Math 307 Final Examination (In class part) **Name: Sample Solution**

1. Suppose the group G has order pq, where p and q are prime numbers.

   (a) Show that $Z = \{g \in G : gx = xg \ \forall x \in G\}$ is a normal subgroup of G.

   (b) Show that $Z = \{e\}$ or $Z = G$.

   Solution. (a) Clearly, $eg = ge$ for all $g \in G$. So, $e \in G$. If $a, b \in Z$, then $(ab)g = agb = g(ab)$ for all $g \in G$. So, $ab \in Z$. Also, if $a \in Z$, then $ag = ga$ for all $g \in G$ so that $ga^{-1} = a^{-1}aga^{-1} = a^{-1}gaa^{-1} = a^{-1}g$. Thus, $a^{-1} \in Z$. Thus, Z is a subgroup.

   Note that $aZ = \{ag : g \in Z\} = \{ga : g \in Z\} = Za$ for any $a \in G$. Thus, left coset is always a right coset, and hence Z is normal.

   Suppose $|Z|$ is neither 1 nor pq. We may assume that $|Z| = p$. Otherwise, change the roles of p and q. Then $|G/Z| = q$. Thus, both Z and G/Z is cyclic. Suppose $Z = \langle a \rangle$ and $G/Z = \langle bZ \rangle$ so that

   $$G = \cup_{i=1}^{q} b^i Z = \cup_{i=1}^{q} \{b^i a^j : j = 1, \ldots, p\} = \{b^i a^j : 1 \le i \le q, 1 \le j \le p\}.$$

   Suppose $x, y \in G$, $x = b^i a^j$ and $y = b^r a^s$. Because $a, a^2, \ldots, a^j \in Z$ will commute with all elements in G, we have $xy = b^i a^j b^r a^s = b^{i+r} a^{j+s} = b^r a^s b^i a^j = yx$. Thus, G is Abelian, and $|Z| = pq$, which contradicts $|Z| = p$.

   Remark Assume $Z = \langle a \rangle$ has p elements and $G/\langle a \rangle = \langle bZ \rangle$.

   1. One needs to use the fact that $G = \cup_{j=1}^{q} b^j \langle a \rangle$ to justify that
   $$G = \{b_j a_i : 1 \le j \le q, 1 \le i \le p\}.$$
   2. Also, $G/\langle a \rangle = \langle bZ \rangle$ does not imply $|b| = q$ immediately. Here, one can only say that $b^q \in \langle a \rangle$. More arguments are needed to deduce that $|b| = q$.

2. (a) Let R be a commutative ring with no zero divisor. If $r \in R$ is nonzero such that $r^3 = r$, show that $r^2 a = a$ for every $a \in R$, and conclude that r^2 is not the unity of R.

   (b) Find a nonzero element $r \in \mathbb{Z}_{14}$ such that $r^3 = r$ and that r^2 is the unity.

   Solution. (a) Note that for any $a \in R$, we have $r^3 a = ra$ so that $r(r^2 a - a) = 0$. Since $r \neq 0$, we see that $ar^2 = r^2 a = a$. Hence, r^2 is a/the unity in R.

   (b) If $r = [6]$ then $r^3 = [36][6] = [8][6] = [48] = [6] = r$. Clearly, $[6] \neq [1]$.

3. An element a in a commutative ring R is nilpotent if $a^n = 0$ for some positive integer n.

   (a) Prove that $A = \{a \in R : a \text{ is nilpotent}\}$ is an ideal.

   (b) Prove that R has no non-zero nilpotent element if and only if the equation $x^2 = 0$ has no nonzero solution in R.

   Solution. (a) Evidently, $0 \in A$.

   If $a, b \in A$ such that $a^n = 0, b^m = 0$, then

   $$(a-b)^{m+n} = \sum_{j=0}^{m} \binom{m+n}{j} (a)^j (-b)^{m+n-j} + \sum_{j=m+1}^{m+n} \binom{m+n}{j} (a)^j (-b)^{m+n-j} = 0 + 0 = 0$$

because $a^j = 0$ for $j > m$, and $b^{m+n-j} = 0$ for $j \leq m$. Thus, $a - b \in A$.

