Solutions to Homework 8

Problem 1. Let G be a group and H a subgroup of G. Let $X = G/H$ be the set of all left cosets of H in G. Define $* : G \times X \longrightarrow X$ by $g * (aH) = (ga)H$.

a) Prove that $*$ is an action of G on X. Show that this action is transitive and that $St(aH) = aHa^{-1}$ for every $a \in G$.

b) According to the discussion in the lecture on October 9 (see the notes) this action corresponds to a homomorphism $\phi : G \longrightarrow S_X$. Prove that kernel of this homomorphism is the largest normal subgroup of G which is contained in H (i.e. that any normal subgroup of G which is contained in H is also contained in this kernel).

c) Suppose that G is finite and there is a prime divisor p of $|G|$ such that $1 < [G : H] < p$. Prove that G is not simple. Hint: Prove that the homomorphism ϕ from part b) is not injective.

d) Suppose that G is finite and that $[G : H]$ is equal to the smallest prime divisor p of $|G|$. Prove that H is normal in G. Hint: Consider the homomorphism ϕ from part b) and prove that $\ker \phi = H$.

Solution. a) First we check that $*$ is well defined: if $aH = bH$ then $b^{-1}a \in H$. But $b^{-1}a = (gb)^{-1}(ga)$, so $(ga)H = (gb)H$. This means that $*$ is well defined (i.e. independent on how we represent a given coset as xH).

Clearly

$$g * (h * aH) = g * ((ha)H) = (gha)H = (gh) * (aH)$$

and $e * aH = (ea)H = aH$, so $*$ satisfies all the conditions to be an action.

For any $a, b \in G$ we have $bH = (ba^{-1}a)H = (ba^{-1}) * aH$, so any two elements of X are in the same orbit. This means that there is only one orbit, i.e. the action is transitive.

Note first that $St(H) = \{g \in G : gH = H\} = H$. Thus $St(aH) = St(a * H) = aSt(H)a^{-1} = aHa^{-1}$.

b) Consider the homomorphism $G \longrightarrow \mathrm{Sym}(X)$ defined by this action. It sends $g \in G$ to the bijection $l_g : X \longrightarrow X, l_g(aH) = (ga)H$. Let K be the kernel of this homomorphism. K is a normal subgroup of G which consists of all elements $g \in G$ such that $gaH = aH$ for every $a \in G$. Taking $a = e$ we see that any $g \in K$ satisfies $gH = H$, i.e. $g \in H$. Thus $K < H$. Let L be any normal subgroup of G contained in H. Take any $g \in L$. If $a \in G$ then $a^{-1}ga \in L \subseteq H$. This means that $gaH = aH$. This shows that $g \in K$. This proves that $L \subseteq K$. In other words, K is the largest normal subgroup of G which is contained in H.

Remark: It is easy to see that K is the intersection of all the conjugates of H: $K = \bigcap_{g \in G} gHg^{-1}$. In general, the kernel of the permutation representation associated to an actions is the intersection of the stabilizers of all points.

c) the action of G on the set X of left cosets of H in G corresponds to a homomorphism $\psi : G \longrightarrow \mathrm{Sym}(X)$ as discussed in part b). Let $m = |X| = [G : H]$, so $m < p$. Thus $\mathrm{Sym}(X)$ is isomorphic to the symmetric group S_m. Note that $p||G|$ and $p \nmid |\mathrm{Sym}(X)| = m!$. Thus ψ can not be injective (otherwise, the image $\psi(G)$ would be a subgroup of $\mathrm{Sym}(X)$ of order $|G|$ divisible by p, which is not possible). Thus $\ker \psi$ is a non-trivial normal subgroup of G contained in H, so it is a proper subgroup. Thus G is not simple.

d) We keep the notation introduced in part c), so now $m = p$. Let $K = \ker \psi$. By the Fundamental Homomorphism Theorem, the image of ψ is isomorphic to G/K and it is a subgroup of $\mathrm{Sym}(X)$, so its order divides $p!$. It also divides $|G|$, so $|G/K|$ divides $\gcd(|G|, p!)$. Since all prime divisors of $|G|$ are larger or equal to p, we have $\gcd(|G|/p, (p-1)!) = 1$ so $\gcd(|G|, p!) = \gcd(|G|, p) = p$. Thus $|G/K|$ divides p, so it is equal to p (as $K \neq G$). Thus $[G : K] = p = [G : H]$. Since $K \subseteq H$, we must have $H = K$. Thus H is normal in G.

