Prof. Alexandru Suciu

MATH 3175 **Group Theory** **Summer 2, 2022**

Solutions for Assignment 3

---

1. Let $G = \langle a \rangle$ be a finite cyclic group of order n.

(i) For an element $a^k \in G$ with $0 < k < n$, show that the order of a^k is equal to the order of the cyclic subgroup $\langle a^k \rangle$.

Set $m \coloneqq \operatorname{ord}(a^k) = \min\{r > 0 : a^{kr} = e\}$. By definition, $\langle a^k \rangle$ is the subgroup of G consisting of all the powers of a^k. Since $a^m = e$, we have

$$\langle a^k \rangle = \{e, a^k, a^{2k}, \dots, a^{(m-1)k}\}.$$

We need to show that $\left|\langle a^k \rangle\right| = m$; that is, that there are no repetitions in the displayed list. Suppose there was such a repetition, i.e., $a^{ks} = a^{kt}$, for some $0 \le s, t \le m-1$ with, say, $s < t$. Then $a^{(t-s)k} = e$, and since $0 < t - s < m$, this contradicts the fact that $m = \operatorname{ord}(a)$.

(ii) Show that $\langle a^k \rangle = \{a^{ks} : s \in \mathbb{Z}\} = \{a^{ks+nt} : s, t \in \mathbb{Z}\}$.

By Lagrange's theorem, the order of a divides $|G| = n$; thus, $a^n = e$, and the claim follows at once.

(iii) Let $d = \gcd(n, k)$. Use parts (i) and (ii) to show that $\operatorname{ord}(a^k) = n/d$.

Since d is the gcd of n and k, there exist integers s_0, t_0 such that $ks_0 + nt_0 = d$. Therefore, by part (ii), we have that $a^d \in \langle a^k \rangle$; hence, $\langle a^d \rangle \subseteq \langle a^k \rangle$. On the other hand, since $d \mid k$, we also have $k = dr$, for some $r > 0$. Thus, $a^k = (a^d)r \in \langle a^d \rangle$, and hence $\langle a^k \rangle \subseteq \langle a^d \rangle$. Therefore, we have that $\langle a^k \rangle = \langle a^d \rangle$, and so, by part (i) with $k \to d$, we have that m must be equal to $\operatorname{ord}(a^d) = \left|\langle a^d \rangle\right|$.

Now observe that $(a^d)^{n/d} = a^n = e$, and so $m = \operatorname{ord}(a^d)$ must divide n/d. On the other hand, $a^{km} = (a^k)^m = e$; thus, since $\operatorname{ord}(a) = n$, we must have $n \mid km$. Therefore, since $n = \gcd(n, k)$, properties of the gcd imply that $n/d \mid (k/d)m$. But, since $\gcd(n/d, k/d) = 1$, this implies $n/d \mid m$. Putting things together, we conclude that $m = n/d$.

2. Let G be a cyclic group of size at least 3.

(i) Show that G has at least 2 distinct generators.

Since, by assumption, G is a non-trivial cyclic group, we have that $G = \langle a \rangle$, for some $a \in G$, $a \ne e$. Since, in fact, $|G| \ge 3$, we must have $a \ne a^{-1}$. Indeed, otherwise we would have $a^2 = 1$, and so $G = \{e, a\}$, a contradiction. Finally, note that $a = (a^{-1})^{-1}$, which implies $\langle a^{-1} \rangle = \langle a \rangle = G$. Thus, we have showed G has two distinct generators, namely, a and a^{-1}.

(ii) If G is finite, show that G has an even number of distinct generators.

Set $n = |G|$. By the above, if a is a generator of G, so is a^{-1}, and $a \ne a^{-1}$. Likewise, if $a^k \in G$ is any other generator, distinct from $a^{\pm 1}$, then $a^k \ne a^{-k}$. Proceeding in this fashion, we see that the set of generators of G is a list the form $\{a^{\pm 1}, a^{\pm k}, \dots\}$, with no repetitions in it. Hence, this set has even size.

Alternatively, we know that the set of generators of G is in bijection with the set $A = \{k \in \mathbb{Z} : 0 < k < n \text{ and } \gcd(k, n) = 1\}$. This set is the union of two disjoint subsets, $A^+ = \{k \in A : k < n/2\}$ and $A^- = \{\ell \in A : \ell > n/2\}$. Since $\gcd(n, k) = \gcd(n, n-k)$, the correspondence $k \leftrightarrow \ell = n - k$ is a bijection between A^+ and A^-. Therefore, $|A^+| = |A^-|$, and so $|A|$ is even.

