# Solutions to exercises for TATA55, batch 2, 2023

October 10, 2023

1. (4p) How many subgroups of size $k$ are there in $C_n$?

   **Solution:** By Lagrange, unless $k \mid n$ there are no subgroups of size $k$. If $C_n = \langle g \rangle$ and $n = mk$, then $o(g^m) = k$. Thus there exists at least one subgroup $H = \langle g^m \rangle$ of size $k$. The elements of $H$ all have orders dividing $k$. In particular, $\phi(k)$ of them have order $k$.

   Note that any subgroup $K$ of $C_n$ is cyclic, hence generated by $g^\ell$, which have order $\ell n / \gcd(\ell, n)$. If $K$ is to have order $k$, then $n/\gcd(\ell, n) = k = n/m$ hence $m = \gcd(\ell, mk) = m$ hence $1 = \gcd(\ell/m, k)$. There are again $\phi(k)$ possible generators of such a subgroups; therefore, all of them lie in $H$. Hence $K = H$; there is but one cyclic subgroup of a given size.

   Alternative proof: $o(g^{d_1}) = o(g^{d_2}) = k$ so $n/\gcd(n, d_1) = n/\gcd(n, d_2)$, hence $r = \gcd(n, d_1) = \gcd(n, d_2)$. We claim that $g^{d_1} \in \langle g^{d_2} \rangle$, i.e. that $d_1 \equiv s d_2 \mod n$. This is equivalent to the Diophantine equation $d_1 + tn = s d_2$ or $s d_2 - tn = d_1$ which is solvable since $\gcd(d_2, n) = r$ divides $d_1$.

   Alternative proof 2: We show that $\langle g^m \rangle = \langle g^d \rangle$, where $d = \gcd(m, n)$. Since $d \mid m$, we get $g^m \in \langle g^d \rangle$. For the converse, use Bezout to get $d = am + bn$. Then $g^d = g^{am+bn} = (g^m)^a * (g^n)^b = (g^m)^a \in \langle g^m \rangle$.

   In conclusion, the number of subgroups of size $k$ is 1 if $k \mid n$ and zero otherwise.

2. (6p) Same question for the dihedral group $D_n$ (partial credit for partial results).

   **Solution:** Let $r, s \in D_n$ be rotation by $1/n$'th of a lap, and reflection in the $x$-axis, respectively. Then $D_n$ is generated by $r, s$, with relations $r^n = s^2 = 1$, $sr = r^{n-1}s$, and every element can be uniquely written as either $1$, $r^k$, $1 \leq k \leq n-1$, rotations, or $r^k s$, $0 \leq k \leq n-1$, reflections.

   The reflections form a cyclic subgroup with $n$ elements, so any subgroup with just rotations is of the form $\langle r^d \rangle$ with $d \mid n$, and there is exactly one for each $d$, by the previous exercise. Thus, for any $d$ that divides $n$, there is a unique rotation subgroup with $n/d$ elements.

   Suppose now that the subgroup $K \leq D_n$ contains a reflection. For simplicity, assume that this reflection is $s$ (the general case can be deduced from this case). Then $K \cap \langle r \rangle$ is a subgroup of $\langle r \rangle$, and thus $\langle r^d \rangle$, with $d \mid n$. Clearly $\langle r^d, s \rangle \subseteq K$. We claim that the reverse inclusion holds, as well.

To prove this, pick any $k \in K$. If $k$ is a rotation then $k \in \langle r \rangle \cap K = \langle r^d \rangle$. If $k$ is a reflection, then either it is $s$, and we are done, or it is some other reflection, i.e. $k = r^j s$. But $s \in K$ so $ks \in K$ since $K$ is a subgroup, hence closed under multiplication, so $ks = r^j ss = r^j \in K$. Then since this a rotation, it lies in $\langle r \rangle \cap K = \langle r^d \rangle$, so $r^j = r^{d\ell}$ for some $\ell$. But then

$$k = r^j s = r^{d\ell} s = (r^d)^\ell s \in \langle r^d, s \rangle.$$

The $2n/d$ elements of $K$ are

$$r^d, r^{2d}, \ldots, r^n = 1, r^d s, r^{2d} s, \ldots, r^n s = s$$

For the general case, i.e. $K$ contains some reflection $\tilde{s} = r^j s$ different from $s$ but not $s$ itself, we use the fact (I think this is mentioned in Svensson?) that $D_n$ can be generated by $r, \tilde{s}$, and the relations are the same! Then by the previous result, $K = \langle r^d, \tilde{s} \rangle = \langle r^d, r^j s \rangle$. The number of elements of $\langle r^d, r^j s \rangle$ is of course $2n/d$, since these elements are

$$r^d, r^{2d}, \ldots, r^n = 1, r^d \tilde{s}, r^{2d} \tilde{s}, \ldots, r^n \tilde{s} = \tilde{s}$$

A bit trickier to prove is the fact that

$$\langle r^d, r^i s \rangle = \langle r^d, r^j s \rangle \quad \iff \quad i \equiv j \mod d$$

It is true, however, so we may assume that $0 \leq j \leq d - 1$.

