Math 307 Final Examination (Take home part) **Name: Sample solution**

1. Let R be a commutative ring and N an ideal of R.

   (a) Show that $J = \{a \in R : a^n \in N \text{ for some } n \in \mathbb{Z}^+\}$ is an ideal of R.

   Solution. Clearly, $0^1 \in N$ so that $0 \in J$.

   If $a, b \in J$, then $a^n, b^m \in N$. So, $(a-b)^{n+m} = \sum_{j=0}^{n+m} \binom{n+m}{j} a^j b^{m+n-j} \in J$ because $a^j b^{m+n-j} \in J$ as $j \geq n$ or $m+n-j \geq m$.

   Further, if $a^n \in N, c \in R$, then $(ac)^n = a^n c^n \in N$.

   Combining, we see that J is an ideal.

   (b) Suppose $R = \mathbb{Z}$. Give an example of N so that $J \neq N$.

   Proof. Let $N = 4\mathbb{Z}$. Then $2 \notin N$, but $2 \in J$ as $2^2 = 4 \in N$. So, $N \neq J$.

2. (a) Let D' be a subdomain of an integral domain D. Show that $\text{char}(D') = \text{char}(D)$.

   Solution. Suppose $1 \in D$ and $1' \in D'$ are the unity of D and D', respectively. Then $1' = 1'1'$ in D' and $11' = 1'$ in D so that $0 = 11' - 1'1' = (1-1')1'$. Since D has no zero divisor, $1 = 1'$. As a result, $\text{char}(D') = |1'| = |1| = \text{char}(D)$.

   (b) Give an example to show that the characteristic of a subring of a ring R may be different from that of R.

   Solution. Let $R = \mathbb{Z}_4$, $K = \{2, 0\} \subseteq R$. Then $\text{char}(R) = 4$ and $\text{char}(K) = 2$.

   (c) Give an example of a chain of 5 distinct integral domains $D_1 \subseteq D_2 \subseteq D_3 \subseteq D_4 \subseteq D_5$.

   Solution. Examples: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{C}[x]$, $\mathbb{Z} \subseteq \mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$,

   $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R} \subseteq \mathbb{C}$.

   Common mistakes $\mathbb{Z}_2$ is not a subring of $\mathbb{Z}$.

3. Determine (with explanation) ALL ring homomorphisms $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$.

   Solution. Consider all possible values of $\phi(1,0) = (a,b)$ and $\phi(0,1) = (c,d)$. Because $\phi((1,0)(1,0)) = \phi(1,0)$. So, $a^2 = a, b^2 = 1$ so that $a, b \in \{1, 0\}$. Similarly, $\{c, d\} \in \{1, 0\}$.

   Note also that $\phi(1,1)^2 = \phi(1,1)$. So, $a + c, b + d \in \{0, 1\}$.

   If $(a,b) = (0,0)$ then $(c,d) \in \{(0,0),(1,0),(0,1),(1,1)\}$; if $(a,b) = (1,0)$ then $(c,d) \in \{(0,0),(0,1)\}$; if $(a,b) = (0,1)$ then $(c,d) \in \{(0,0),(1,0)\}$; if $(a,b) = (1,1)$ then $(c,d) = (0,0)$.

   Thus, we may have $\phi(x,y) = (0,0),(y,0),(0,y),(y,y),(x,0),(x,y),(0,x),(y,x)$, or (x,x). It is easy to check that each of these 9 cases indeed yield a ring homomorphism: First, $\phi(x,y) = x\phi(1,0) + y\phi(0,1) \in \mathbb{Z} \oplus \mathbb{Z}$ so that ϕ is well defined. Also, if $(a,b),(c,d) \in \mathbb{Z} \oplus \mathbb{Z}$, then $\phi(a,b) + \phi(c,d) = [a\phi(1,0) + b\phi(0,1)] + [c\phi(1,0) + d\phi(0,1)] = (a+c)\phi(1,0) + (b+d)\phi(0,1) = \phi((a,b) + (c,d))$, and $\phi(a,b)\phi(c,d) = [a\phi(1,0) + b\phi(0,1)][c\phi(1,0)d\phi(0,1)] = a\phi(1,0)c\phi(1,0) + ad\phi(1,0)\phi(0,1)bc\phi(0,1)\phi(1,0) + bd\phi(0,1)\phi(0,1) = ac\phi(1,0) + bd\phi(0,1) = \phi(ac,bd) = \phi((a,b)(c,d))$.

4. Let $A = \langle x^4 + x + 1 \rangle$ in $\mathbb{Z}_2[x]$.

   (a) Show that $\mathbb{F} = \mathbb{Z}_2[x]/A$ is a field.

