# Solutions of exercise sheet 5

The content of the marked exercises **(*)** should be known for the exam.

**1.** Let $G$ be a group, and consider the set of maps $C(G) = \{f : G \to \mathbb{C}\}$.

1. Prove that defining $(g \cdot f)(x) = f(xg)$, for every $g, x \in G$ and $f \in C(G)$ we obtain an action of $G$ on $C(G)$. Is it faithful?
2. If $|G| \neq 1$, find a non-trivial invariant subset of $C(G)$.

**Solution:**

1. First, notice that the association $(g, f) \mapsto g \cdot f$ defines a map $G \times C(G) \to C(G)$. Moreover, we can easily check compatibility with the group structure:

$$((gh) \cdot f)(x) = f(xgh) = (h \cdot f)(xg) = (g \cdot (h \cdot f))(x), \forall g, h, x \in G, f \in C(G),$$

so that $(gh) \cdot f = g \cdot (h \cdot f)$ for every $g, h \in G$ and $f \in C(G)$. Finally, the identity $1_G \in G$ acts trivially on $C(G)$:

$$(1_G \cdot f)(x) = f(x1_G) = f(x), \forall x \in X, \forall f \in C(G),$$

so that $1_G \cdot f = f$ for every $f \in C(G)$. This proves that we have a group action, which can also be seen as a group map $\varrho : G \to \mathrm{Sym}(C(G))$ sending $g \mapsto g \cdot -$. Consider the characteristic function $\chi : G \to \mathbb{C}$ sending $1_G \mapsto 1_{\mathbb{C}}$ and $1_G \neq g \mapsto 0$. Then if $g \in \mathrm{Stab}_G(\chi)$, one has that $g \cdot \chi(1_G) = \chi(1_G) = 1_{\mathbb{C}}$, where $(g \cdot \chi)(1_G) = \chi(g)$, which is one if and only $g = 1_G$, so that $\mathrm{Stab}_G(\chi) = \{1_G\}$. Hence

$$\ker(\varrho) = \bigcap_{f \in C(G)} \mathrm{Stab}_G(f) \subseteq \mathrm{Stab}_G(\chi) = \{1_G\}$$

Hence the action is faithful, the kernel being trivial.

2. We just need to find a subset $Y \subseteq C(G)$ such that $G \cdot Y \subseteq Y$. Of course this is true for $Y = C(G)^G$, the set of invariant elements. This is nothing but the set of constant functions on $G$. It is clear by definition that a constant function is invariant by $G$. On the other hand, if $f$ is invariant by $G$, then for every $x \in G$ we have $f(x) = (x^{-1} \cdot f)(x) = f(1)$, so that $f$ is constant. Since constant functions are parametrized by $\mathbb{C}$, we obtained $C(G)^G$ is a non-trivial invariant subset of $C(G)$.

Notice that there are *many* more invariant subsets of $C(G)$. We have that $Y \subseteq C(G)$ if and only if for every $f \in Y$ and $g \in G$, one has $g \cdot f \in Y$, that is, if $Y$ contains only whole orbits of the action of $G$ on $C(G)$. Since functions in the same orbit have the same image (easy to check), every orbit is completely contained in the set of maps having image inside the image of the functions in that orbit. Hence if we take $T \subseteq \mathbb{C}$ and $Y = \{f \in C(G) : \mathrm{Im}(f) \subseteq T\}$, then we obtain an invariant subset of $C(G)$.

**2.** Let $G$ be a group and suppose there is an action of $G$ on a set $X$. For $H \subseteq G$, define $X^H = \{x \in X | \forall h \in H, h \cdot x = x\}$. Prove: if $H \trianglelefteq G$, then the action of $G$ on $X$ induces an action of $G/H$ on $X^H$.

