + sb = 1$ for some $a, b, r, s \in \mathbb{Z}$, then show that $\gcd(a, b) = 1$.

Answer. (a) It follows from that $(a) + (b) = (a)$ since $b \in (a)$ by assumption.

(b) Since $a, b+xa \in (a)+(b)$, $(a)+(b+xa) \subset (a)+(b)$. Conversely, $a, b \in (a)+(b+xa)$, thus $(a)+(b) \subset (a)+(b+xa)$. Thus $(a)+(b) = (a)+(b+xa)$. The assertion follows from this as $\mathbb{Z}$ is a PID.

(c) Since p is nonzero and prime, (p) is maximal. Thus $(a) + (p) = (1)$ or (p), which implies the assertion.

(d) Since $ab \in (a)$ and $ab \in (b)$, we have $(1) = (ab) + (c) \subset (a) + (c)$ and $(1) = (ab) + (c) \subset (b) + (c)$, from which the result follows.

(e) The condition means that $1 \in (a) + (b)$. Thus $(1) = (a) + (b)$, which implies the result.

Question 4. Nilpotent radical of a commutative ring ..... 15 points

Let A be a commutative ring. We say that $a \in A$ is a nilpotent element if $a^n = 0$ for some $n \in \mathbb{Z}_{>0}$. We define $\mathrm{nil}(A) := \{a \in A \mid a \text{ is nilpotent}\}$.

3 pts (a) Show that $\mathrm{nil}(A)$ is closed under addition.

3 pts (b) Show that $(\mathrm{nil}(A), +)$ is an abelian subgroup of $(A, +)$.

3 pts (c) Show that $\mathrm{nil}(A)$ is an ideal of A.

3 pts (d) For $x \in A/\mathrm{nil}(A)$, show that x is nilpotent if and only if x is zero.

3 pts (e) Suppose that $P \subset A$ is a prime ideal of A. Prove that $\mathrm{nil}(A) \subset P$.

Answer. (a) Let $a, b \in \mathrm{nil}(A)$. Then there exists $m, n \in \mathbb{Z}_{>0}$ such that $a^m = b^n = 0$. Now we have

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i} = 0,$$

thus $a + b \in \mathrm{nil}(A)$.

(b) As $0^1 = 0$, $0 \in \mathrm{nil}(A)$. Also if $a \in \mathrm{nil}(A)$, then there exists $n \in \mathbb{Z}_{>0}$ such that $a^n = 0$, thus $(-a)^n = (-1)^n a^n = 0$ which means $-a \in \mathrm{nil}(A)$. Combined with (a), we conclude that $\mathrm{nil}(A)$ is an abelian subgroup of A.

(c) By (b), it remains to show that $\mathrm{nil}(A)$ absorbs products in A. Now for $a \in A$ and $x \in \mathrm{nil}(A)$, there exists $n \in \mathbb{Z}_{>0}$ such that $x^n = 0$. Then $(ax)^n = a^n x^n = 0$, thus $ax \in \mathrm{nil}(A)$. Thus $\mathrm{nil}(A)$ is an ideal of A.

(d) If $x = 0$ then it is clearly nilpotent (e.g. by (b)). Conversely, suppose that x is nilpotent and $x = a + \mathrm{nil}(A)$ for some $a \in A$. Then there exists $n \in \mathbb{Z}_{>0}$ such that $x^n = 0$, i.e. $a^n \in \mathrm{nil}(A)$. Thus there exists $m \in \mathbb{Z}_{>0}$ such that $a^{nm} = (a^n)^m = 0$. But it means that a is nilpotent, i.e. $a \in \mathrm{nil}(A)$. Thus $x = a + \mathrm{nil}(A) = \mathrm{nil}(A)$, i.e. $x = 0$ as desired.

(e) Let $a \in \mathrm{nil}(A)$. Then there exists $n \in \mathbb{Z}_{>0}$ such that $a^n = 0$. Thus $a^n \in P$. Now we proceed by induction on n to prove that $a \in P$. If $n = 1$, then $a^1 = a \in P$, thus it is obvious. In general, if $n > 1$ then by the definition of a prime ideal we have $a \in P$ or $a^{n-1} \in P$. Thus $a \in P$ by induction assumption. Since $a \in \mathrm{nil}(A)$ was arbitrary, it follows that $\mathrm{nil}(A) = P$.

