Solutions for Problem Sheet 3

1. *Prove that in a group of even order there always exists an element of order* 2.

Solution: Note that an element g has order 2 if and only if $g \neq 1$ but $g^2 = 1$, or equivalently, $g \neq 1$ but $g = g^{-1}$. Since the inverse of an inverse is the original element, we can form pairs of the elements of G and their inverses. Some of them remain alone: those which are the inverses of themselves. But G has an even number of elements, so the number of lonely elements will also be even. 1 is among these, so there must be another g such that $g = g^{-1}$, and this is what we wanted to prove.

2. *Show that* 6 *is a divisor of* $|S_4|$ *but* S_4 *has no element of order* 6*.*

Solution: The order of S_4 is $4! = 24$, which is divisible by 6. On the other hand, if a permutation has order 6 then in its disjoint cycle form there must either be a 6-cycle among the cycles, and for this we need at least 6 elements in the base set, or there must be two disjoint cycles, so that the length of one is divisible by 2 and the other by 3, for which we need at least 5 elements in the base set. But the base set of S_4 has only four elements, so neither of the two cases can happen here.

3. *Prove that every group of prime order is cyclic.*

Solution: Suppose $|G| = p$ is a prime. By the Lagrange theorem, $|H|$ is a divisor of p for every subgroup $H \leq G$, so $|H| = 1$ or p. But then for any $g \in G \setminus \{ 1 \}$, we have $| \langle g \rangle | > 1$, so $o(g) = | \langle g \rangle | = p = |G|$, implying that $G = \langle g \rangle$ is cyclic.

4. *Prove that every cyclic group is commutative. Give an example for a commutative subgroup in* S_4 *which is not cyclic.*

Solution: Let $G = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$ be cyclic. We first observe that a^{-1} and a commute since $aa^{-1} = a^{-1}a = 1$, so in a product of copies of a and a^{-1} we can rearrange the elements in any way. So $a^k a^\ell = a^\ell a^k$ even if some of k or ℓ are negative. This shows that G is commutative.
Since any group of order 1, 2 or 3 is cyclic by the previous problem, we try to find a 4-element subgroup which is not cyclic, that is, it has no element of order 4. But then by the Lagrange theorem the orders of the elements can only be 1 or 2, that is, $H = \langle 1, a, b, c \rangle$ where $o(a) = o(b) = o(c) = 2$. Since ab (and ba) cannot be equal to 1, a or b, we must have $ab = ba = c$. So we are looking for a, b of order 2 which commute with each other. Such can be two disjoint 2-cycles, so let $a = (12)$, $b = (34)$ and $c = (12)(34)$. It is easy to check that this H is indeed a subgroup, and it is abelian (the inverse of each element is itself, and the product of any two nonidentity elements is the third nonidentity element).
(We could have chosen also $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$, they have the same multiplication structure, that is, $\langle (12), (34) \rangle \cong \langle (12)(34), (13)(24) \rangle$.)

5. *Let* $A, B \leq G$ *and* $|G| < \infty$.
Prove that the cardinality of the subset $AB = \{ ab \mid a \in A,\ b \in B \}$ *is*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Solution: The cartesian product $\{(a, b) \mid a \in A,\ b \in B \}$ has $|A| \cdot |B|$ elements. Let us partition the elements of this cartesian product so that (a, b) and (a', b') are in one class if

$ab = a'b'$, that is, if $a^{-1}a' = b(b')^{-1}$. Since the latter element lies both in A and B, if we call this element x then $x \in A \cap B$, and $a' = ax$, while $b' = x^{-1}b$, that is, $(a', b') = (ax, x^{-1}b)$. So in each class there are exactly as many elements as the cardinality of $A \cap B$. The product ab can have $|AB|$ different values, so $|A| \cdot |B| = |A \cap B| \cdot |AB|$, which gives the formula in the problem.

6. *a) Let $A, B \le G$. Show that AB is also a subgroup if and only if $AB = BA$.*
b) Check that for $A = \langle (12) \rangle$, $B = \langle (123) \rangle$ and $C = \langle (13) \rangle$, the subset AB is a subgroup of S_3 but AC is not a subgroup.
c) Show that for $A = \langle (12) \rangle \le S_4$ and $B = \langle (234) \rangle \le S_4$ the cardinality $|AB|$ of the subset AB is a divisor of $|S_4|$ but AB not a subgroup of S_4.

Solution: a) We use the condition that a nonempty subset $H \subseteq G$ is a subgroup if and only if $HH = H$ and $H^{-1} = H$. Note that the definition of the set product and set inverse immediately implies that the product is associative:

$$(XY)Z = \{(xy)z \,|\, x \in X,\ y \in Y,\ z \in Z\} = \{\, x(yz) \,|\, x \in X,\ y \in Y,\ z \in Z\,\} = X(YZ),$$

$$(X^{-1})^{-1} = \{\, x^{-1} \,|\, x \in X\,\}^{-1} = \{(x^{-1})^{-1} \,|\, x \in X\,\} = \{\, x \,|\, x \in X\,\} = X, \text{ and}$$

$$(XY)^{-1} = \{(xy)^{-1} \,|\, x \in X,\ y \in Y\,\} = \{\, y^{-1}x^{-1} \,|\, x \in X,\ y \in Y\,\} = Y^{-1}X^{-1}.$$

$\Rightarrow$: If $AB \le G$ then $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$.