So, for each divisor $d$ of $n$, there is one rotational subgroup $\langle r^d \rangle$ of order $n/d$, and $d$ "dihedral" subgroups $\langle r^d, r^i s \rangle$ of order $2n/d$. For instance, in $D_5$ there is 1 subgroup of size 5, 1 of size 10, 1 of size 1, and 5 of size 2.

3. (4p) Let $G$ be a group, and suppose that $a^2 = 1$ for all $a \in G$. Show that $G$ is abelian. On the other hand, show that the relations $a^3 = b^3 = 1$ for a group $G$ generated by $a, b$ does not imply that the group is abelian.

   **Solution:** In the first case, take $x, y \in G$. Then $x^2 = y^2 = 1$ so $x^{-1} = x$, $y^{-1} = y$, and

   $$1 = (xy)^2 = xyxy = xyx^{-1}y^{-1}$$

   so

   $$yx = xy.$$

   Secondly, take $g = (1,2,3)$ $h = (2,3,4)$, $G = \langle g, h \rangle \leq S_4$. Then $g^3 = h^3 = 1$ but $gh \neq hg$.

4. (5p) Denote the adjacent transposition $(j, j+1)$ by $s_j$.

   (a) Show that the set $\{s_1, \ldots, s_{n-1}\}$ generate $S_n$.

   (b) Find the relations (including self-relations) among these generators.

(c) Show that the set of all $t_{ij} = s_i s_j$ generate $A_n$.

(d) Show that the set of all $u_j = (12j)$ generate $A_n$.

(e) Find the relations between the $u_j$'s.

**Solution:** It is shown in the textbook that the $s_j$ generate $S_n$, see that. The relations are $s_j^2 = 1$, so $s_i^{-1} = s_i$, and $s_i s_j = s_j s_i$ when $|i-j| > 1$, and finally $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$. It is enough to find and verify these relations, you need no prove that they generate all relations.

From the theorem about the well-definedness of signs of permutations we know that any even permutation is a product of an even number of transpositions; thus by the first part, it is the product of an even number of $s_j$'s, thus a product of $t_{ij}$'s.

It is known (see e.g. Svensson 10.43) that every even permutation is the product of 3-cycles. Thus, it is enough to show that every 3-cycle is the product of $u_j$'s.

We have that $u_j^{-1} = u_j^2$ and

$$\begin{aligned}
(1,2,j) &= u_j \\
(1,j,2) &= u_j^{-1} = u_j^2 \\
(1,j,k) &= u_k u_j^{-1} = (1,2,k)(1,j,2) \\
(2,j,k) &= u_k^{-1} u_j = (1,k,2)(1,2,j) \\
(i,j,k) &= (1,k,i)(1,i,j) = u_i u_k^{-1} u_j u_i^{-1}
\end{aligned}$$

So every 3-cycle is indeed a product of $u_j$'s.

It is easy enough to find that the following words in the $u_j$'s correspond to the identity permutation: $u_j^3 = (1,2,j)^3$ and

$$(u_i u_j)^2 = (1,2,i)(1,2,j)(1,2,i)(1,2,j).$$

SAGEMATH indicates that these relations generate all relations, but I have not proved this.

5. (3p, a bit harder) Let $\sigma \in S_n$ be a permutation of cycle type $\lambda = [\lambda_1, \lambda_2, \ldots, \lambda_r]$. Let $V = \mathbb{C}^n$ with canonical basis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ and denote by $T_\sigma : \mathbb{C}^n \to \mathbb{C}^n$ the linear map that satisfies $T_\sigma(\mathbf{e}_j) = \mathbf{e}_{\sigma(j)}$. What are the eigenvalues of $T_\sigma$? Start with the case where $\sigma$ is $k$-cycle.

**Solution:** If $\sigma = (1,2,\ldots,n)$ then let $\xi = \exp(2\pi i/n)$ the standard primitive $n$'th root of unity. For $0 \le k < n$, define the vector

$$v_k = (1, \xi^k, \xi^{2k}, \ldots, \xi^{(n-1)k}).$$

Then

$$\xi^k v_k = (\xi^k, \xi^{2k}, \ldots, \xi^{(n-1)k}, \xi^{nk}) = (\xi^k, \xi^{2k}, \ldots, \xi^{(n-1)k}, 1) = T_\sigma(v_k)$$

so this is an eigenvector with corresponding eigenvalue $\xi^k$. We have found $n$ different eigenvalues, they are all there is.

If $\sigma$ is the product of disjoint cycles $\sigma = \prod_j \gamma_j$ then $T_\sigma = \prod_j T_{\gamma_j}$. Each $T_{\gamma_j}$ fixes the subspace of $V$ spanned by the $e_i$'s with $i$ in the fixpointset of $\gamma_i$, and has as an invariant subspace the subspace spanned by the $e_i$'s with $i$ not in the fixpointset of $\gamma_i$.

Thus, after a simultaneous permutation of the rows and columns of the matrix of $T_\sigma$ it has a diagonal block shape, where each block correspond to the matrix of $\gamma_i$. Thus the set of eigenvalues of $T_\sigma$ is the union of all $k_i$'th roots of unity, where the $k_i$'s are the cycle lengths.