Finally, if $a \in A$ and $c \in R$ such that $a^n = 0$, then $(ac)^n = a^n c^n = 0$. Thus, $ac \in A$.

Combining, A is an ideal.

Remark Here, many forget to check that $A \neq \emptyset$. Also, some forgot to check that $a, b \in A$ implies $a - b \in A$.

(b) If there is a nonzero nilpotent element $a \in R$, then $a^n = 0$ for some positive integer n and $a^{n-1} \neq 0$. Clearly, $n > 1$. Else, we have a nonzero a such that $a^1 = 0$, which is absurd. Let $b = a^{n-1} \neq 0$. Then $b^2 = a^{2n-2} = a^n a^{n-2} = 0$. Thus, $x^2 = 0$ has a nonzero solution b.

Conversely, if R has a nonzero x such that $x^2 = 0$, then x is nonzero nilpotent element in R.

4. Let $\mathbb{F}$ be a finite field such that the Abelian group $(\mathbb{F}^*, \cdot)$ has n elements. Suppose the $(\mathbb{F}^*, \cdot)$ is isomorphic to $\mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{m_r}}$, where $p_1, \ldots, p_r$ are prime numbers.

   (a) If $k = \text{lcm}(p_1^{m_1}, \ldots, p_r^{m_r})$, show that $a^k = 1$ for every $a \in \mathbb{F}^*$.

   (b) Use the fact that a degree ℓ polynomial in $\mathbb{F}[x]$ has at most ℓ zeros to deduce that $k = n$ and

   that $\mathbb{F}^*$ is cyclic.

   Solution. (a) Suppose $\phi : \mathbb{F}^* \to \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{m_r}}$ is an isomorphism. Then $\phi(a) = (a_1, \ldots, a_r)$ for some $(a_1, \ldots, a_r) \in \mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{m_r}}$. The order of $|a_j| = \gamma_j$ is a factor of $p_r^{m_r}$. Thus, the $\text{lcm}(\gamma_1, \ldots, \gamma_r)$ is a factor of $\text{lcm}(p_1^{m_1}, \ldots, p_r^{m_r})$. Thus, $|a| = |\phi(a)| = |(a_1, \ldots, a_r)|$ is a factor of $\text{lcm}(p_1^{m_1}, \ldots, p_r^{m_r}) = k$. So, $a^k = 1$.

   (b) By (a), every $a \in \mathbb{F}^*$ satisfies the equation $x^k - 1 = 0$. It follows that $k \geq |\mathbb{F}^*$. Clearly, we have $p_1^{m_1} \cdots p_r^{m_r} \geq \text{lcm}(p_1^{m_1}, \ldots, p_r^{m_r})$. So, we have

$$p_1^{m_1} \cdots p_r^{m_r} = k = |\mathbb{F}^*| = \text{lcm}(p_1^{m_1}, \ldots, p_r^{m_r}).$$

   Thus, $p_1, \ldots, p_r$ are distinct, and $(1, \ldots, 1)$ has order $p_1^{m_1} \cdots p_r^{m_r}$ will be a generator of the group $\mathbb{Z}_{p_1^{m_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{m_r}}$. Thus, $\phi(\mathbb{F})$ is cyclic and so is $\mathbb{F}^*$

   Remark Here, many forget to justify why $\mathbb{F}^*$ is cyclic after showing that $k = n$.

MATH 307 Final Examination (Take home component).

1. Let R_1 and R_2 be rings, and $\phi : R_1 \to R_2$ be a ring homomorphism. **Prove or disprove** the following.

   (a) If A is an ideal of R_1, then $\phi(A)$ is an ideal in R_2.

   (b) If B is an ideal of R_2, then $\phi^{-1}(B) = \{a \in R_1 : \phi(a) \in B\}$ is an ideal of R_1.