**Solution:**

We consider the following map:

$$\begin{aligned} l : G/H \times X^H &\to X^H \\ (gH, x) &\mapsto g \cdot x, \end{aligned}$$

where the dot $(\cdot)$ is the given action of $G$ on $X$. First, we have to prove that $l$ is a map, that is, the image of any $gH$ lies in $X^H$ and does not depend on the representative $g$:

- For every $g \in G$, $x \in X^H$ and $h \in H$, we have that $h \cdot (g \cdot x) = g \cdot ((g^{-1}hg) \cdot x) = g \cdot x$ as $H \trianglelefteq G$. Hence $g \cdot x \in X^H$.
- If $gH = g'H$, then $g = g'h$ for $h \in H$. Then $g \cdot x = (g'h) \cdot x = g' \cdot (h \cdot x) = g' \cdot g$ for every $x \in X^H$, so that the image of $gH$ does not depend on the choice of $g$.

Then the map $l$ is an action of $G/H$ on $X^H$, since $l(1_G \cdot H, x) = 1_G \cdot x = x$ for every $x \in X^H$, and compatibility is inherited from compatibility of the given action.

**3.** Let $G$ act transitively on a finite set $X$, with $|X| \geq 2$. Show that there exists at least one element of $g \in G$ such that $g$ has no fixed point.

**Solution:**

We have that $g \in G$ has a fixed point if and only if $g \in \bigcup_{y \in X} \mathrm{Stab}_G(y)$. Applying our solution of Exercise 4 (independent from other exercises) and using the fact that the action is transitive gives that the set of elements in $G$ fixing some point in $X$ is $\bigcup_{y \in X} \mathrm{Stab}_G(y) = \bigcup_{g \in G} g\mathrm{Stab}_G(x)g^{-1}$, where $x \in X$ is fixed. This set cannot be equal to the whole group $G$, as seen in class, being $\mathrm{Stab}_G(x)$ a subgroup of $G$ of finite index $|X|$ by the orbit-stabiliser theorem.

**4.** Let $G$ be a group acting on $X$. Show that the stabilizers of two elements in the same orbit are conjugate. What happens if for $x \in X$ one has $\mathrm{Stab}_G(x) \trianglelefteq G$?

**See next page!**

**Solution:**

Let $x, y \in X$ lie in the same orbit, that is, $y = g \cdot x$ for some $g \in G$. Then

$$\begin{aligned}\mathrm{Stab}_G(y) &= \{u | u \in G : u \cdot y = y\} = \{u | u \in G : ug \cdot x = g \cdot x\} = \\ &= \{u | u \in G : g^{-1}ug \in \mathrm{Stab}_G(x)\} \overset{u'=g^{-1}ug}{=} \{gu'g^{-1} | u' \in \mathrm{Stab}_G(x)\} = \\ &= g\mathrm{Stab}_G(y)g^{-1},\end{aligned}$$

so that $\mathrm{Stab}_G(x)$ and $\mathrm{Stab}_G(y)$ are conjugate in $G$ (precisely by $g$), as desired.

If $\mathrm{Stab}_G(x) \trianglelefteq G$, then by definition it coincides with its conjugates, so that all the elements in the orbit of $x$ have the same stabilizer.

**5.** Consider the group $G = \mathrm{GL}_n(\mathbb{R})$, where $n$ is a positive integer, and let $H$ be the subgroup consisting of diagonal matrices.

1. Suppose that $g \in H$ has distinct eigenvalues. Compute $C_G(g)$. Try to generalize this for $g \in G$ a (non-necessarily diagonal) diagonalizable matrix with distinct eigenvalues.
2. Now suppose that $n = 2$. Compute $N_G(H)$ and show that $N_G(N_G(H)) = N_G(H)$.

**Solution:**

Notation: for $u_1, \ldots, u_n \in \mathbb{R}^\times$, we denote

$$\mathrm{diag}(u_1, \ldots, u_n) = \begin{pmatrix} u_1 & 0 & \ldots & 0 \\ 0 & u_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & u_n \end{pmatrix} \in H.$$

Recall that the centralizer in $G$ of $g \in G$ is the set of elements in $G$ commuting with $g$. It is easily seen that $C_G(x) = \mathrm{Stab}_G(x)$ for every $x \in G$, the action of $G$ on itself being done by conjugation. We will denote this action with $g * h = ghg^{-1}$ in order not to confuse it with the product in $G$.

