Abstract Algebra

Professor Ben Richert

Exam 1

Key

Problem 1. *(25 pts.)*

(a – 5 pts) Write the permutation $\alpha = (1235)(24567)(1872)(2946)$ as a product of disjoint cycles in the canonical form discussed in class.

Solution. We use the method described in class (and in the book) by reading the expression right to left, (and reading left to right within the individual cycles). So, in canonical form, $\alpha = (1835629)(47)$. □

(b – 5 pts) For what n is α a permutation in S_n?

Solution. As it stands, writing α down uses the integers from 1 to 9, and so α certainly gives instructions for permuting 9 elements (that is, $\alpha \in S_9$). Of course, α can also be said to act on a set of more than 9 elements—we simply let it permute $\{1, \ldots, 9\}$ as before and fix all larger integers. (Another way to say this is that can write $(1835629)(47) = (1835629)(47)(10) = (1835629)(47)(10)(11) = \cdots$). So α is a permutation in S_n for $n \geq 9$. □

(c – 5 pts) What is the inverse of α?

Solution. The inverse of α is $(1926538)(47)$. Note that the cycles are (1835629) and (47) written backwards. This should be the inverse because we read from left to right in a cycle—thus to invert that action we should reverse the cycle. Of course, that isn't a proof, but multiplying α and our candidate together do verify that this is the inverse as claimed. □

(d – 5 pts) What is the order of α?

Solution. According to a theorem from the text, the order of a permutation in disjoint cycle form is the least common multiple of the lengths of the cycles. For us, $\alpha = (1835629)(47)$, so we have lengths 7, and 2. Thus the order of α is $\text{lcm}(7, 2) = 14$. □

(e – 5 pts) Is α an even or an odd permutation?

Solution. The algorithm we used in class to write a cycle as a product of transpositions is

$$(a_1, \cdots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2).$$

So α can be written as $(19)(12)(16)(15)(13)(18)(47)$. From this it is apparent that α is an odd cycle (it is made up of seven transpositions). □

Problem 2. *(15 pts.) Prove that elements of finite order in an Abelian group G form a subgroup of G.*

Solution. Let $H = \{g \in G \mid |g| < \infty\}$. By our usual theorem, it is enough to demonstrate that $H \neq \emptyset$, and that for all $a, b \in H$, $ab^{-1} \in H$. That $H \neq \emptyset$ is clear because the identity element $e \in G$ has finite order (in particular, $e^1 = e$ so $|e| = 1$), and thus $e \in H$. Suppose then that $a, b \in H$. Making use of the fact that G is Abelian and the fact that $(b^{-1})^n = (b^n)^{-1}$, we note that

$$(ab^{-1})^{|a||b|} = (a^{|a|})^{|b|}((b^{-1})^{|b|})^{|a|} = e^{|b|}((b^{|b|})^{-1})^{|a|} = e((e)^{-1})^{|a|} = e.$$

Thus $|ab^{-1}| \leq |a||b| < \infty$, and so $ab^{-1} \in H$ as required. □

Problem 3. *(10 pts.) Prove that $|ab| = |ba|$ for any $a, b \in G$, G a group.*

Solution. Suppose that ab has infinite order. Then if $|ba| = n < \infty$, we have that $(ba)^n = e$ and thus $a(ba)^n b = aeb$, that is $(ab)^{n+1} = ab$. Canceling a copy of (ab) from both sides, we have that $(ab)^n = e$, which is a contradiction, thus we conclude that $|ab| = |ba| = \infty$.
So suppose that $|ab| = m < \infty$. Then $(ab)^m = e$, and $b(ab)^m a = bea$ and hence $(ba)^{m+1} = ba$. Canceling a copy of (ba) from both sides yields $(ba)^n = e$ and thus $|ba| \leq |ab|$. By symmetry, $|ab| \leq |ba|$, and thus $|ab| = |ba|$ as required. □

Problem 4. *(15 pts.) Discuss the cyclic group $\mathbb{Z}_{18}$. (What is its order, which elements are its generators, how many subgroups does it have and what are they?)*

Solution. There are two relevant facts (two corollaries) which we will use below. The first is that $a \in \mathbb{Z}_n$ generates $\mathbb{Z}_n$ if and only if $(a, n) = 1$. The second fact is that for each divisor k of n, there is exactly one subgroup $\langle n/k \rangle$ of $\mathbb{Z}_n$, and that these are the only subgroups.
Now the order $\mathbb{Z}_{18}$ is 18 (because $\mathbb{Z}_{18} = \{0, 1, \ldots, 17\}$ setwise by definition). By the first fact above we can identify the generators of $\mathbb{Z}_{18}$; they are the integers 1, 5, 7, 11, 13, and 17. The divisors of 18 are 1, 2, 3, 6, 9, and 18, so by the second fact above these correspond to the subgroups $\langle 0 \rangle$, $\langle 9 \rangle$, $\langle 6 \rangle$, $\langle 3 \rangle$, $\langle 2 \rangle$, $\langle 1 \rangle = \mathbb{Z}_{18}$ which have orders 1, 2, 3, 6, 9, and 18 respectively. □

Problem 5. *(10 pts.) Use induction to show that $(ab)^n = a^n b^n$ for a, b in an Abelian group G.*

Solution. The assertion is obvious if $n = 0$ so we will assume that $(ab)^n = a^n b^n$ for some $n \geq 0$, and demonstrate the veracity of the statement $(ab)^{n+1} = a^{n+1} b^{n+1}$. Now $(ab)^{n+1} = (ab)^n (ab) = a^n b^n ab$ by the induction hypothesis, and because G is Abelian, $a^n b^n ab = a^n ab^n b = a^{n+} b^{n+1}$. Thus by induction, $(ab)^n = a^n b^n$ for all $n \geq 0$, $a, b \in G$, G an Abelian group.
If $n < 0$, we then note that $(ab)^n = (ab)^{-|n|} = \left((ab)^{|n|}\right)^{-1} = (a^{|n|} b^{|n|})^{-1} = (b^{|n|})^{-1}(a^{|n|})^{-1} = (b^{-|n|})(a^{-|n|}) = b^n a^n = a^n b^n$ (we made use of the Abelian hypothesis, the fact that $(ab)^{-1} = b^{-1}a^{-1}$, and the statement for positive n proved above). □