MATH 111A HOMEWORK 3 SOLUTIONS

4) If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of Section 1.]

Solution. We shall use the following facts (see p. 25 of the textbook):

$$|r| = n \qquad r^i s = sr^{-i} \quad \text{for } 0 \leq i \leq n-1 \qquad D_{2n} = \{1, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}.$$

(We will prove this without using Exercise 33.) There are three things to prove.

(1) r^k has order 2: Notice that $(r^k)^2 = r^n = 1$ and $r^k \neq 1$ because $|r| = n$. It follows that $|r^k| = 2$.

(2) r^k commutes with all elements in D_{2n} : Clearly

$$(r^k)(r^i) = r^{k+i} = r^{i+k} = (r^i)(r^k)$$

for all $i = 0, 1, ..., n-1$. On the other hand, for $0 \leq i \leq n-1$ we have

$$\begin{aligned}
(r^k)(sr^i) &= (r^k s)(r^i) \\
&= (sr^{-k})(r^i) \qquad (\text{since } r^k s = sr^{-k}) \\
&= (sr^k)(r^i) \qquad (r^{2k} = 1 \text{ implies } r^k = r^{-k}) \\
&= (sr^i)(r^k) \qquad (r^k r^i = r^i r^k)
\end{aligned}$$

and so r^k commutes with all of the sr^i also. Thus, r^k commutes with every element in D_{2n}.

(3) r^k is the only nonidentity element in D_{2n} which commutes with all elements in D_{2n} : Suppose that $x \in D_{2n}$ and $x \neq 1$. If $x = r^i$, $1 \leq i \leq n-1$ and $i \neq k$, then x does not commute with s, for otherwise

$$r^i s = sr^i = r^{-i} s \implies r^i = r^{-i} \implies r^{2i} = 1.$$

This implies $2i \geq n$ since $|r| = n$. Now, observe that $r^{2i-n} = 1$ also, but

$$n \leq 2i \leq 2n - 2 \implies 0 \leq 2i - n \leq n - 2.$$

So, by definition of the order of r, we deduce that $2i - n = 0$ and so $i = k$, which is a contradiction. On the other hand, if $x = sr^i$, $1 \leq i \leq n-1$, then x does not commute with r, for otherwise

$$\begin{aligned}
& (r)(sr^i) = (sr^i)(r) \\
\implies \; & sr^{-1}r^i = sr^i r \qquad (rs = sr^{-1}) \\
\implies \; & r^{i-1} = r^{i+1} \\
\implies \; & r^2 = 1.
\end{aligned}$$

But $|r| = n \geq 4$ so we have a contradiction. Therefore, indeed r^k is the only nonidentity element that commutes with all elements in D_{2n}.

14) Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be true if p is not prime.

Solution. Since id does not have order p and the cycle decomposition of id is not a product of p-cycles, we do not have to consider id in our proof. So let $\sigma \in S_n \backslash \{id\}$ and $\sigma = \sigma_1 \cdots \sigma_r$ be its cycle decomposition, with $l_i = |\sigma_i| \geq 2$ for every i (we need $\sigma \neq id$ in order to have this). Then, we know that

$$|\sigma| = \text{lcm}\{l_1, ..., l_r\}.$$

Now suppose that σ has order p. Then $p = \text{lcm}\{l_1, ..., l_r\}$, and so $l_i = p$ for all i, since p is prime and $l_i \neq 1$ by hypothesis. This shows that the cycle decomposition of σ is a product of p-cycles (they commute as they are disjoint by construction). Conversely, suppose that $l_i = p$ for all i. Then clearly $|\sigma| = \text{lcm}\{l_1, ..., l_r\} = p$, which proves the claim.

This need not be true if p is not prime. For example, take $p = 6$, we have that

$$|(12)(345)| = 6$$

and yet $(12)(345)$ is not a product of 6-cycles.

---

2) If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assume to be a homomorphism?

Solution. From Exercise 1 $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$ (when $n = 0$ we have $\varphi(1_G) = 1_H$). If $|x| = m$ is finite, then $x^m = 1_G$ and so $\varphi(x)^m = 1_H$, which shows $|\varphi(x)| \leq |x|$. So $|\varphi(x)| = k$ is finite also. Now,

$$\varphi(x)^k = 1_H \implies \varphi(x^k) = 1_H \implies x^k = 1_G$$

since φ is injective. This shows that $|x| \leq |\varphi(x)|$ and hence in fact $|\varphi(x)| = |x|$. On the other hand, if $|x| = \infty$, then $|\varphi(x)| = \infty$ also, for otherwise $\varphi(x)^k = 1$ for some $k \in \mathbb{N}$. The same calculation above shows that $x^k = 1_G$, which comtradicts that $|x| = \infty$.

Fix $n \in \mathbb{Z}^+$. Let $A = \{x \in G \mid |x| = n\}$ and $B = \{y \in H \mid |y| = n\}$. We want to show that $\text{card}(A) = \text{card}(B)$, i.e. there exists a bijection between A and B. Consider the map

$$\tilde{\varphi} : A \to B \quad \text{defined by } \tilde{\varphi}(x) = \varphi(x),$$

i.e. $\tilde{\varphi}$ is obtained by restricting the domain of φ to A and the codomain to B. Since $|x| = n$ implies $|\varphi(x)| = n$, this is well-defined (the image $\tilde{\varphi}(x)$ indeed lies in B). Injectivity follows from that of φ. For surjectivity, suppose that $y \in B$. Let $x \in G$ be such that $\varphi(x) = y$ (which exists since φ is surjective). Then $|x| = |\varphi(x)| = |y| = n$. Hence, $x \in A$ and $\tilde{\varphi}(x) = y$, proving surjectivity. Thus, $\tilde{\varphi}$ is a bijection.

This result need not be true if φ is only a homomorphism. Let $\varphi : \{-1, 1\} \to \{1\}$ be the trivial homomorphism. We have $|-1| = 2$ but $|\varphi(-1)| = |1| = 1$.

---

4) Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Solution. Notice that $i \in \mathbb{C} - \{0\}$ has order 4. By Exercise 2, if $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ were isomorphic, then there would exists $x \in \mathbb{R} - \{0\}$ with $|x| = 4$. This would imply $x^4 = 1$ and so $x = \pm 1$. But $|1| = 1$ and $|-1| = 2$, so we have a contradiction.
