PROBLEM SET 7

HAMID SAGBAN

Exercise 1. *Find all subgroups of* $(\mathbb{Z}_{13}^*, \times_{13})$.

Solution. We know $|(\mathbb{Z}_{13}^*, \times_{13})| = \varphi(13) = 12$. Also, the factors of 12 are $1, 2, 3, 4, 6,$ and 12. We now form the 6 cyclic subgroups of $\mathbb{Z}_{13}^*$. For the factors 1 and 12, we have $12 = 12 \times 1$, and thus $< \bar{2}^{12} >= \{\bar{1}\}$, and $< \bar{2}^1 >= \mathbb{Z}_{13}^*$. Now for the factors 6 and 2, we have $12 = 6 \times 2$, and thus $< \bar{2}^2 >= \{\bar{2}^2, \bar{2}^4, \bar{2}^6, \bar{2}^8, \bar{2}^{10}, \bar{2}^{12}\} = \{\bar{4}, \bar{3}, \bar{12}, \bar{9}, \bar{10}, \bar{1}\}$, and $< \bar{2}^6 >= \{\bar{2}^6, \bar{2}^{12}\} = \{\bar{12}, \bar{1}\}$. Finally, for the factors 4 and 3, we have $12 = 4 \times 3$, and thus $< \bar{2}^3 >= \{\bar{2}^3, \bar{2}^6, \bar{2}^9, \bar{2}^{12}\} = \{\bar{8}, \bar{12}, \bar{5}, \bar{1}\}$, and $< \bar{2}^4 >= \{\bar{2}^4, \bar{2}^8, \bar{2}^{12}\} = \{\bar{3}, \bar{9}, \bar{1}\}$. $\square$

Exercise 2. *Let* $n \geq 3$. *Show that* $[n-1] \in (U(\mathbb{Z}_n), \times_n)$ *is an element of order 2.*

Proof. To show that $[n-1] \in U(\mathbb{Z}_n)$, it suffices to show that $\gcd(n, n-1) = 1$. Let k be a divisor of n. Then $n = mk$ for some positive integer m. Thus $n - 1 = mk - 1$, and hence k cannot be a divisor of $n-1$, for otherwise $n - 1 = rk$ for some $r \in \mathbb{Z}^+$, so that $n = rk + 1$, contradiction. Thus $\gcd(n, n-1) = 1$. Since $n \geq 3$, we know $[n-1] \neq [1]$. So we compute $(n-1)^2 \bmod n$; we have $(n-1)(n-1) = (n(n-2)+1) \equiv 1 \bmod n$, since $n(n-2) \equiv 0 \bmod n$. Thus $[n-1]^2 = [1]$, and $|[n-1]| = 2$. $\square$

Exercise 3. *Show that* $(U(\mathbb{Z}_{35}), \times_{35})$ *is not a cyclic group. (Hint: find elements in* $U(\mathbb{Z}_{35})$ *that have order 2)*

Proof. We know by (3) that there is an element of order 2 in $U(\mathbb{Z}_{35})$, namely $[35-1] = [34]$. Therefore, we can form a cyclic subgroup of order 2; that is, $< \bar{34} >= \{\bar{34}, \bar{1}\}$. If $U(\mathbb{Z}_{35})$ is cyclic, then there is exactly one cyclic subgroup of order 2. But it turns out that the order of $\bar{6} = 2$; so $< 6 >= \{\bar{6}, \bar{1}\}$. We have found two distinct cyclic subgroups of order 2 in $U(\mathbb{Z}_{35})$, thus $U(\mathbb{Z}_{35})$ cannot be cyclic. $\square$

Exercise 4. *We know that* $(\mathbb{Z}_{47}^*, \times_{47})$ *is a cyclic group. Show that there are as many elements of order 23 as there are elements of order 46.*

Proof. We know there exist cyclic subgroups of orders 1,2,23, and 46. Let b be an element of order 46. Then for all $k < 46$ such that $\gcd(46, k) = 1$, $|b^k| = \frac{46}{\gcd(k,46)} = 46$. There are $\varphi(46) = 22$ such k's and thus 22 elements of order 46. Now let a be an element of order 23. We know $|a^n| = \frac{23}{\gcd(n,23)} = 23$ for all $n < 23$; there are $\varphi(23) = 22$ such n's and thus 22 elements of order 23.

