Nathan Bickel
MATH 701: Section 001
Professor: Dr. Tsai
December 11, 2024

MATH 701 Final Exam

Problem 1 Let $M = (2, x)$ be the ideal in $\mathbb{Z}[x]$ generated by 2 and x. Prove that M cannot be generated by a single element.

Suppose (toward contradiction) that $M = \big(a(x)\big)$ for some $a(x) \in \mathbb{Z}[x]$. Since we have $2 \in M$, there exists some $p(x) \in \mathbb{Z}[x]$ such that $2 = p(x)a(x)$. Since the degree of $p(x)a(x)$ is the degree of $p(x)$ plus the degree of $a(x)$, and 2 has degree 0, $p(x)$ and $a(x)$ also have degree 0 and thus we have that $p(x)$ and $a(x)$ are constant. Since 2 is prime, we have $a(x) \in \{1, -1, 2, -2\}$.

Case 1: $a(x) \in \{1, -1\}$. Then $a(x) \in M$, so by definition of M we have $a(x) = 2p(x) + xq(x)$ for some $p(x), q(x) \in \mathbb{Z}[x]$. But $xq(x)$ has degree 1 for any choice of $q(x)$ other than $q(x) = 0$, so we must have $a(x) = 2p(x)$ as $a(x)$ has degree 0. So $p(x) \in \{-\frac{1}{2}, \frac{1}{2}\}$, a contradiction.

Case 2: $a(x) \in \{2, -2\}$. We have $x \in M = \big(a(x)\big)$, and thus $x = a(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. But then $2 \mid x$, a contradiction. $\square$

Problem 2 Let R be a commutative ring. Recall that the radical of an ideal I is the set

$$\sqrt{I} := \{a \in R : a^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 1}\}.$$

(i) Prove that $\sqrt{I}$ is an ideal.

(ii) Prove, for two ideals I and J, that $\sqrt{I} + \sqrt{J} \subseteq \sqrt{I + J}$.

(iii) Do we always have $\sqrt{I} + \sqrt{J} = \sqrt{I + J}$? Prove or find a counterexample.

(i) First, we note that $I \subseteq \sqrt{I}$ since for all $a \in I$ we have $a^1 \in I$. So $\sqrt{I}$ is non-empty.

Now, let $a, b \in \sqrt{I}$. We will show that $a - b \in \sqrt{I}$. Let $m, n \in \mathbb{Z}_{\geq 1}$ such that $a^m \in I$ and $b^n \in I$. Since $(-b)(-b) = b^2$ is true for all rings, we have $(-b)^n \in \{b^n, -b^n\} \subseteq I$. From the binomial theorem, we have that

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

For each k, we either have $k \geq m$ or $m + n - k \geq n$, so either a^k or $(-b)^{m+n-k}$ are in I by closure of multiplication. Thus, each term of the sum is in I by closure of multiplication, so the sum is in I by closure of addition. Thus, $(a - b)^{m+n} \in I$ and so $a - b \in \sqrt{I}$.

Finally, let $a \in \sqrt{I}$ and $r \in R$. We will show that $ra \in \sqrt{I}$. Let $n \in \mathbb{Z}_{\geq 1}$ such that $a^n \in I$. Since R is commutative, we have $(ra)^n = r^n a^n$, so $(ra)^n \in I$ since I is an ideal. Thus, $ra \in \sqrt{I}$.

Therefore, $\sqrt{I}$ is an ideal. $\square$

(ii) Let $x \in \sqrt{I} + \sqrt{J}$. Then $x = a + b$ for some $a \in \sqrt{I}$, $b \in \sqrt{J}$. Let $m, n \in \mathbb{Z}_{\geq 1}$ such that $a^m \in I$ and $b^n \in J$. Then, we can use the binomial theorem to write

$$x^{m+n} = (a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}.$$

Let

$$\alpha := \sum_{k=m}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}, \ \beta := \sum_{k=0}^{m-1} \binom{m+n}{k} a^k b^{m+n-k}.$$

Clearly, $x^{m+n} = \alpha + \beta$. Each term in α has $k \geq m$, so $a^k \in I$ and thus each term is in I by closure of multiplication. By closure of addition, $\alpha \in I$. By the same reasoning, $\beta \in J$. So $x^{m+n} = \alpha + \beta \in I + J$, and therefore $x \in \sqrt{I+J}$. $\square$