   Solution. We need to show that $f(x) = x^4 + x + 1$ is irreducible. Clearly, $f(0) = f(1) = 1$. So, $f(x)$ has no linear factor. Suppose $f(x)$ has a quadratic factor $g(x) = x^2 + bx + c$.

Then $c = 1$. So, $g(x) = x^2 + 1$ or $g(x) = x^2 + x + 1$. Now, $f(x) = (x^2 + 1)^2 + x$ and $f(x) = (x^2 + x + 1)(x^2 + x + 1) + 1$. Hence, $f(x)$ is irreducible and $\mathbb{Z}_2[x]/A$ is a field.

(b) Pair up all the elements in $(\mathbb{F}^*, \cdot)$ that are multiplicative inverses of each other.

Solution. We have the following pairs of mutually inverse elements: $(1+A, 1+A), (x+A, 1+x^3+A), (x^2+A, 1+x^2+x^3+A), (x^3+A, 1+x+x^2+x^3+A), (1+x+A, x+x^2+x^3+A), (x+x^2+A, 1+x+x^2+A), (x+x^3+A, x^2+x^3+A), (1+x^2+A, 1+x+x^3+A)$.

Common mistakes. Write elements in $\mathbb{F}^*$ as polynomials $1, x$ instead of $1 + A, x + A$, etc.

(c) Determine all the generators (with explanation) of the group $(\mathbb{F}^*, \cdot)$.

Solution. Note that $(x + A)^3 = x^3 + A \neq 1 + A$ and $(x + A)^5 = x^5 + A = x(x + 1) + A = x^2 + x + A \neq 1 + A$. We see that $(x + A)$ has order 15, and is a generator.

Common mistake. Just say $(x + A)^5 \neq 1 + A$ without explanation.

Furthermore, $(x+A)^m$ is a generator if and only $\gcd(m, 15) = 1$. So, $x+A$, $(x+A)^2 = x^2+A$, $(x+A)^4 = 1+x+A$, $(x+A)^7 = 1+x+x^3+A$, $(x+A)^8 = 1+x^2+A$, $(x+A)^{11} = x+x^2+x^3+A$, $(x + A)^{13} = 1 + x^2 + x^3 + A$, $(x + A)^{14} = a + x^3 + A$ are all the generators.

Common mistake. Just say that $(x + A)^m$ is a generator if $\gcd(m, 15) = 1$ without even writing down what the values m are.

5. Let $p > 2$ be a prime number.

(a) Show that $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ defined by $\phi(x) = x^2$ is a homomorphism with $\ker(\phi) = \{1, -1\}$, and deduce that $H = \phi(\mathbb{Z}_p^*)$ has $(p - 1)/2$ elements.

Solution. Evidently, if $a = b$ then $a = b + kp$ and $\phi(a^2) = (b + kp)^2 = b^2 + 2bp + b^2p^2 = b^2$ so that ϕ is well defined. Further, $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$ for any $a, b \in \mathbb{Z}_p^*$. So, ϕ is a well-defined homomorphism on $(\mathbb{Z}_p^*, \cdot)$.

Note that $x \in \ker(\phi)$ if and only if $x^2 = 1$. The only solutions for the quadratic polynomial $x^2 - 1$ in the field $\mathbb{Z}_p$ is ± 1, i.e., 1 and $p - 1$. Thus, $\phi(\mathbb{Z}_p^*)$ is isomorphic to $\mathbb{Z}_p^*/\{1, p - 1\}$ has $(p - 1)/2$ elements.

Common mistakes. Forget to check that ϕ is well defined; no justification for no other $r \in \ker(\phi)$ besides $1, -1$.

(b) Show that there is $a \in \mathbb{Z}_p$ such that $a^2 \in \{-1, 2, -2\}$, i.e., the subgroup H in (a) contains an element in $\{-1, 2, -2\}$.

Solution. Let $\mathbb{Z}_p^*/H = \{H, rH\}$ has order 2. If -1 or -2 is in H, then we have $a \in \mathbb{Z}_p^*$ such that $\phi(a) = a^2 = -1$ or -2. If $-1, -2 \notin H$, then $(-1)H = (-2)H = rH$. So, $2H = (-1)H(-2)H = rHrH = r^2H = H$. Thus, $2 \in H$ and there is $a \in \mathbb{Z}_p^*$ such that $a^2 = 2$.

(c) Show that $x^4 + 1 \in \mathbb{Z}_p[x]$ is reducible.

If there is $a^2 = -1$, then $(x^2 + a)(x^2 - a) = x^4 + 1$.

If there is $a^2 = -2$, then $(x^2 + ax - 1)(x^2 - ax - 1) = x^4 - (2 + a^2)x^2 + 1 = x^4 + 1$.

If there is $a^2 = 2$, then $(x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1 = x^4 + 1$.

(d) Show that $x^4 + 1$ is reducible in $\mathbb{Z}_2[x]$.