Question 5. Ideals and homomorphisms . . . . . 15 points

Let A and B be commutative rings and $f : A \to B$ be a ring homomorphism. Also let $I \subset A$ be an ideal of A and $J \subset B$ be an ideal of B.

3 pts (a) Show that $f^{-1}(J)$ is an ideal of A.

3 pts (b) Suppose that f is surjective. Show that $f(I)$ absorbs product in B, i.e. for any $y \in f(I)$ and $b \in B$ we have $by \in f(I)$.

3 pts (c) In general, find an example such that $f(I)$ is not an ideal of B. Explain why your example satisfies such a given condition.

For an ideal I of A we define $I^e \subset B$ to be the ideal generated by $f(I) \subset B$, i.e. $I^e = (f(I))$. By (c), I^e is not necessarily equal to $f(I)$.

3 pts (d) Show that $(f^{-1}(J))^e \subset J$.

3 pts (e) Show that $(f^{-1}(I^e))^e = I^e$.

Answer. (a) $f^{-1}(J)$ is an abelian subgroup of A since J is an abelian subgroup of B and f is a group homomorphism. Now for any $a \in A$ and $x \in f^{-1}(J)$, $f(ax) = f(a)f(x) \in J$. Thus $ax \in f^{-1}(J)$ which means that $f^{-1}(J)$ absorbs products in A.

(b) For any $b \in B$ and $y \in f(I)$, choose $a \in A$ and $x \in I$ such that $f(a) = b$ and $f(x) = y$. Then $by = f(a)f(x) = f(ax) \in f(I)$, thus $f(I)$ absorbs product in B.

(c) Let $f : \mathbb{Z} \to \mathbb{Q}$ and $I = \mathbb{Z}$. Then $f(I) = \mathbb{Z} \subset \mathbb{Q}$ is not an ideal of $\mathbb{Q}$ since the only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$ itself.

(d) Since J is an ideal of B, it suffices to show that $f(f^{-1}(J)) \subset J$. But it is clear from the property of a function.

(e) By (d), we have $(f^{-1}(I^e))^e \subset I^e$. Conversely, it is clear that $f(I) = f(f^{-1}(f(I)))$ from the property of a function. (In general, for any $X \subset \operatorname{im} f$ we have $X = f(f^{-1}(X))$.) Thus we have (here we use bold parentheses to denote ideals generated by a subset)

$$I^e = \big(f(I)\big) = \big(f(f^{-1}(f(I)))\big) \subset \big(f(f^{-1}(I^e))\big) = (f^{-1}(I^e))^e.$$

Here, the middle inclusion is from the fact that $f(I) \subset I^e$. Thus the result follows.

Question 6. Polynomials over a finite field.....15 points

Consider all the monic quadratic polynomials over $\mathbb{Z}_3$, i.e.

$$x^2 + ax + b \in \mathbb{Z}_3[x] \quad \text{where} \quad a, b \in \{0, 1, 2\}.$$

We want to find all the irreducible polynomials among them. For example, x^2+1 is irreducible because it is not possible to find $c, d \in \mathbb{Z}_3$ such that $x^2 + 1 = (x + c)(x + d)$.

3 pts (a) There are two more irreducible polynomials besides $x^2 + 1$. What are they? (You do not need to justify your answer.)

$$x^2 + x + 2, \quad x^2 + 2x + 2$$

We define $F := \mathbb{Z}_3[x]/(x^2+1)$. Then F is a field because x^2+1 is an irreducible polynomial.

3 pts (b) There are 9 elements in F. List all of them without repetition. (You do not need to justify your answer.)

$$F = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$$

3 pts (c) Recall that $(F^\times, \cdot)$ is an abelian group. For $\alpha \in F^\times$, show that $\langle\alpha\rangle = (F^\times, \cdot)$ if and only if $\alpha^4 \neq 1$.

3 pts (d) Find $a, b \in \mathbb{Z}_3$ such that $(x + 1)^4 = ax + b$ in F and check that $(x + 1)^4 \neq 1$.

Thus, $x + 1$ is a generator of $(F^\times, \cdot)$. In other words, $(F^\times, \cdot) \simeq (\mathbb{Z}_8, +)$.

3 pts (e) Find all the generators of $(F^\times, \times)$. (You do not need to justify your answer.) (Hint: How can you find all the generators of a cyclic group if you know one of them?)

$$x + 1, x + 2, 2x + 1, 2x + 2$$

Answer. (c) Since $|F^\times| = 8$, by Lagrange's theorem an order of any element in $F^\times$ is either 1, 2, 4, or 8. Thus $\langle a\rangle = F^\times \Leftrightarrow |a| = 8 \Leftrightarrow a \neq 1, a^2 \neq 1, a^4 \neq 1 \Leftrightarrow a^4 \neq 1$ since 1, 2, 4 are divisors of 4.

