SOLUTION TO MIDTERM EXAM

Problem 1. Find a primitive root of $(\mathbb{Z}/37\mathbb{Z})^\times$.

Proof. 2 is a primitive root of $(\mathbb{Z}/37\mathbb{Z})^\times$. Check that $2^{18} \neq 1 \pmod{37}$ and $2^{12} \neq 1 \pmod{37}$. □

Problem 2. Is 30 a quadratic residue modulo 157?

Proof. Using reciprocity law, we have

$$(\frac{30}{157}) = (\frac{2}{157})(\frac{3}{157})(\frac{5}{157}) = (-1)^{(157^2-1)/8}(\frac{157}{3})(\frac{157}{5}) = -(\frac{1}{3})(\frac{2}{5}) = 1.$$

□

Problem 3. Find a polynomial $f \in \mathbb{Z}[x,y,z]$ such that

$$f(x,y,z) \equiv x \pmod 3, f(x,y,z) \equiv y \pmod 5, f(x,y,z) \equiv z \pmod{13}$$

for all $x, y, z \in \mathbb{Z}$.

Proof. Choose $f(x,y,z) = ax + by + cz$, such that

$$\begin{array}{lll} a \equiv 1 \pmod 3 & b \equiv 0 \pmod 3 & c \equiv 0 \pmod 3 \\ a \equiv 0 \pmod 5 & b \equiv 1 \pmod 5 & c \equiv 0 \pmod 5 \\ a \equiv 0 \pmod{13}, & b \equiv 0 \pmod{13}, & c \equiv 1 \pmod{13}. \end{array}$$

For example, we can choose $f(x,y,z) = 130x + 156y + 105z$. □

Problem 4. Determine $n \in \mathbb{Z}$ such that the congruences $5x - y \equiv 2 \pmod n$ and $4x + 3y \equiv 2 \pmod n$ are solvable.

Proof.

$$\begin{cases} 5x - y \equiv 2 \pmod n \\ 4x + 3y \equiv 2 \pmod n \end{cases} \Leftrightarrow \begin{cases} 5x - y \equiv 2 \pmod n \\ x - 4y \equiv 0 \pmod n \end{cases}$$

$$\Leftrightarrow \begin{cases} 19y \equiv 2 \pmod n \\ x - 4y \equiv 0 \pmod n \end{cases}.$$

So these equations are solvable if and only if $19 \nmid n$. □

Problem 5. Give a definition of a *field*.

Proof. Omitted. □

Problem 6. Determine the centralizer of the matrix $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/3\mathbb{Z})$.

Proof. Assume $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in the centralizer of $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, and then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We get $a = d$ and $c = 0$. So the centralizers are

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/3\mathbb{Z}) : a = d, c = 0 \right\}.$$

□

Problem 7. Let $N \subset G$ be a normal subgroup, with $|N| = 17$ and $|G|$ an odd integer. Show that N is contained in the center $Z(G)$ of G.

Proof. Since N is normal, for any $g \in G$, $\sigma_g : h \mapsto ghg^{-1}$ is an automorphism on N, and then $\varphi : g \mapsto \sigma_g$ is a group homomorphism from G to $Aut(N)$.

$N \cong C_{17}$ is cyclic and assume h is a generator of N, then any automorphism of N can be uniquely determined by the map $h \mapsto h^k$ for $1 \leq k \leq 16$. So $|Aut(N)| = 16$. $\varphi(G) = G/ker(\varphi)$ is a subgroup of $Aut(N)$, a quotient group of G. So $|\varphi(G)|$ divides both $|Aut(N)|$ and G, and thus $|\varphi(G)| = 1$, which means $\sigma_g = id$ for any $g \in G$. □

Problem 8. How many elements of order 3 could be contained in a group of order 30?

Proof. Assume n is the number of 3-Sylow subgroups. By Sylow's theorem $n \equiv 1 \pmod 3$ and $n|10$, and then $n = 1$ or 10.

If $n = 1$, there is only 1 subgroup of order 3 and 2 elements of order 3. In C_{30}, we have 2 elements of order 3.

Now we prove n cannot be 10. If $n = 10$, there are 20 elements of order 3. By Sylow's theorem we have 1 subgroup N_5 of order 5 and it is normal. Pick a subgroup G_3 of order 3, then using the normality of N_5 we can show N_5G_3 is a subgroup of order 15.

By a result in class $N_5G_3 \cong C_{15}$. So there are $\phi(15) = 2 \times 4 = 8$ elements in N_5G_3 of order 15, and 4 elements of order 5. So the total number of elements $\geq 20 + 8 + 4 = 32 > 30$, contradictory. □

Problem 9. Exhibit a subgroup of the symmetric group $\mathfrak{S}_7$ which is nonabelian and of order 21.

Proof. Assume G is the wanted subgroup of order 21. By Sylow's theorem there exists a normal subgroup N_7 of order 7. W.L.O.G, we may assume $N_7 =< (1234567) >$. Since G is nonabelian, G does not have elements of order 21, so there are $21 - 7 = 14$ elements of order 3.

Assume $g \in G$ and is order of 3, then g is of form (abc) or $(abc)(def)$, and $g(1234567)$ is of order 3. By trial and error we find $g = (142)(563)$ satisfies such condition and

$$g(1234567)g^{-1} = (1357246) = (123456)^2.$$

Then we can prove if $G_3 =< g >$, $G_3 N_7$ forms a subgroup of $\mathfrak{S}_7$. $\square$

Problem 10. Let G be a group of order 39. Show that G is generated by two elements x, y, with relations $x^{13} = y^3 = 1$, $yxy^{-1} = x^r$, for some $r, 1 \leq r \leq 13$. Which r are possible?

Proof.

$$x = y^3 x y^{-3} = y^2 x^r y^{-2} = y(yxy^{-1})^r y^{-1} = yx^{r^2} y^{-1} = x^{r^3}.$$

So $x^{r^3-1} = e$ and $13 | r^3 - 1$, and so $r = 1$ or 3 or 9.

Now we construct G realizing $r = 1, 3, 9$. Using prime root in module 13, we can prove $Aut(C_{13}) = C_{12}$. Assume $C_{13} =< g >$ and $C_3 =< h >$ and there are 3 different homomorphisms $\varphi_0, \varphi_1, \varphi_2$ from C_3 to $Aut(C_{13})$ which map h to $id, (g \mapsto g^3), (g \mapsto g^9)$ respectively.

Given φ_i, we define the semi-direct product on set $C_{13} \times C_3$ as follows

$$(g^a, h^b) \times_i (g^c, h^d) = (g^a(\varphi_i(h)^b(g))^c, h^{b+d}).$$

We can straightforward verify that $(C_{13} \times C_3, \times_i)$ forms a group, and if we let $x = (g, e), y = (e, h)$, we have $x^{13} = y^3 = 1$, $yxy^{-1} = x^{3^i}$. $\square$