(iii) Consider $R = \mathbb{Z}[x]$ and the ideals $I = (x^2+2)$ and $J = (2x-1)$ of R. Then,

$$(x+1)^2 = x^2 + 2x + 1 = (x^2+2) + (2x-1) \in I + J,$$

so $x+1 \in \sqrt{I+J}$. However, because x^2+2 and $2x-1$ are irreducible polynomials, we have that $\sqrt{I} = I$ and $\sqrt{J} = J$. It can then be shown that $x + 1 \notin I + J = \sqrt{I} + \sqrt{J}$. Therefore, $\sqrt{I+J} \neq \sqrt{I} + \sqrt{J}$.$\square$

Problem 3 Suppose p and $p+2$ are primes. Classify groups of order $p^3 + 2p^2$ up to isomorphism.

We claim the two groups of order $p^3 + 2p^2$ up to isomorphism are $Z_{p^3+2p^2}$ and $Z_p \times Z_{p^2+2p}$. In particular, we claim that if G is an order $p^3 + 2p^2$ group and has an element of order $p^3 + 2p^2$, then $G \cong Z_{p^3+2p^2}$, and otherwise $G \cong Z_p \times Z_{p^2+2p}$.

Proof. Let G be a group with $|G| = p^3 + 2p^2 = p^2(p+2)$. By Sylow's theorem, we have $n_p \equiv 1 \pmod{p}$, and since $n_p \mid p+2$ we clearly have $n_p = 1$. We also have $n_{p+2} \equiv 1 \pmod{p+2}$ and $n_{p+2} \mid p^2$. So $n_{p+2} \in \{1, p, p^2\}$.

Case 1: $n_{p+2} = p$. Then $p \equiv 1 \pmod{p+2}$, so $p = 1 + k(p+2)$ for some $k \in \mathbb{N}$. This implies $p - pk = 1 + 2k$, so $p = \frac{1+2k}{1-k}$. Thus we must have $k = 0$, so $p = 1$, contradicting the primality of p.

Case 2: $n_{p+2} = p^2$. Then $p^2 \equiv 1 \pmod{p_2}$, so $p^2 = 1 + k(p+2)$ for some $k \in \mathbb{N}$. Then we have

$$\begin{aligned} p^2 - 4 &= k(p+2) - 3 \\ \implies (p+2)(p-2) &= k(p+2) - 3 \\ \implies p - 2 &= \frac{k(p+2) - 3}{p+2} \\ \implies p - 2 &= k - \frac{3}{p+2} \\ \implies p + 2 &= 3 && (\tfrac{3}{p+2} \in \mathbb{Z} \text{ so } (p+2) \mid 3) \\ \implies p &= 1, \end{aligned}$$

contradicting the primality of p.

Therefore, $n_{p+2} = 1$. So G has one subgroup P of order p^2 and one subgroup Q of order $p+2$. Also, we have $G \cong PQ$ since $|G| = |P| \cdot |Q|$. By Lagrange, every element in P will have order 1, p, or p^2, and every element in Q will have order 1 or $p+2$. So the subgroups are disjoint except for e and we have $P \cap Q = \{1\}$. Thus, we have $G \cong PQ \cong P \times Q$.

We proved in class that the only groups of order p^2 up to isomorphism are $Z_p \times Z_p$ and Z_{p^2}. The only group of order $p+2$ is Z_{p+2} since $p+2$ is prime. Thus, the two possibilities for G are $(Z_p \times Z_p) \times Z_{p+2}$ and $Z_{p^2} \times Z_{p+2}$, which are isomorphic to $Z_{p(p+2)} = Z_{p^2+2p}$ and $Z_{p^2(p+2)} = Z_{p^3+2p^2}$ respectively by the Chinese Remainder Theorem. $\square$

Problem 4

(i) Is the following statement true or false? "If H and K are normal subgroups of a finite group G, with $H \cong K$, then $G/H \cong G/K$."

(ii) Let G be a group of order p^n for some p and let H be a normal subgroup of G, with $H \neq \{1\}$. Prove that $Z(G) \cap H \neq \{1\}$, where $Z(G)$ is the center of G.

