MATH 251: ABSTRACT ALGEBRA I
EXAM #1

Problem 1(a). Compute the inverse of 15 in the group $(\mathbb{Z}/127\mathbb{Z})^\times$.

Solution. We have $127 = 8(15)+7$ and $15 = 2(7)+1$, so indeed $\gcd(15, 127) = 1$, and undoing these steps, we have $1 = 15 - 2(7) = 15 - 2(127 - 8(15)) = 17(15) - 2(127)$, so $15^{-1} \equiv 17 \pmod{127}$.

Problem 1(b). Determine if the group $(\mathbb{Z}/12\mathbb{Z})^\times$ is cyclic. Justify your answer.

Solution. Not cyclic: $(\pm 1)^2 \equiv (\pm 5)^2 \equiv 1 \pmod{12}$, so no element generates $(\mathbb{Z}/12\mathbb{Z})^\times$.

Problem 2(a). Let $H = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \text{ not both zero} \right\} \subset M_2(\mathbb{R})$. Show that $H \subset GL_2(\mathbb{R})$.

Solution. We have $\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 \neq 0$ whenever a, b are not both zero.

Problem 2(b). Show that H is a subgroup of $GL_2(\mathbb{R})$.

Solution. Clearly, $H \neq \emptyset$. We have

$$AB = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{pmatrix} \in H$$

and $\det(AB) \neq 0$ so $AB \neq 0$ and hence H is closed under multiplication. Finally,

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in H$$

so H is closed under inverses. Hence H is a subgroup.

Problem 3(a). What is the largest order of an element $\sigma \in S_5$?

Solution. The order of $\sigma \in S_5$ is the lcm of the lengths of its cycles in its cycle decomposition. The sum of the cycle lengths is 5 (including 1-cycles), so the possibilities for the cycle lengths are $5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1$, and so the largest order is $6 = 3 \cdot 2$.

Problem 3(b). Show that the groups D_{60} and S_5 are not isomorphic.

Solution. The element $r \in D_{60}$ has order 30, but S_5 has no element of order 30 by (a), so $D_{60} \not\cong S_5$. Or $\#S_5 = 120 \neq 60 = \#D_{60}$, which also implies $D_{60} \not\cong S_5$.

Problem 4. Let G be a group. Let $a, g \in G$, and suppose that a has order $n \in \mathbb{Z}_{>0}$. Prove that gag^{-1} has order n.

Solution. Let $k \in \mathbb{Z}$. Then $(gag^{-1})^k = (gag^{-1}) \cdots (gag^{-1}) = ga^k g^{-1}$. Therefore $(gag^{-1})^k = 1$ if and only if $ga^k g^{-1} = 1$; multiplying by g^{-1} on the left and g on the right, this holds if and only if $a^k = g^{-1} g = 1$. Since a has order n, we see that $a^k \neq 1$ for $0 < k < n$ and $a^n = 1$, and the same holds for gag^{-1}; hence gag^{-1} has order n.

Problem 5. A group G is called *triplic* if for all $x \in G$, we have $x^3 = 1$. Let $\phi : G \to H$ be an injective homomorphism of groups. Show that if H is triplic, then G is triplic.

Solution. Let $x \in G$. Then $\phi(x^3) = \phi(x)^3$ since ϕ is a homomorphism, and $\phi(x)^3 = 1$ since $\phi(x) \in H$ and H is triplic. But $\phi(1) = 1$ so $\phi(x^3) = \phi(1) = 1$; since ϕ is injective, we have $x^3 = 1$, so G is triplic.

Date: 8 October 2007.