SOLUTIONS FOR MIDTERM EXAM

一、(15') (a) State the third Sylow Theorem.

(b) Classify groups of order 10, and write down their class equations.

Solution: (a) Let $|G| = n = p^e m$, $p \not| m$. The number $s(p)$ of Sylow p-subgroups of G divides m and is congruent to 1 modulo p.

(b) See the homework for the proof that a group of order $2p$, with p a prime, is either C_{2p} or D_p. For $p = 5$, their class equations are

$$1 + 1 + \cdots + 1 \quad \text{and} \quad 1 + 2 + 2 + 5.$$

respectively. □

二、(15') (a) Show that the following two elements in S_7 are conjugate, and find their orders.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$$

(b) Does S_7 contain an element of order 14? Does S_7 contain a subgroup of order 14? Explain why.

Solution: (a) Their cycle decompositions are $(246)(1357)$ and $(123)(4567)$, which have the same pattern. The order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition, hence these two elements have the same order 12.

(b) From the above description of order, S_7 does not contain an element of order 14. It contains a subgroup of order 14 isomorphic to D_7: let x be the 7-cycle (1234567) and $y = (17)(26)(35)$, then $x^7 = y^2 = 1$ and $yxy = x^{-1}$. □

三、(10') Prove that a group of order $2n$, where n is odd, contains a subgroup of index 2. (Hint: Cayley's Theorem)

Solution: By Cayley's Theorem, the action of G on itself by left multiplication embeds G as a subgroup of S_{2n}. Let $N = A_{2n} \cap G$. Then G/N is a subgroup of S_{2n}/A_{2n}, hence it has order 1 or 2. Take an element $a \in G$ of order 2, and representatives $b_1, \ldots, b_n$ of the cosets $G/\langle a \rangle$, so that $G = \{b_1, ab_1, \ldots, b_n, ab_n\}$. Then the left multiplication by a on G is a product of n transpositions, hence is an odd permutation. Thus $G \neq N$, i.e. N is a subgroup of index 2 in G. □

四、(15') (a) Prove that the following formula defines a group action of $\mathrm{SL}_2(\mathbb{R})$ on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\ z > 0\}$

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathcal{H} \to \mathcal{H}, \quad z \mapsto \frac{az+b}{cz+d}.$$

(b) Prove that this action is transitive, and find the stabilizer of $i \in \mathcal{H}$.

Solution: (a) We first show that if $z \in \mathcal{H}$ then $g \cdot z \in \mathcal{H}$ as well. This follows from

$$\mathrm{Im}\ g \cdot z = \frac{\det g}{|cz+d|^2} \mathrm{Im}\ z = \frac{1}{|cz+d|^2} \mathrm{Im}\ z > 0.$$

Clearly $I \cdot z = z$. Finally, take another $g' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Then

$$g \cdot (g' \cdot z) = \frac{a\frac{a'z+b}{c'z+d'} + b}{c\frac{a'z+b}{c'z+d'} + d} = \frac{(aa'+bc')z + ab + bd'}{(ca'+dc')z + cb + bd'} = (gg') \cdot z.$$

This verifies the group action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$.

(b) For any $z = x + yi \in \mathcal{H}$, the matrix $g = \begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ takes i to z, hence the action is transitive. The stabilizer of i is

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \mid 0 \le \theta < 2\pi \right\}. \quad \square$$

五、(15') An ideal I of a ring R is called a prime ideal if $I \neq R$ and $ab \in I$, $a, b \in R$ implies that either $a \in I$ or $b \in I$.

(a) Prove that I is a prime ideal if and only if R/I is an integral domain.

(b) Prove that a maximal ideal is a prime ideal.

(c) Prove that $p \in R$ is a prime element if and only if the principal ideal (p) is a prime ideal.

Solution: (a) For $r \in R$, write $\bar{r}$ for the image of r in R/I. Then I is a prime ideal if and only if $\overline{ab} = 0$ implies that $\bar{a} = 0$ or $\bar{b} = 0$ if and only if R/I is an integral domain.

(b) If I is maximal, then R/I is a field. In particular it is a domain hence I is a prime ideal by (a).

(c) A non-unit element p is a prime element if and only if $p|ab$ implies that $p|a$ or $p|b$ if and only if $ab \in (p)$ implies that $a \in (p)$ or $b \in (p)$ if and only if (p) is a prime ideal. $\square$

六、(15') (a) An element a of a ring R is nilpotent if $a^n = 0$ for some $n > 0$. Prove that if $a \in R$ is nilpotent, then $R[x]/(ax-1)$ is the zero ring.

(b) Describe the ring $\mathbb{Z}[x]/(x^2+x)$.

Solution: (a) If $a^n = 0$, then $(1-ax)(1 + ax + a^2x^2 + \cdots + a^{n-1}x^{n-1}) = 1 - a^nx^n = 1$, hence $1 - ax$ is a unit of $R[x]$, which implies that $R[x]/(ax-1)$ is the zero ring.

(b) Write $\bar{x}$ for the image of x in $R := \mathbb{Z}[x]/(x^2+x)$. Then $e = \bar{x}$ and $e' = 1 - \bar{x}$ are idempotents of R, which implies that

$$R \cong eR \times e'R \cong \mathbb{Z} \times \mathbb{Z}. \quad \square$$

七、(15') Let p be a prime number and A be an $n \times n$ integer matrix such that $A^p = I$ but $A \neq I$. Prove that $n \geq p-1$. Given examples for $n = p-1$ and $n = p$ respectively.

Solution: Let $f(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of A. From $A^p = 1$ we know that each eigenvalue of A is a p-th root of unity. If all the eigenvalues of A are equal to 1, then from $A^p = I$ it follows that $A = I$. Thus, A has an eigenvalue ζ which is a primitive p-th root of unity. Then ζ is a root of the cyclotomic polynomial $x^{p-1} + \cdots + 1$ which is irreducible. Since $\mathbb{Z}[x]$ is a UFD, we have $(x^{p-1} + \cdots + 1) | f(x)$, hence $n \geq p-1$.

If $n = p-1$, we may take

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 \\ -1 & -1 & -1 & \cdots & -1 \end{pmatrix}_{(p-1)\times(p-1)}$$

If $n = p$, we may take

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}_{p\times p}$$

$\square$