Problem 2. a) Find all Sylow 2−subgroups of S_4. Hint: The group S_4 can be considered as the group of all permutations of the vertices $1, 2, 3, 4$ of a square (numbered clockwise). It contains as a subgroup the dihedral group D_8 of order 8 (which consists of those permutations which are isometries; thus the rotation clockwise by 90 degrees is $R = (1, 2, 3, 4)$ and the reflection in the diagonal joining 1 and 3 is $S = (2, 4)$).

b) What is the number of Sylow 3−subgroups of S_4?

Solution: a) Using the hint, we see that that S_4 has a subgroup of order 8 isomorphic to D_4, namely

$$P = \{e, (1,2,3,4) = R, (1,3)(2,4) = R^2, (1,4,3,2) = R^3,$$
$$(2,4) = S, (1,4)(2,3) = SR, (1,3) = SR^2, (1,2)(3,4) = SR^3\}.$$

P is a Sylow 2-subgroup of S_4. By Sylow Theorem we know that all Sylow 2-subgroups are conjugate and their number t_2 divides 3. Note that

$$Q = (1,4)P(1,4)^{-1} = \{e, (4,2,3,1), (4,3)(2,1), (4,1,3,2),$$
$$(2,1), (1,4)(2,3), (4,3), (4,2)(3,1)\}$$

is not equal to P, so P is not normal and $t_3 > 1$. It follows that $t_3 = 3$, i.e. S_4 has 3 Sylow 2−subgroups. We already found two of them: P and Q. It is easy to find the third:

$$R = (1,2)P(1,2)^{-1} = \{e, (2,1,3,4), (2,3)(1,4), (2,4,3,1),$$
$$(1,4), (2,4)(1,3), (2,3), (1,2)(3,4)\}$$

is the third one. Thus P, Q, R are the Sylow 2−subgroups of S_4.

b) Note that a Sylow 3-subgroup of S_4 has order 3. Thus $P = \{e, (1,2,3), (1,3,2)\}$ $=< (1,2,3) >$ is a Sylow 3−subgroup of S_4 and $Q = \{e, (1,2,4), (1,4,2)\} =< (1,2,4) >$ is another one. Thus $t_3 > 1$. Now $t_3 \equiv 1 \pmod 3$ and $t_3 | 8$ by Sylow Theorem. The only possibility for t_3 is then $t_3 = 4$. It is easy to list the remaining two Sylow 3−subgroups, namely $R = \{e, (2,3,4), (2,4,3)\} =< (2,3,4) >$ and $S = \{e, (1,3,4), (1,4,3)\} =< (1,3,4) >$.

Problem 3. Let G be a finite group and let P be a Sylow p−subgroup of G (for some prime p).

a) Suppose that $f : G \longrightarrow H$ is a surjective homomorphism. Prove that $f(P)$ is a Sylow p−subgroup of H.

b) Let N be a normal subgroup of G. Prove that $P \cap N$ is a Sylow p−subgroup of N.

Solution: a) Let $|G| = p^a m$, $p \nmid m$, $K = \ker f$ and $|K| = p^b n$, $p \nmid n$. Since $|K| | |G|$, we have $b \leq a$ and $n | m$. By the Fundamental Homomorphism Theorem, H is isomorphic to G/K, so $|H| = p^{a-b} m/n$. Again by the Fundamental Homomorphism Theorem, $f(P)$ is

isomorphic to $P/(P\cap K)$. Since $P\cap K$ is a $p-$subgroup of K, $|P\cap K| = p^c$ for some $c \leq b$. Thus $|f(P)| = p^{a-c}$. On the other hand, $p^{a-c} = |f(P)||H|$, so $a - c \leq a - b$, i.e. $c \geq b$. Since $c \leq b$ and $c \geq b$, we have $c = b$ and $|f(P)| = p^{a-b}$, i.e. $f(P)$ is a Sylow $p-$subgroup of H.

b) Apply the solution to part a) when f is the quotient homomorphism $f : G \longrightarrow G/N$, so $H = G/N$ and $K = \ker f = N$. We have seen that if $|N| = |K| = p^b n$ with $p \nmid n$, then $|P \cap N| = |P \cap K| = p^b$. Thus $P \cap N$ is a Sylow $p-$subgroup of N.

Problem 4. Let G be a finite group of order pq, where $p < q$ are primes.

a) Show that G has a normal Sylow $q-$subgroup.

b) Suppose that $p \nmid (q - 1)$. Prove that G has a normal Sylow $p-$subgroup.

c) Suppose that $p \nmid (q - 1)$. Let P be the Sylow $p-$subgroup of G and let Q be the Sylow $q-$subgroup of G. Prove that $G \cong P \times Q$ conclude that G is cyclic.