□

Exercise 5. *Let $\alpha \in S_{99}$ such that $|\alpha| = 99$. Show that α^{66} is either a 3-cycle or the composition of disjoint 3-cycles.*

Proof. $|\alpha^{66}| = \frac{99}{\gcd(66,99)} = 3$. Permutations of order 3 can be obtained by 3-cycles, since the order of a 3-cycle is 3. One can also get cycles of order 3 by setting $\operatorname{lcm}(a, b, \ldots, n) = 3$, where $a, b, \ldots, n$ are orders of some disjoint cycles ($\neq (1)$) whose composition equate to α. Thus $a, b, \ldots, n$ must all be 3 for this to be satisfied since 3 is a prime number. □

Exercise 6. *Let $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z}_{23} \right\}$. It is easy to see that $(S, \times_{23})$ is a monoid. Note that $\times_{23}$ is the normal multiplication of matricies modulo 23. Let $U(S)$ be the set of all invertible elements of S under $\times_{23}$. Thus we know $(U(S), \times_{23})$ is a group. Find $|U(S)|$, and explain whether U(S) is an abelian or a non-abelian group.*

Solution. All arithmetic operations are modulo 23, so the subscripts indicating this are absent. We begin by showing that S is a monoid; we first show closure. Take two elements $\alpha, \beta \in S$. Then $\alpha = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ and $\beta = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$, for a, b, c and $x, y, z \in \mathbb{Z}_{23}$. Computing $\alpha\beta$, we get $\alpha\beta = \begin{bmatrix} ax & ay + bz \\ 0 & cz \end{bmatrix}$, with $ax, ay + bz, cz \in \mathbb{Z}_{23}$. Thus $\alpha\beta \in S$. We claim that $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. This can easily be seen by taking $\alpha \in S$, and computing αe and $e\alpha$. Therefore, S is a monoid. Now, we describe the group $U(S)$; that is, $U(S) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid \gcd(a, 23) = \gcd(b, 23) = 1,\ a, b, c \in \mathbb{Z}_{23} \right\}$. Note that a, c cannot be $[0]$ by the gcd criterion. Take $\alpha \in U(S)$, thus $\alpha = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ for $a, b, c \in \mathbb{Z}_{23}$, and with $\gcd(a, 23) = \gcd(c, 23) = 1$. a^{-1}

can be easily verified to be $\begin{bmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$, and invertibility of a and c is guaranteed since a, c are relatively prime to 23. The order of $U(S)$ is thus $\varphi(23) \times \varphi(23) \times 23 = 22 \times 22 \times 23$. $U(S)$ is clearly nonabelian for take $\alpha = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$. Then $\alpha\beta = \begin{bmatrix} 1 & 8 \\ 0 & 3 \end{bmatrix}$ and $\beta\alpha = \begin{bmatrix} 1 & 4 \\ 0 & 3 \end{bmatrix}$. □

Exercise 7. *Let* $a = \begin{bmatrix} 2 & 18 \\ 0 & 7 \end{bmatrix}$. *Then* $a \in S$. *Is* $a \in U(S)$*? If yes, then find* a^{-1}. *Note that* S *and* $U(S)$ *are as defined previously.*

Solution. $a \in U(S)$ since $\gcd(2, 23) = \gcd(7, 23) = 1$. We can use the form described above for the inverse to find a^{-1}, which is $\begin{bmatrix} 12 & 2 \\ 0 & 10 \end{bmatrix}$. □

Exercise 8. *Let* $M = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\}$. *It is easy to see that* $(M, \times)$ *is a monoid. Note that* $\times$ *is the normal multiplication of matricies. Let* $U(M)$ *be the set of all invertible elements of* S *under* $\times$. *Thus we know* $(U(M), \times)$ *is a group. Is* $U(M)$ *an abelian or a nonabelian group? If* $\alpha \in U(M)$*, find a general form of* α. *Let* $a = \begin{bmatrix} 2 & 18 \\ 0 & 7 \end{bmatrix}$. *Then* $a \in M$. *Is* $a \in U(M)$*? If yes, then find* a^{-1}.

Solution. $U(M)$ is not abelian, for take $\alpha = \begin{bmatrix} 1 & 5 \\ 0 & -1 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}$. Then $\alpha\beta = \begin{bmatrix} 1 & 9 \\ 0 & -1 \end{bmatrix}$ and $\beta\alpha = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$. Now a general form of α is $\begin{bmatrix} \pm 1 & b \\ 0 & \pm 1 \end{bmatrix}$ with $b \in \mathbb{Z}$. Thus clearly, a as given in the last part of the question does not belong to $U(M)$. □