1. If $g$ is a diagonal matrix $g = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ with dinstict eigenvalues $\lambda_i$, we claim that $C_G(g)$ is the subgroup $H$ consisting of diagonal matrices. It is clear that all diagonal matrices commute with each other, so we only need to prove that for $a$ a matrix commuting with $g$ we have $a \in H$. To do so, write $a = (a_{ij})_{1 \leq i,j \leq n}$, where $i$ is the row index and $j$ is the column index. Then denoting $a \cdot g = (b_{ij})_{1 \leq i,j \leq n}$ and $g \cdot a = (c_{ij})_{1 \leq i,j \leq n}$ we get $b_{ij} = \lambda_j a_{ij}$ and $c_{ij} = \lambda_i a_{ij}$ and imposing equality for each index we get $(\lambda_i - \lambda_j)a_{ij} = 0$. For every $i \neq j$, we have $\lambda_i \neq \lambda_j$ by hypothesis, giving $a_{ij} = 0$. Hence $a \in H$, and we proved $C_G(g) = H$.

Now suppose $g$ is a diagonalizable matrix with dinstinct eigenvalues $\lambda_1, \ldots, \lambda_n$. This means that $g = p \cdot d \cdot p^{-1}$, for some $p \in G$ and $d = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \in H$. Then applying Exercise 4 and what we got for the diagonal case, we get

$$C_G(g) = \mathrm{Stab}_G(g) = \mathrm{Stab}_G(p * d) = p\mathrm{Stab}_G(d)p^{-1} = pHp^{-1}$$

Hence $C_G(g) = pHp^{-1}$ where $p$ is any matrix diagonalizing $g$.

2. Suppose that $s \in N_G(H)$. Then for every $d \in H$ we have $sds^{-1} \in H$, and since $sds^{-1}$ has the same eigenvalues as $d$ there are only two possibilities: either $sds^{-1} = d$ (i.e., $s \in C_G(d)$), or $sds^{-1}$ is equal to the matrix obtained by switching the elements in the diagonal of $d$, that is, $sds^{-1} = ede^{-1}$, where $e = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ [indeed, conjugating with the matrix $e$ corresponds to change the basis of $\mathbb{R}^2$ by switching the basis elements]. But observing that $e = e^{-1}$, this second case is just equivalent to $es \in C_G(d)$, that is, $s \in eC_G(d)$. Those two conditions on $s$ are verified by any element in $G$ when $d$ has equal eigenvalues, and they are satisfied precisely by the elements of $H \cup eH$ when $d$ has distinct eigenvalues. This proves that $N_G(H) \subseteq H \cup eH$. We claim that we have in fact equality, since for any $h \in H$ one has $hH = Hh$ (as diagonal matrices commute with each others) and $ehH = Heh$ (which is equivalent to $ehHh^{-1}e = H$, i.e., $eHe = H$, true since interchanging the two elements in the diagonal gives a bijection of $H$ with itself). In conclusion, $N_G(H) = H \cup eH$, that is,

$$N_G(H) = \left\{ s \in G | \exists a, b \in \mathbb{R}^\times : s = \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \text{ or } s = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\}.$$

Now we want to check that $N_G(N_G(H)) = N_G(H)$. The inclusion "$\supseteq$" is trivial since $N_G(H)$ is a subgroup of $G$. For the other inclusion, let $a \in N_G(N_G(H))$. Then we can choose $h \in H$ with distinct eigenvalues, e.g. $h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and the condition $a \in N_G(H \cup eH)$ implies $aha^{-1} \in H \cup eH$. If $aha^{-1} \in H$, by the previous argument we obtain $a \in N_G(H)$. Else $aha^{-1} \in eH$, meaning that this matrix has zero values in the principal diagonal, but same eigenvalues as $h$, so that the only two possibilities are $aha^{-1} = eh$ and $aha^{-1} = he$. But those give both a contradiction, by considering the determinants, as $\det(aha^{-1}) = \det(h) \neq -\det(h) = \det(eh) = \det(he)$. In conclusion, we have $N_G(N_G(H)) = N_G(H)$ as desired.

**6.** Let $G$ be a finite group. Prove that any subgroup of index equal to the smallest prime dividing $|G|$ is normal. [*Hint:* Consider an action of $G$ on the coset space with respect to the subgroup, and find its kernel.]

