Matematiska Institutionen
KTH

Solutions to homework number 4 to SF2736, fall 2012.

Please, deliver this homework at latest on Tuesday, November 27.

The homework must be delivered individually, and, in general, just hand written notes are accepted. You are free to discuss the problems below with your class mates, but you are not allowed to copy the solution of another student.

1. (0.2p) The group $G = (Z_{17} \setminus \{0\}, \cdot)$ is cyclic. Find all generators of G.

   Solution. We first find one generator by trial and error: We try with $g = 2$. The size of G is 16 so if the order of 2 is 16 then 2 is a generator of G. From one of the corollaries of the theorem of Lagrange, we know that the order of 2 divides 16. As

   $$2^8 = 256 \equiv 1 (\text{mod } 17)$$

   the element 2 has not order 16, instead the element 2 generates the following subgroup of G:

   $$< 2 >= \{2, 4, 8, 16, 15, 13, 9, 1\}.$$

   and none of these elements can be a generator of G as they are elements of a group of size 8 and thus have an order that divides 8, or explicitely:

   $$(2^i)^8 = (2^8)^i = 1.$$

   Next we search the order of the element 3, regarding our knowledge that the order divides 16:

   $$3^2 = 9 \neq 1, \quad 3^4 = 9^2 = -4 \neq 1, \quad 3^8 = 16 \neq 1,$$

   so 3 is a generator of G. Thus,

   $$G = \{3, 3^2, 3^3, \ldots, 3^{16} = 1\}.$$

   Now we search the other generators of G. If $n = 2k$ for some integer k, then

   $$(g^n)^8 = (3^{2k})^8 = 1$$

so even powers of the element 3 cannot be generators of G. If $n = 2k+1$ for some integer k, then

$$(g^n)^8 = (3^{2k+1})^8 = 3^8 \cdot (3^{16})^k = -1$$

so the order of 3^{2k+1} cannot be equal to 8, or 4, or 2, as if $h^4 = 1$ then also $h^8 = 1$.

Answer: The elements in the set

$$\{3, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}\} = G\backslash < 2 >= \{3, 5, 6, 7, 10, 11, 12, 14\}.$$

2. (0.2p) The set of invertible (by multiplication) elements in Z_{25} constitutes an Abelian group denoted $\mathrm{U}(Z_{25})$. This group is isomorphic to a direct product of some cyclic groups. Find these cyclic groups.

   Solution. An element a in a ring Z_n is invertible if and only if $\gcd(a, n) = 1$. Hence

   $$\mathrm{U}(Z_{25}) = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}.$$

   The number of elements in this group is 20. The order of 2 is neither 2, 4, 5 or 10 as

   $$2^{10} = -1 \neq 1, \qquad 2^4 = 16 \neq 1.$$

   So the given group is isomorphic to a cyclic group with 20 elements, as

   $$< 2 >= \mathrm{U}(Z_{25}).$$

   However, we can continue and we now prove that

   $$\mathrm{U}(Z_{25}) \approx < 2^5 > \times < 2^4 > .$$

   We find that

   $$< 2^5 >= \{2^5, 2^{2\cdot 5}, 2^{3\cdot 5}, 1\}, \qquad < 2^4 >= \{2^4, 2^{2\cdot 4}, 2^{3\cdot 4}, 2^{4\cdot 4}, 1\}$$

   and define the map φ from $< 2^5 > \times < 2^4 >$ to $\mathrm{U}(Z_{25})$ by

   $$\varphi : (2^i, 2^j) \mapsto 2^{i+j}.$$

   It is easy to check that φ is a bijective map, and that it furthermore is a group isomorphism.

   If we denote a cyclic group with n elements by C_n then we get the

   Answer: The group $\mathrm{U}(Z_{25})$ is isomorphic to both C_{20} and $C_4 \times C_5$.

3. Let $\mathcal{S}_n$ denote the group consisting of all permutations on the set $\{1, 2, 3, \ldots, n\}$.

   (a) (0.1p) Find the smallest subgroup $\mathcal{T}_3$ to $\mathcal{S}_4$ that contains the permutations $\tau_2 = (1\ 2)$ and $\tau_3 = (1\ 3)$.

   Solution. We observe that

   $$(i\ j)(i\ k)(i\ j) = (j\ k). \tag{1}$$

   Thus $\mathcal{T}_3$, besides the 2-cycles (1 2) and (1 3), also contains the 2-cycle (2 3). We know that each of the $3! = 6$ permutations of the elements 1, 2 and 3 can be expressed as a product of these 2-cycles. Consequently

   Answer: $\mathcal{T}_3 = \{\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

   (b) (0.2p) Find all subgroups H to $\mathcal{S}_4$ such that $\mathcal{T}_3 \subseteq H \subseteq \mathcal{S}_4$.

   Solution. An element φ in H that does not belong to $\mathcal{T}_3$ must map 4 to an element in the set $\{1, 2, 3\}$. We write φ as a product of disjoint cycles

   $$\varphi = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_c. \tag{2}$$

   Then exactly one of these cycles, say γ_1, will contain the element 4. The other cycles belong to $\mathcal{T}_3$. We multiply with the inverses to these cycles, that also belongs to H, and obtain that

   $$\gamma_1 = \varphi \circ \gamma_c^{-1} \circ \cdots \circ \gamma_2^{-1} \in H.$$

   Without loss of generality we may assume that

   $$\gamma_1 = (i_1\ \ldots\ i_k\ 4) = (i_1\ 4)(i_1\ i_k) \cdots (i_1\ i_2). \tag{3}$$

   We may multiply with the inverses of the last $k - 1$ cycles in the product above, as they also belong to $\mathcal{T}_3$ and thus also to H. We then get that

   $$(i_1\ 4) \in H.$$

   By using the equation (1) with $k = 4$ we get that all 2-cycles in $\mathcal{S}_4$ belong to subgroup H. As in subproblem (a) we get that this implies that

   ANSWER: $H = \mathcal{S}_4$ if $\mathcal{T}_3 \subseteq H$ with $H \neq \mathcal{T}_3$.

(c) (0.3p) Generalize your answer above.

Solution. Let $\mathcal{T}_{n-1}$ denote the smallest subgroup that contains the 2-cycles $(1\ 2), (1\ 3), \ldots,\ (1\ n-1)$. The equation (1) then gives that $\mathcal{T}_{n-1}$ contains all the 2-cycles that does not contain the element n, and thus $\mathcal{T}_{n-1}$ contains all permutations in $\mathcal{S}_n$ that fix the element n.

Now, we repeat the solution in subproblem (b) with 4 substituted by n. This gives that

ANSWER: The only subgroups to $\mathcal{S}_n$ that contain $\mathcal{T}_{n-1}$ are both these subgroups, that is, just the trivial possibilities.