   Solution. (a) False. Let $R_1 = \mathbb{Z}$ and $R_2 \in \mathbb{Q}$ and $\phi : R_1 \to R_2$ be defined by $\phi(x) = x$. Then $A = R_1$ is an ideal and $\phi(R) = \mathbb{Z}$ is not an ideal of R_2. Say, $1 \in \phi(R_1) = \mathbb{Z}$ and $x = 1/2 \in R_2$, but $1 \cdot x \notin \phi(R_1)$.

   (b) True. If B is an ideal of R_1. Then $\phi(0) = 0 \in B$ so that $0 \in \phi^{-1}(B)$ is non-empty. For any $a, b \in \phi^{-1}(B)$, we have $\phi(a), \phi(b) \in B$. Then $\phi(a-b) = \phi(a)-\phi(b) \in B$ so that $a-b \in \phi^{-1}(B)$. Also, if $a \in \phi^{-1}(B)$ and $b \in R_1$, then $\phi(ab) = \phi(a)\phi(b) \in B$ and $\phi(ba) = \phi(b)\phi(a) \in B$. So, $ab, ba \in \phi^{-1}(B)$. So, $\phi^{-1}(B)$ is an ideal in R_1.

   Remark Here many forgot to check that $\phi^{-1}(B) \neq \emptyset$. Some forgot to check $a, b \in \phi^{-1}(B)$ implies that $a - b \in \phi^{-1}(B)$.

2. Let $\mathbb{D}$ be an integral domain with unity 1.

   (a) Show that $\tilde{\mathbb{D}} = \{r \cdot 1 : r \in \mathbb{Z}\}$ is a subdomain of $\mathbb{D}$, **and** $\tilde{\mathbb{D}}$ is contained in every subdomain of $\mathbb{D}$. (Make sure that that subdomain has same unity.)

   (b) Show that the characteristic of any subdomain of $\mathbb{D}$ is the same as that of $\mathbb{D}$.

   Solution. (a) Note that if r is a positive integer, then $r \cdot 1 = 1 + \cdots + 1$ for r times, $(-r) \cdot 1 = (-1) + \cdots + (-1)$ for r times, and $0 \cdot 1 = 0$, the additive identity of $\mathbb{D}$. Clearly, $0 \in \tilde{\mathbb{D}}$ is non-empty. If $a = m \cdot 1, b = n \cdot 1 \in \tilde{\mathbb{D}}$, then $a - b = (m - n) \cdot 1 \in \tilde{\mathbb{D}}$, and $ab = (mn) \cdot 1 \in \tilde{\mathbb{D}}$. Furthermore, $\tilde{\mathbb{D}}$ contains 1. Because $\mathbb{D}$ is commutative and has no zero divisors, $\tilde{\mathbb{D}}$ behaves the same. Thus, $\tilde{\mathbb{D}}$ is an integral domain, and is a subdomain of $\mathbb{D}$.

   Now, any subdomain S of $\mathbb{D}$ is a commutative subring with identity, say, $1'$. But $1\dot{1}'$ in $\mathbb{D}$ and $1' \cdot 1' = 1'$ in $\tilde{\mathbb{D}}$. So, $1' \cdot 1' = 1 \cdot 1'$, i.e., $(1 - 1') \cdot 1'$ Because $\mathbb{D}$ has no zero divisor, we see that $1 = 1'$. So, S contains 1 and the subgroup generated by 1. Thus, $\tilde{\mathbb{D}} \subseteq S$.

   Remark Here, many forgot to justify why the unity in any subdomain must be 1. Note that the unity of a subring can be different from the parent ring in general. For example, $(1, 1)$ is the unity of $\mathbb{Z} \oplus \mathbb{Z}$, and $(1, 0)$ is the unity of the subring $S = \mathbb{Z} \oplus \{0\} = \{(z, 0) : z \in \mathbb{Z}\}$.

   (b) Note that the characteristic of $\mathbb{D}$ is the order of the unity 1. By (a), we have show that the unity in any subdomain is the same as that of $\mathbb{D}$. Thus, the order of the unity in the subdomain is the same as that of $\mathbb{D}$. So, it has the same characteristic as the original domain.