Solution: a) Recall that the number t_q of Sylow $q-$subgroups of G satisfies $t_q|p$ and $t_q \equiv 1 \pmod q$. If $t_q \neq 1$ then $t_q \geq q + 1 > p$ which contradicts the condition $t_q|p$. Thus $t_q = 1$, i.e. G has normal Sylow q-subgroup Q.

b) As in part a), we have $t_p|q$ and $t_p \equiv 1 \pmod p$. The first condition implies that $t_p = 1$ or $t_p = q$. The latter case implies that $q \equiv 1 \pmod p$, which is excluded by our assumption that $p \nmid (q - 1)$. Thus $t_p = 1$ and G has normal Sylow $p-$subgroup P.

c) Note that the order of $P \cap Q$ divides both the order of P and the order of Q. Since these orders are relatively prime, we have $P \cap Q = \{e\}$. Since both P and Q are normal, we have $PQ \cong P \times Q$, so PQ has pq elements. Since PQ is contained in G and $|G| = pq$, we see that $PQ = G \cong P \times Q$. Note that P and Q has prime orders, so they are cyclic of orders p and q respectively: $P \cong \mathbb{Z}_p$ and $Q \cong \mathbb{Z}_q$. Since $\gcd(p, q) = 1$, we see that

$$G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

so G is cyclic.

Problem 5. This problem sketches a different proof of existence of Sylow $p-$subgroups. Let p be a prime. Let G be a finite group and suppose that every group of order smaller than $|G|$ has a Sylow $p-$subgroup (so this proof goes by induction on $|G|$). If $p \nmid |G|$, there is nothing to prove, so we assume that $p||G|$. We use the action of G on itself by conjugation. Recall that the stabilizer of an element $a \in G$ is simply its centralizer $C(a)$ and the orbit of a is the conjugacy classes of a. In particular, the fixed points of this action are the elements of the center $Z(G)$.

a) Prove that if $p \nmid |Z(G)|$ then there is a non-central element a whose conjugacy class has size not divisible by p. Then justify the following claims:

- $C(a)$ is a proper subgroup of G so it has a Sylow $p-$subgroup P by the inductive assumption;
- p does not divide the index $[G : C(a)]$;
- P is a Sylow p-subgroup of G.

b) Suppose that $p||Z(G)|$. Since $Z(G)$ is abelian, it has an element g of order p (we do not want to use Caychy's theorem here, only the special case for abelian groups since then we can derive Cauchy's theorem from the existence of Sylow subgroups). Show that $Q =< g >$ is a normal subgroup of G of order p. Consider the quotient homomorphism $f : G \longrightarrow G/Q$. Since $|G/Q| < |G|$, G/Q has a Sylow $p-$subgroup P. Prove that $f^{-1}(P)$ is a Sylow $p-$subgroup of G.

Solution: a) The orbits of the action of G on itself by conjugation are the conjugacy classes. Note that $Z(G)$ is the set of fixed points of the action so $|Z(G)|$ is the number of fixed points. If every orbit had either size 1 or size divisible by p, then (since orbits partition G) we would have $|G| \equiv |Z(G)| \pmod{p}$, which is false (since $p||G|$ and $p \nmid |Z(G)|$). Thus there is $a \in G$ whose orbit, i.e. conjugacy class, has size bigger than 1 and not divisible by p. In particular, a is non-central.

Since $C(a)$ is the stabilizer of a and a is not a fixed point, $C(a)$ is a proper subgroup of G so $|C(a)| < |G|$. Thus $C(a)$ has a Sylow p-subgroup P. Recall that $[G : C(a)]$ is equal to the size of the orbit of a, so $p \nmid [G : C(a)]$. Since $|G| = |C(a)|[G : C(a)]$, we see that the highest power of p which divides $|G|$ is the same as the highest power of p which divides $|C(a)|$, which equals the order of P. Thus P is a Sylow $p-$subgroup of G.

b) Since $g \in Z(G)$ has order p, the group $Q =< g >$ has order p. Since Q is in the center, Q is normal in G (every subgroup of the center is normal, since conjugation is trivial on the center). Let $|G| = p^a m$, $p \nmid m$. Then $|G/Q| = p^{a-1}m$. Thus G/Q has a Sylow $p-$subgroup P and its order is p^{a-1}. Note that the quotient homomorphism $f : G \longrightarrow G/Q$ maps the group $R = f^{-1}(P)$ onto P. It follows that R/Q is isomorphic to P. Thus $|R| = |P||Q| = p^{a-1}p = p^a$. It follows that $f^{-1}(P) = R$ is a Sylow $p-$subgroup of G.