We have $(x^2 + 1)(x^2 - 1) = x^4 + 1$.

Math 307 Final Examination In class part **Name: Sample solution**

1. Show that if G is a group with no proper non-trivial subgroup and has at least two elements, then G is isomorphic to $\mathbb{Z}_p$ for some prime number p.

   Solution. Let $a \in G$ not equal to e. Then $H = \langle a \rangle \neq \{e\}$. So, $G = \langle a \rangle$ is cyclic. If $|a|$ is infinite, then $\langle a^2 \rangle$ is a proper subgroup of G, which is a contradiction. If $|a| = n$, then it must be a prime; else $\langle a^k \rangle$ will be a proper subgroup of G for any proper factor k of n. So, G is isomorphic to $\mathbb{Z}_n$ for a prime n.

   Common mistake. Forget to discuss the case when $|a|$ is infinite.

2. Let $\phi : G_1 \to G_2$ be a group homomorphism, and H be a normal subgroup of G_1.

   (a) Show that $\phi(H)$ is a normal subgroup of $\phi(G_1)$.

   Solution. It is known that subgroups of G_1 are mapped to subgroups of G_2.

   So, $\phi(H), \phi(G_1)$ are subgroups of G_2. Evidently, $\phi(H) \subseteq \phi(G_1)$. Note that $\phi(e_1) = e_2 \in \phi(H) \subseteq G_2$ so that $\phi(H)$ is non-empty. If $y_1, y_2 \in \phi(H)$, then there are $h_1, h_2 \in H$ such that $\phi(h_1) = y_1$ and $\phi(h_2) = y_2$. So, $y_1^{-1} y_2 = \phi(h_1)^{-1} \phi(h_2) = \phi(h_1^{-1} h_2) \in \phi(H)$ as $h_1^{-1} h_2 \in H$. Let $H = G_1$. We see that $\phi(G_1)$ is a subgroup of G_2.

   Clearly, $\phi(H) \subseteq \phi(G_1)$. To show that $\phi(H)$ is a normal subgroup of $\phi(G_1)$, suppose $y \in \phi(H)$ and $z \in \phi(G_1)$. Then there are $h \in H$ and $g \in G_1$ such that $\phi(h) = y$ and $\phi(g) = z$. Thus $zyz^{-1} = \phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$ as $ghg^{-1} \in H$. So, $\phi(H)$ is a normal subgroup of $\phi(G_1)$.

   Common mistake. Forget to mention or check that $\phi(H)$ is a subgroup of $\phi(G_1)$. Forget to pick $y \in \phi(H)$ and $z \in \phi(G_1)$ to check the condition $zyz^{-1} \in \phi(H)$.

   (b) Give an example to show that $\phi(H)$ may not be a normal subgroup of G_2.

   Solution. For example, let $H = G_1 = \mathbb{Z}_2$ and $G_2 = S_3$. Define $\phi : G_1 \to G_2$ by $\phi(1) = (1, 2)$, the transposition. Then $\phi(H) = \{(1, 2), \varepsilon\}$, where ε is the identity in S_3, is not normal in G_2 because $(1, 3)\phi(H) = \{(1, 2, 3), \varepsilon\} \neq \{(1, 3, 2), \varepsilon\} = \phi(H)(1, 3)$.

3. Let $R_1 = \{a + i\sqrt{2}b : a, b \in \mathbb{Z}\}$.

   (a) Show that R_1 is a subring of $\mathbb{C}$.

   Solution. Let $0 = 0 + i\sqrt{2}0 \in R_1$. So, R_1 is nonempty. If $z_1 = a_1 + i\sqrt{2}b_1, z_2 = a_2 + i\sqrt{2}b_2 \in R_1$, then $z_1 - z_2 = (a_1 - a_2) + \sqrt{2}(b_1 - b_2) \in R_1$, and $z_1 z_2 = (a_1 a_2 - 2b_1 b_2) + \sqrt{2}(a_1 b_2 + a_2 b_1) \in R_1$. So, R_1 is a subring.

   (b) Show that R_1 is isomorphic to $R_2 = \left\{ \begin{pmatrix} a & b \\ -2b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

   Solution. Clearly, $\phi(z) \in R_2$ for every $z \in R_1$. So, ϕ is well-defined.

   1-1: If $f(z_1) = f(z_2) = \begin{pmatrix} a & b \\ -2b & a \end{pmatrix}$, then $z_1 = z_2 = a + \sqrt{2}bi$.

   Onto: For any $A = \begin{pmatrix} a & b \\ -2b & a \end{pmatrix} \in R_2$, we have $z = a + i\sqrt{2}b \in R_1$ satisfying $\phi(z) = A$.

