Matematiska Institutionen
KTH

Solutions to homework number 4 to SF2736, fall 2011.

1. (0.2p) Let $(G, \cdot)$ denote the group that consists of all elements in the ring Z_{20} that are invertible by multiplication. This group is isomorphic to a direct product of cyclic groups. Find this direct product of cyclic groups and describe the isomorphism.

   Lösning: The invertible elements in this ring are

   $$(G, \cdot) = \{1, 3, 7, 9, 11, 13, 17, 19\},$$

   which we know constitute a group $G = (G, \cdot)$ under multiplication. We first find the orders of the elements. We know that the order $\sigma(g)$ divides the size $|G|$ of G, for every element $g \in G$.

   $$3^2 = 9 \neq 1 \qquad 3^4 = 1$$

   Hence the order of 3 is 4, and the group generated by 3 consists of the following elements:

   $$\langle 3 \rangle = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 1\}.$$

   The element 9 has order 2 and the element 7 has order 2. The elements in the coset $19\langle 3 \rangle$ are the remaining elements:

   $$(-1)\langle 3 \rangle = \{17, 11, 13, 19\}$$

   have also the orders 1, 2 and 4 as

   $$((-1)g)^4 = g^4 = 1 \qquad \text{and} \qquad ((-1)g)^2 = g^2$$

   for all elements g in $\langle 3 \rangle$.

   As no element has order 8, we conclude that G is not a cyclic group. We claim that G is isomorphic to the group

   $$(Z_2, +) \times (Z_4, +) = \{(h, k) \mid h \in (Z_2, +),\ k \in (Z_4, +)\}.$$

The isomorphism is defined by

$$\varphi : G \to (Z_2, +) \times (Z_4, +), \qquad \varphi : (-1)^e g^f \mapsto (e, f).$$

As

$$(-1)^e g^f \cdot (-1)^{e'} g^{f'} = (-1)^{e+e' (\mathrm{mod}\ 2)} g^{f+f' (\mathrm{mod}\ 2)}$$

it is clear that the map φ is an isomorphism.

2. (0.2p) Consider the group $\mathcal{S}_8$ consisting of all permutation of the set $\{1, 2, 3, \ldots, 8\}$. Find all possible orders of the elements of $\mathcal{S}_8$.

   Lösning: We consider the permutations as products of disjoint cycles. Then the order of a permutation is the least common multiple of the lengths of these cycles. Then lengths of the cycles can be

   $$1, 2, 3, 4, 5, 6, 7, 8.$$

   The sum of the lengths of the disjoint cycles in a permutation can at most be 8. So a 7 cycle can just appear if the other cycle is a 1-cycle. A 6-cycle can appear with two 1-cycles or a 2-cycle. So if there are 8-cycles, 7-cycles or 6-cycles in a permutation, then the order of the permutation is 8, 7 and 6.

   A 5-cycle can be combined with just 1-cycles, or one 2-cycle and one 1-cycle, or combined with a 3-cycle. This gives the orders 5, 10 and 15.

   A 4-cycle can be combined with a 3-cycle, and else with 1-cycles and 2-cycles, so such a permutation can contribute with the orders 12 and 4.

   If there are just 3-cycles and/or 2-cycles, the only further orders you obtain is 3, 2 and 1.

   So summarizing we get

   Answer: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 15.

3. (0.3p) Show that if H and K are subgroups of an abelian group G satisfying

   $$|H| \cdot |K| = |G| \qquad \text{and} \qquad |H \cap K| = 1,$$

   then every element g in G can in a unique way be written as a sum

   $$g = h + k,$$

of elements $h \in H$ and $k \in K$.

Lösning: First assume there are $h, h' \in H$ and $k, k' \in K$ such that

$$h + k = g = h' + k'.$$

Then

$$H \ni h - h' = k' - k \in K$$

As $|H \cap K| = 1$ we get that $H \cap K = \{0\}$ (as $H \cap K$ is a subgroup of G). So

$$h - h' \in K \cap H \quad \implies \quad h - h' = 0 \quad \implies \quad h = h'.$$

and similarly for k and k', in fact they are equal. The set

$$H + K = \{h + k \mid h \in H,\ k \in K\} \subseteq G$$

thus contains $|H| \cdot |K| = |G|$ elements, as this is the exact number of combinations $h + k$, with $h \in H$ and $k \in K$, and as furthermore, all these combinations are distinct. So every element of G must belong to $H + K$, which proves the desired result.

4. (0.3p) Show that all abelian groups of size 35 are isomorphic.

   Lösning: We claim that every such group G is cyclic. Assume that G is not cyclic. The elements then has order 5 or 7 (or 1) as the order of an element must divide 35. Assume all elements, except the identity, have order 5. Every non identity element g in a group generated by an element of order 5 must have order 5, as the order of an element divides the size of the group. Hence

$$\langle g \rangle = \{g, g^2, g^3, g^4, g^5 = e\} = \langle g^2 \rangle = \langle g^3 \rangle = \langle g^4 \rangle,$$

   and consequently, every non identity element belongs to one and only one subgroup of size 5. This implies that the 34 non identity elements in G are partitioned into subsets of type

$$\langle g \rangle \setminus \{e\} = \{g, g^2, g^3, g^4\},$$

   i.e., of size 4. This is evidently impossible. Thus G cannot solely consist of elements of order 5 (and the identity).

Similarly we can prove that there can not just be elements of order 7.

Now let g be an element of order 5 and h an element of order 7. Then, the order of gh divides 35. It can neither be 5 nor 7 as

$$(gh)^5 = g^5 h^5 = eh^5 \neq e, \qquad (gh)^7 = g^2 e \neq e.$$

So the order of gh is 35, the same number as the size of G.

We have proved that G must be cyclic. All cyclic groups of the same size are isomorphic.