**Solution:**

Let $G$ be a finite group, $p$ the minimal prime dividing $|G|$ and $H \leq G$ subgroup of index $[G : H] = p$. It is easily seen that $G$ acts on $G/H$ by left multiplication, so that

**See next page!**

we have a group homomorphism

$$\varrho : G \to \mathrm{Sym}(G/H).$$

The action has kernel

$$\begin{aligned}\ker(\varrho) &= \{g \in G | \forall x \in G, gxH = xH\} = \{g \in G | \forall x \in G, x^{-1}gx \in H\} = \\ &= \{g \in G | \forall x \in G, g \in xHx^{-1}\} = \bigcap_{x \in G} xHx^{-1} \subseteq H \neq G.\end{aligned}$$

so that the action is not trivial. By the First Isomorphism Theorem, we have $|G|/|\ker(\varrho)| = |\operatorname{Im}(\varrho)|$, so that the image of the action has order dividing $|G|$. By Lagrange's Theorem, the image's order also divides the order of its supergroup $\mathrm{Sym}(G/H)$, which is $p!$. Hence $|\operatorname{Im}(\varrho)|$ divides both $|G|$ (whose factorization contains only primes $\geq q$) and $p!$ (whose factorization contains only primes $< p$ and the prime $p$ once), so that the image can only contain 1 or $p$ elements. The only possibility is that $|\operatorname{Im}(\varrho)| = p$, being the action non-trivial. Then $[G : \ker(\varrho)] = p$, and the containment $\ker(\varrho) \subseteq H$ (together with the multiplicativity of the index) gives $H = \ker(\varrho)$. In particular, $H$ is a normal subgroup of $G$.

**7. (*)** We want to give a proof of Sylow theorems. Given a prime number $p$ and a finite group $G$, we call $p$-subgroup of $G$ any subgroup of order equal to a power of $p$. We call *$p$-Sylow subgroup* of a finite group $G$ any subgroup of order equal to the maximal power of $p$ dividing $|G|$. (For instance, if $G = S_4$, then a 2-Sylow subgroup of $G$ is a subgroup of order 8, and the only 5-Sylow subgroup is $\{1_G\}$).

1. Let $G$ be a finite group, and write $G = p^n h$, with $p$ a prime number, and $n, h$ positive integers such that $p$ does not divide $h$. Consider the set $\mathcal{P} = \{I \subseteq G : |I| = p^n\}$:
   a) Prove that the following defines an action of $G$ on $\mathcal{P}$:
   $$\forall g \in G, \forall I \in \mathcal{P}, g \cdot I := gI = \{gi | i \in I\};$$
   b) Prove that $p$ does not divide $|\mathcal{P}|$, and deduce that there exists an orbit $\mathcal{O} \subseteq \mathcal{P}$ of the action above whose cardinality is not divisible by $p$. Deduce that $|\mathcal{O}|$ divides $h$;
   c) Prove that $\bigcup_{S \in \mathcal{O}} S = G$, and deduce from this that $|\mathcal{O}| \geq h$. Find the cardinality of $H = \mathrm{Stab}_G(S_0)$, for $S_0 \in \mathcal{O}$.

   Conclude: any finite group $G$ has a $p$-Sylow subgroup (*First Sylow Theorem*).
2. *Second Sylow Theorem.* Let $P$ be a $p$-Sylow subgroup of $G$ and $Q$ a $p$-subgroup of $G$.
   d) Prove that the following defines an action of $Q$ on $G/P$:
   $$\forall q \in Q, \forall g \in G, q \cdot gP := (qg)P;$$

**Please turn over!**

e) Prove that the cardinality of any orbit is 1 or is divisible by $p$. Deduce that there is a fixed point $gP \in G/P$, and that $P$ contains a conjugate of $Q$.

Conclude: $p$-Sylow subgroups of $G$ are conjugate in $G$ (*Second Sylow Theorem*).

3. Let $n_p$ be the number of $p$-Sylow subgroup of $G$, and $P$ a $p$-Sylow subgroup of $G$.
   f) Prove that $P$ acts on $X := \{Q \text{ } p\text{-Sylow in } G\}$ by conjugation;
   g) Prove that the action above has precisely one fixed point, and that $p$ divides the size of the other orbits.