Note: What we have proved here is that the Euler totient function $\varphi(n)$ takes only even values for $n \ge 3$.

3. For each of the following groups, find all their cyclic subgroups:

(i) $\mathbb{Z}_{14}^{\times} = \{1, 3, 5, 9, 11, 13\}$ is cyclic of order 6, generated by 3. Thus, all its subgroups are cyclic; the complete list consists of 4 subgroups: $\{1\}$, $\langle 13\rangle = \{1, 13\}$, $\langle 9\rangle = \{1, 9, 11\}$, and $\langle 3\rangle = \mathbb{Z}_{14}^{\times}$.

(ii) $\mathbb{Z}_{20}^{\times} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ has 6 cyclic subgroups: $\{1\}$, $\langle 9\rangle = \{1, 9\}$, $\langle 11\rangle = \{1, 11\}$, $\langle 19\rangle = \{1, 19\}$, $\langle 3\rangle = \{1, 3, 9, 7\}$, and $\langle 13\rangle = \{1, 13, 9, 17\}$.

4. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8. Find all the subgroups of Q_8 and draw the corresponding lattice of subgroups.

The subgroups of Q_8 are: $\{1\}$, $\{\pm 1\}$, $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$, $\mathbb{Q}_8$.

5. Let $H = \{(x, y) \in \mathbb{R}^2 : x + y = 0\}$.

(i) Sketch H in the plane.

H is a line of slope -1 going through the origin.

(ii) Consider $\mathbb{R}^2$ as a group under vector addition. Show that H is a subgroup of $\mathbb{R}^2$. Is H commutative?

If $v_1 = (x_1, y_1)$ and $v_2 = (x_2, y_2)$ are both in H, then $v_1 - v_2 = (x_1 - x_2, y_1 - y_2)$ is also in H, since $(x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2) = 0 + 0 = 0$. Thus, H is a subgroup of $\mathbb{R}^2$. Since $\mathbb{R}^2$ is commutative, H is also commutative.

(iii) Describe the cosets of H in geometric terms and make a sketch of a few of the cosets.

The (right) cosets of H are of the form $H + v$, where $v = (v_1, v_2)$ is an arbitrary vector in $\mathbb{R}^2$. That is, they are all the (parallel) lines in $\mathbb{R}^2$ of slope -1.

6. Let S_4 be the group of permutations of the set $\{1, 2, 3, 4\}$. Consider the subgroup H generated by the cyclic permutation $(1\ 2\ 3\ 4) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$.

(i) Write down all the right cosets and all the left cosets of H in S_4.

Right cosets:

$$\begin{aligned}
H &= \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \\
H \cdot (1,2) &= \{(2,3,4), (1,2), (1,3,2,4), (1,4,3)\} \\
H \cdot (2,3) &= \{(2,3), (1,2,4,3), (1,3,4), (1,4,2)\} \\
H \cdot (1,4) &= \{(2,4,3), (1,2,3), (1,3,4,2), (1,4)\} \\
H \cdot (2,4) &= \{(2,4), (1,2)(3,4), (1,3), (1,4)(2,3)\} \\
H \cdot (3,4) &= \{(3,4), (1,2,4), (1,3,2), (1,4,2,3)\}
\end{aligned}$$

Left cosets:

$$\begin{aligned}
H &= \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \\
(1,2) \cdot H &= \{(2,3,4), (1,3,2,4), (1,4,3), (1,2)\} \\
(2,3) \cdot H &= \{(2,3), (1,3,4), (1,2,4,3), (1,4,2)\} \\
(1,4) \cdot H &= \{(2,4,3), (1,4), (1,2,3), (1,3,4,2)\} \\
(2,4) \cdot H &= \{(2,4), (1,4)(2,3), (1,3), (1,2)(3,4)\} \\
(3,4) \cdot H &= \{(3,4), (2,3,1,4), (4,3,1,2), (1,3,2)\}
\end{aligned}$$

(ii) What is the index of H in S_4?

$[S_4 : H] = \#\{\text{right cosets}\} = \#\{\text{right cosets}\} = |S_4| \,/\, |H| = 6.$