$\Leftarrow$: Clearly, $1 = 1 \cdot 1 \in AB$, so AB is not empty, and supposing that $AB = BA$, we have $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$, and $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$, so $AB \le G$.

b) We can calculate the elements of the sets AB and AC but we may first calculate the cardinalities by the formula in problem 5. Since $A = \{\,1, (12)\,\}$, $B = \{\,1, (123), (132)\,\}$, $C = \{\,1, (13)\,\}$, we see that $A \cap B = A \cap C = 1$, so $|AB| = 2 \cdot 3/1 = 6$, and $|AC| = 2 \cdot 2/1 = 4$. In the first case we got that for the subset $AB \subseteq S_3$, $|AB| = 6 = |S_3|$, so AB is the whole S_3, thus it is a subgroup. In the second, $|AC| = 4$ is not a divisor of $|S_3| = 6$, so it cannot be a subgroup by the Lagrange theorem. So in these special cases we were able to decide if the set product is a subgroup, without actually calculating elements in the product. In many cases, it is not enough, see part c).

c) Here $A = \{\,1, (12)\,\}$ and $B = \{\,1, (234), (243)\,\}$, so $A \cap B = 1$, and $|AB| = 2 \cdot 3/1 = 6$ is a divisor of $|S_4| = 24$. So the cardinality does not decide if AB is a subgroup or not. However, if we calculate $AB = \{\,1, (12), (234), (1342), (243), (1432)\,\}$, we see that it is not closed for multiplication, for example $(1342)^2 = (14)(23) \notin AB$, so AB is not a subgroup.

(A shorter argument could be, though one needs a bit of intuition for this, is that $(12)(234) = (1342) \in B$ has order 4 but 4 does not divide $|AB| = 6$, so AB cannot be a subgroup.)

7. *Show that $Hg \leftrightarrow g^{-1}H$ is a bijection between the right and left cosets of $H \le G$, and for a right transversal R the set R^{-1} is a left transversal.*

Solution: The map $Hg \mapsto g^{-1}H$ is well-defined and injective since $Hx = Hy \Leftrightarrow Hxy^{-1} = H \Leftrightarrow xy^{-1} \in H \Leftrightarrow xy^{-1}H = H \Leftrightarrow y^{-1}H = x^{-1}H$, and it is clearly surjective, so it gives

a bijection between the right and left cosets of H.
R is a right transversal $\Leftrightarrow G = \dot{\bigcup}_{r\in R} Hr$, but then $G = G^{-1} = \dot{\bigcup}_{r\in R} (Hr)^{-1} = \dot{\bigcup}_{r\in R} r^{-1}H^{-1} = \dot{\bigcup}_{r\in R} r^{-1}H = \dot{\bigcup}_{s\in R^{-1}} sH$, so R^{-1} is a left transversal.

8. *Prove that the cyclic group C_n has exactly $\varphi(d)$ elements of order d for every divisor d of n, where $\varphi(d) = \{\, m \mid 1 \le m \le d,\ \gcd(m,d) = 1 \,\}$.*

Solution: Note first that by Lagrange's theorem, all the orders of elements in C_n are divisors of n. Now let d be a positive divisor of n.
We know that $C_n = \langle a \rangle = \{\, a, \ldots, a^n = 1 \,\}$ where the n elements listed here are all different. Furthermore we proved in 2/6., part 2) that $o(a^m) = \frac{o(g)}{\gcd(m,o(g))} = \frac{n}{\gcd(m,n)}$, so $o(a^m) = d \Leftrightarrow \gcd(m,n) = n/d \Leftrightarrow m = k\frac{n}{d}$, where $\gcd(k,d) = 1$. Since $1 \le m \le n$, we also have $1 \le k \le d$, thus the number of possible choices for this k is exactly $\varphi(d)$.

9. *What are the possible orders of the elements of D_n, and what is the number of elements for each order?*

Solution: The n rotations form a cyclic subgroup of order n, so in it there are exactly $\varphi(d)$ elements of order d for every $d \mid n$. The rest of the group consists of the n reflections, and each of those has order 2. To summarize: if n is odd then there are n elements of order 2 and $\varphi(d)$ elements of order d for each $d \mid n$; if n is even then there are $n+1$ elements of order 2 and $\varphi(d)$ elements of order d for every divisor $d \ne 2$ of n.

10. *Show that every nontrivial (that is, $\ne 1$) subgroup of C_∞ has a finite index, i.e. it has finitely many cosets.*

Solution: Let $H \ne 1$ be a subgroup of $G = \langle a \rangle \cong C_\infty$, and let k be the smallest positive integer such that $a^k \in H$ (there is such a k since $H \ne 1$). (We have seen in the proof of the theorem about the subgroups of a cyclic group that in this case $H = \langle a^k \rangle$.) Now we show that $R = \{\, 1, a, \ldots, a^{k-1} \,\}$ is a (right and left, since G is abelian) transversal for H. For any $n \in \mathbb{Z}$ and euclidean division $n = kq + r$ (with $0 \le r < k$), we have $a^n = (a^k)^q a^r \in Ha^r$, so R contains an element from every coset. Furthermore, for $0 \le i < j \le k-1$, $(a^j)(a^i)^{-1} = a^{j-i} \notin H$, so $Ha^i \ne Ha^j$, which shows that R contains only one element from any coset.

HW1. *Let $A, B \le G$, where G is a finite group. Show that the subgroups A and B are contained in the set AB, and both $|A|$ and $|B|$ are divisors of $|AB|$ (though AB is not necessarily a group).*

HW2. *Prove that the (multiplicative) group of invertible 3×3 upper triangular matrices over $\mathbb{Z}_2$ is not a cyclic group. (For example, you may show that it is not commutative.)*