Operation preserving. For any $z_1 = a_1 + \sqrt{2}b_1 i, z_2 = a_2 + i\sqrt{2}b_2 \in R_1$ so that $z_1 z_2 = (a_1a_2 - 2b_1b_2) + \sqrt{2}(a_1b_2 + a_2b_1)$, we have $\phi(z_1) = A_1 = \begin{pmatrix} a_1 & b_1 \\ -2b_1 & a_1 \end{pmatrix}$ and $\phi(z_2) = A_2 = \begin{pmatrix} a_2 & b_2 \\ -2b_2 & a_2 \end{pmatrix}$. Then $\phi(z_1) + \phi(z_2) = A_1 + A_2 = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -2b_1 - 2b_2 & a_1 + a_2 \end{pmatrix} = \phi(z_1 + z_2)$ and $\phi(z_1)\phi(z_2) = A_1A_2 = \begin{pmatrix} a_1a_2 - 2b_1b_2 & a_1b_2 + a_2b_1 \\ -2(a_1b_2 + a_2b_1) & a_1a_2 - 2b_1b_2 \end{pmatrix} = \phi(z_1z_2)$. The result follows.

Remark This is a straight forward problem. One does not need to check that R_2 is a subring. The result will imply that R_2 is isomorphic to R_1 and hence is a subring.

Undesirable mistake. One consider $z = a + i\sqrt{2}b$, z^{-1}, $\phi(z)^{-1}$, etc. and gave some wrong formula and cause some unnecessary deduction of points.

4. (a) Show that $R_1 = \{(a, a) : a \in \mathbb{Z}\}$ is a subring, but not an ideal of $\mathbb{Z} \oplus \mathbb{Z}$.

   Solution. Clearly, $(0, 0) \in R_1$ is non-empty. If $(a, a), (b, b) \in R_1$, then $(a, a) - (b, b) = (a - b, a - b) \in R_1$ and $(a, a)(b, b) = (ab, ab) \in R_1$. So, R_1 is a subring.

   Now, $(1, 1) \in R_1$ and $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$, but $(1, 1)(1, 0) = (1, 0) \notin R_1$. So, R_1 is not an ideal.

   (b) Show that $R_2 = \{(3a, 5b) : a, b \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z} \oplus \mathbb{Z}$, but not a prime ideal.

   Solution. Clearly, $(0, 0) \in R_2$ is non-empty. If $(3a, 5b), (3c, 5d) \in R_2$ and $(f, g) \in \mathbb{Z} \oplus \mathbb{Z}$, then $(3a, 5b) - (3c, 5d) = (3(a - c), 5(b - d) \in R_2$ and $(3a, 5b)(f, g) = (3af, 5bg) \in R_2$. So, R_2 is an ideal.

   Now, $(1, 0), (0, 1)$ do not belong to R_2, but their product $(0, 0)$ lies in R_2. So, R_2 is not a prime ideal.

5. Show that $A = \{f(x) \in \mathbb{Z}[x] : f(1) = 0\}$ is a prime ideal but not a maximal ideal of $\mathbb{Z}[x]$.

   Solution. Clearly, the zero polynomial $g(x) = 0$ lies in A so that A is nonempty.

   If $a(x), b(x) \in A$, then $a(1) = b(1) = 0$. So, $a(1) - b(1) = 0$. Furthermore, for any $a(x) \in A$ and $c(x) \in \mathbb{Z}[x]$, $a(1)c(1) = 0$ so that $a(x)c(x) \in A$. So, A is an ideal.

   Suppose $c(x), d(x) \in \mathbb{Z}[x]$ satisfy $c(x)d(x) \in A$. Then $c(1)d(1) = 0$ so that $c(1) = 0$ or $d(1) = 0$. Hence, $c(x)$ or $d(x)$ lies in A. We see that A is a prime ideal.

   Now, $g(x) \in A$ if and only if $g(1) = 0$, i.e., $(x - 1)$ is a factor of $g(x)$. So, $A = \{(x - 1)q(x) : q(x) \in \mathbb{Z}[x]\}$. For any $h(x) \in \mathbb{Z}[x]$, we have $h(x) = (x - 1)q(x) + h(1)$ with $c = h(1) \in \mathbb{Z}$ by the factor theorem. So, $\mathbb{Z}[x]/A = \{c + A : c \in \mathbb{Z}\}$. Now, if $2 + A \in \mathbb{Z}[x]/A$, there is no $c + A$ such that $(2 + A)(c + A) = 2c + A = 1 + A$. So, $\mathbb{Z}[x]/A$ is not a field, i.e., A is not maximal.

   Common mistake To construct an ideal B lying strictly between A and $\mathbb{Z}[x]$, one needs to give the detailed explanation that B is an ideal, $A \neq B$ and $B \neq \mathbb{Z}[x]$. In fact, some examples were given that B is not an ideal, $B = A$ or $B = \mathbb{Z}[x]$.