   Conclude: $p$ divides $n_p - 1$, that is, $n_p \equiv 1 \pmod{p}$ (*Third Sylow Theorem*).

**Solution (sketch):**

1. a) It is clear that for each $g \in G$ the left-translation map $g \cdot - : G \to G$ is a bijection, so that for $I \subseteq G$ we have that $|g \cdot I| = |I|$, and sets with $p^n$ elements are sent to sets with $p^n$ elements. This implies that it makes sense to define $G \times \mathcal{P} \to \mathcal{P}$ via $(g, I) \mapsto gI$. Of course $1_G I = I$, and $(gh)I = g(hI)$, so that we have indeed a group action.
   b) We have

$$|\mathcal{P}| = \binom{p^n h}{p^n} = \frac{p^n h \cdot \cdots (p^n h - p^n + 1)}{p^n} = \prod_{i=0}^{p^n - 1} \frac{p^n h - i}{p^n - i}$$

   and it is easily seen that each $p^n h - i$ is divisible by $p$ as many time as $p^n - i$ is (we say that a number is divisible $l$ times by $p$ if it is divisible by $p^l$ but not by $p^{l+1}$). This implies that $p$ does not divide $|\mathcal{P}|$, and since the orbits form a partition of $\mathcal{P}$, we have an orbit $\mathcal{O}$ whose cardinality is not divisible by $p$. Since the cardinality of $\mathcal{O}$ divides the cardinality of the group $G$ (why?), $|\mathcal{O}|$ divides $h$.
   c) Fixing $S_0 \in \mathcal{O}$, one can easily see that $\bigcup_{S \in \mathcal{O}} S = \bigcup_{g \in G} gS_0$, and that this union is the whole $G$. But the first union consisted of $|\mathcal{O}|$ sets of $p^n$ elements, and in order for it to be equal to the whole $G$ we need that $|\mathcal{O}| \geq h$. This, together with previous point, gives $|\mathcal{O}| = h$. Then, $|\mathrm{Stab}_G(S_0)| = p^n$ (why?), and this stabilizer is a $p$-Sylow of $G$, proving the First Sylow Theorem.
2. d) This is just the restriction of the action $G \to \mathrm{Sym}(G/P)$ (see previous Exercise for $H = P$).
   e) The cardinality of any orbit divides $|Q|$, which is a power of $p$. Hence orbits with more than 1 point have number of points equal to a multiple (positive power) of $p$. As the orbits form a partition of $G/P$ which has $h$ elements, some orbit must have just one point, meaning that there exists a fixed point. This means that for some $g \in G$ one has $QgP = gP$, i.e. $P \supseteq g^{-1}Qg$. If now we suppose that $Q$ is also a $p$-Sylow, then the inclusion above needs to be an equality (why?) and $P$ and $Q$ are conjugate.
3. f) Since conjugation leaves the cardinality unchanged it makes sense to let $G$ act on $X$ by conjugation. Then we can restrict the action to the subgroup $P$

**See next page!**

g) We have that each orbit has a cardinality dividing $|P| = p^n$, so that $X \setminus X^P$ is the union of all the orbits with a number of element divisible by $p$, meaning that $p$ divides $n_P - |X^P|$. Hence it is enough to prove that there is precisely one fixed point and we can conclude. Clearly, $P \in X^P$. Conversely, if $Q \in X^P$ then $gQg^{-1} = Q$ for every $g \in P$, so that $P \leq N_G(Q)$. As $Q \trianglelefteq N_G(Q)$, and $P$ and $Q$ are conjugate in $N_G(Q)$, we obtain $P = Q$ (why?). Hence the only fixed point is $P$.

Notice that for a fixed Sylow subgroup $P$, we have $n_p = |\{gPg^{-1}\}| = [G : N_G(P)]$. Since $P \leq N_G(P)$, we have that $h = [G : P]$ divides $n_p$. Moreover, we have that $n_p = 1$ if and only if $P$ coincides with all its conjugates, that is $n_P \trianglelefteq G$.