(d) $(x+1)^4 = (x^2+x+2)(x^2+1)+2 = 2$ in F, thus $(a, b) = (0, 2)$. Also, $(x+1)^4 \neq 1$.

Question 7. Local ring . . . . . 20 points

Fix a prime number $p \in \mathbb{Z}$. We define $A_p \subset \mathbb{Q}$ to be

$$A_p := \left\{ r \in \mathbb{Q} \mid r = \frac{n}{m} \text{ for some } n \in \mathbb{Z},\ m \in \mathbb{Z} - p\mathbb{Z} \right\}.$$

Equivalently, A_p is a set of rational numbers "whose denominator is not a multiple of p." For example, when $p = 2$ we have

$$1, \frac{1}{3}, \frac{1}{5}, \ldots \in A_p \quad \text{but} \quad \frac{1}{2}, \frac{1}{4}, \frac{1}{6}, \ldots \notin A_p.$$

Also, $\mathbb{Z}$ is contained in A_p.

3 pts (a) Show that A_p is closed under addition.

3 pts (b) Show that $(A_p, +)$ is an abelian subgroup of $(\mathbb{Q}, +)$.

3 pts (c) Show that A_p is a subring of $\mathbb{Q}$.

Let $(p) \subset A_p$ be the ideal generated by $p \in A_p$, i.e.

$$(p) = \left\{ r \in A_p \mid r = \frac{n}{m} \text{ for some } n \in p\mathbb{Z},\ m \in \mathbb{Z} - p\mathbb{Z} \right\}.$$

4 pts (d) Show that A_p is a disjoint union of (p) and $A_p^\times$.

3 pts (e) Show that (p) is a maximal ideal of A_p.

4 pts (f) Suppose that $I \subset A_p$ is a maximal ideal of A_p. Show that $I = (p)$.

Answer. (a) For any $a, b, c, d \in \mathbb{Z}$ such that $b, d \notin p\mathbb{Z}$, we have $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $bd \notin p\mathbb{Z}$. Thus if $\frac{a}{b}, \frac{c}{d} \in A_p$ then $\frac{a}{b} + \frac{c}{d} \in A_p$.

(b) Clearly $0 = 0/1 \in A_p$. Also for any $a, b \in \mathbb{Z}$ such that $b \notin p\mathbb{Z}$, $-\frac{a}{b} = \frac{-a}{b}$ and $b \notin p\mathbb{Z}$. Thus if $\frac{a}{b} \in A_p$ then $-\frac{a}{b} \in A_p$. Combined with (a), it follows that A_p is an abelian subgroup of $\mathbb{Q}$.

(c) For any $a, b, c, d \in \mathbb{Z}$ such that $b, d \notin p\mathbb{Z}$, we have $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ and $bd \notin p\mathbb{Z}$. Thus if $\frac{a}{b}, \frac{c}{d} \in A_p$ then $\frac{a}{b}\frac{c}{d} \in A_p$. Furthermore, $1 = 1/1 \in A_p$. Thus A_p is a subring of $\mathbb{Q}$.

(d) Let $r \in A_p - A_p^\times$. It suffices to show that $r \in (p)$. If $r = 0$ then we are done, so suppose otherwise and write $r = \frac{n}{m}$ for some $n \in \mathbb{Z}, m \in \mathbb{Z} - p\mathbb{Z}$. Clearly $n \neq 0$, and in $\mathbb{Q}$ the multiplicative inverse of r is given by $\frac{m}{n}$. Since r is not invertible in A_p, it means that $\frac{m}{n} \notin A_p$. By definition of A_p, it means that $n \in p\mathbb{Z}$, thus $\frac{n}{m} \in (p)$ as desired.

(e) Suppose that J is an ideal of A_p such that $(p) \subsetneq J$. Then there exists $x \in J - (p)$, which is a unit of A_p by (d). Thus $J = A_p$. It follows that (p) is maximal.

(f) Since $I \neq A_p$, I cannot contain a unit, which means that $I \cap A_p^\times = \emptyset$. By (d), it means $I \subset (p)$. Since I is maximal, it follows that $I = (p)$.

(This page is intentionally left blank)