3. Let $\mathbb{F}$ be a fields. Suppose $f(x) \in \mathbb{F}[x]$, and $A = \langle f(x) \rangle = \{f(x)h(x) : h(x) \in \mathbb{F}[x]\}$.

   (a) If $f(x) \in \mathbb{F}[x]$ is reducible[1], show that the factor ring $\mathbb{F}[x]/A$ is **not** an integral domain. (It follows that $\mathbb{F}[x]/A$ is not a field.)

   (b) Suppose $f(x)$ is irreducible. Show that A is an maximal ideal.

[1] That is, $f(x) = f_1(x)f_2(x)$ such that $f_1(x), f_2(x)$ has degrees strictly smaller than that of $f(x)$.

(It follows that $\mathbb{F}[x]/A$ is a field.)

Solution. (a) If $f(x) = f_1(x)f_2(x)$ of lower degrees in $\mathbb{F}[x]$, then $f_1(x)+A, f_2(x)+A \in \mathbb{F}[x]/A$ is not $0 + A$. But $(f_1(x) + A)(f_2(x) + A) = f(x) + A = A$. So, $\mathbb{F}[x]/A$ has zero divisor, and is not an integral domain.

(b) If $f(x)$ is irreducible, and if $A \subseteq B \subseteq \mathbb{F}[x]$ for some proper ideal B of $\mathbb{F}[x]$ not equal to A, then we can let $g(x) = g_0 + \cdots + g_m x^m \in B$ with **minimum** positive degree. Then every polynomial of B is a multiple of $g(x)$, else, there is $h(x) \in B$ such that $h(x) = g(x)q(x)+r(x)$ with $r(x) = h(x) - g(x)q(x) \in B$ having a degree smaller than that of $g(x)$. In particular, $f(x) \in A \subseteq B$ has the form $f(x) = g(x)q(x)$. As $f(x)$ is irreducible, then $q(x) = q_0$ is a constant polynomial with $q_0 \neq 0$. But then $g(x) = f(x)/q_0 \in A$ so that $B = \langle g(x)\rangle \subseteq A$, which is a contradiction. So, there cannot be a proper ideal B containing A and not equal to A. Hence, A is a maximal ideal.

Remark Here many forgot to justify that $q(x)$ cannot be a constant polynomial.

4. Let $A = \langle x^2 + 1\rangle \subseteq \mathbb{Z}_3[x]$, and $\mathbf{E} = \mathbb{Z}_3[x]/A$.

   (a) Show that $f(x) = x^2 + 1$ is irreducible. [Only need to show that $f(a) \neq 0$ for all $a \in \mathbb{Z}_3$.]

   (b) Determine (with proof) all the generators of the cyclic group $(\mathbb{E}^*, \dot{)}$.

   (c) Find the inverse of $2x + 1 + A$ in $\mathbb{E}$.

   Solution. (a) If $f(x)$ is reducible, it is a product of two linear factors. But $f(0) \neq 0$, $f(1) \neq 0$, and $f(2) \neq 0$. So, $f(x)$ has no linear factor, and hence $f(x)$ is irreducible.

   (b) Note that $\mathbb{E} = \{ax+b+A : a, b \in \mathbb{Z}_3$ has 9 elements so that $\mathbb{E}^*$ has 8 elements. So, $(\mathbb{E}^*, \cdot)$ is isomorphic to $(\mathbb{Z}_8, +)$, and has 4 generators. Now, $1 + A$ has order 1, $2 + A$ has order 2, $(x+A)^4 = x^4+A = 1+A$, $(2x+A)^4 = 1+A$. Thus, $x+1+A, x+2+A, 2x+1+A, 2x+2+A$ are elements in $(\mathbb{E}^*, \cdot)$ of order 8 that will generate $\mathbb{E}^*$.

   (c) Note that $(2x + 1 + A)(2x + 2 + A) = x^2 + 2 + A = 1 + A$. So, $2x + 2 + A$ is the inverse of $2x + 1 + A \in \mathbb{E}^*$.