(i) The statement is false. For example, consider $G := \mathbb{Z}_4 \times \mathbb{Z}_2$, and the subgroups $H := \langle (2,0) \rangle$ and $K := \langle (0,1) \rangle$. The subgroups are normal since G is abelian, and they are isomorphic since they are both cyclic with order 2. We have

$$G/H := \{H, (1,0)+H, (0,1)+H, (1,1)+H\},\ G/K := \{K, (1,0)+K, (2,0)+K, (3,0)+K\}.$$

It is evident that $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $G/K \cong \mathbb{Z}_4$, so $G/H \ncong G/K$ (the latter is cyclic but the former is not). $\square$

(ii) Since $H \trianglelefteq G$, H is equal to the union of some set $U := \{\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_m\}$ of conjugacy classes of G. For each $h \in H$, the conjugacy class of h has cardinality $|G : C_G(h)|$. Since $C_G(h) \leq G$, by Lagrange we have $|C_G(h)| = p^i$ for some $i \in \mathbb{N}$ and thus the size of the conjugacy class of h is $|G : C_G(h)| = p^{n-i}$. Since $H \neq \{1\}$, by Lagrange we have $|H| = p^k$ for some $k \geq 1$. Thus, we have

$$p^k = |H| = |\mathcal{K}_1| + |\mathcal{K}_2| + \cdots + |\mathcal{K}_m| = p^{i_1} + p^{i_2} + \cdots + p^{i_m}$$

for some $i_1, i_2, \ldots, i_m \in \mathbb{N}$. The $\mathcal{K}_t$ that contains 1 will have $|\mathcal{K}_t| = 1$, so we have $i_j < k$ for all $j \in [m]$. Thus, by prime number properties, there must be another conjugacy class in U with size 1. The element in this conjugacy class is necessarily in $Z(G)$, and therefore we have $Z(G) \cap H \neq \{1\}$. $\square$

Problem 5 Let $M_2(\mathbb{Q})$ be the ring of 2×2 matrices with rational entries. Let R be the set of matrices in $M_2(\mathbb{Q})$ that commute with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

(i) Prove that R is a subring of $M_2(\mathbb{Q})$.

(ii) Prove that R is isomorphic to the ring $\mathbb{Q}[x]/(x^2)$.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix that commutes with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then we have

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

From $a = a+c$, we have $c = 0$, and from $a+b = b+d$ we have $a = d$. It is easy to check that all matrices of this form do commute with the matrix, so

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}.$$

(i) Clearly $I_2 \in R$, so $R \neq \emptyset$. Now let $X = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, Y = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in R$. It is clear that

$$X - Y = \begin{pmatrix} a-c & b-d \\ 0 & a-c \end{pmatrix} \in R$$

based on our characterization, as well as

$$XY = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in R.$$

So R is a subring. $\square$

(ii) Let $\varphi : R \to \mathbb{Q}[x]/(x^2)$ be defined by, for all $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$,

$$\varphi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \overline{a + bx}.$$

Now let $X = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, Y = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in R$. We have

$$\begin{aligned}
\varphi(X+Y) &= \varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) \\
&= \varphi \begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix} \\
&= \overline{(a+c)+(b+d)x} \\
&= \overline{a+bx} + \overline{c+dx} \\
&= \varphi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \varphi \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \\
&= \varphi(X) + \varphi(Y).
\end{aligned}$$

and

$$\begin{aligned}
\varphi(XY) &= \varphi\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) \\
&= \varphi \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \\
&= \overline{ac + (ad+bc)x} \\
&= \overline{ac + adx + bcx + bdx^2} && (\text{“unquotienting” by } (x^2)) \\
&= \overline{(a+bx)(c+dx)} \\
&= \left(\overline{a+bx}\right)\left(\overline{c+dx}\right) \\
&= \varphi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \varphi \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \\
&= \varphi(X)\varphi(Y).
\end{aligned}$$

So φ is a homomorphism.

For any $p(x) \in \mathbb{Q}[x]/(x^2)$, any terms of degree 2 or higher can be written as a multiple of x^2, so we can write $p(x)$ in the form $a + bx$. Thus, $\varphi(R) = \mathbb{Q}[x]/(x^2)$. Clearly, we have

$$\ker\varphi = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\} = \{0_R\}.$$

So using the First Isomorphism Theorem for Rings, we can write

$$R \cong R/\{0_R\} \cong \varphi(R) = \mathbb{Q}[x]/(x^2).$$

$\square$