1. G-SETS [s:gsets]

1.1. **First definitions.** [ss:gsetdef] Let G be a group. A *permutation representation of* G or G*-set* consists of a set X and a group homomorphism ρ from G into the group $\operatorname{Bij} X$ of bijections of X.[1] We often just say that X is a G-set, the homomorphism ρ being tacitly understood. Assuming that bijections act on the left,[2] we say more precisely that X is a *left* G-set and write gx or ${}^g x$ or $g \cdot x$ in place of $\rho(g)x$. If bijections act on the right, then X is a *right* G-set and we write xg or x^g or $x \cdot g$ for $(x)\rho(g)$.

Whereas it is common to see action from one side or the other being preferred exclusively, ambidexterity allows for simpler and more elegant notation. There is, in any case, the following standard way to convert right actions to left actions and vice-versa: ${}^g x := xg^{-1}$ and $x^g := g^{-1}x$. We will show a slight non-exclusive preference for the left. In particular, we will assume actions to be on the left unless the contrary is explicitly stated or obviously implied from the context. Convention

Let X be a G-set as above. Since ρ is a group homomorphism, $(gh)x = g(hx)$ and $1x = x$, where 1 denotes the identity element of G. Conversely, if for a set X, there is a map $G \times X \to X$ the image of (g, x) under which, denoted gx, satisfies $(gh)x = g(hx)$ and $1x = x$, then X is a left G-set.

A G*-morphism* or G*-map* $f : X \to Y$ of G-sets is any map such that $gfx = fgx$ for all g, x. We write $\operatorname{Mor}_G(X, Y)$ for the space of G-maps from X to Y. The space $\operatorname{End}_G X$ of G-endomorphisms of X is the centralizer in the semi-group $\operatorname{End} X$ of all self-maps of X of the image of G in $\operatorname{Bij} X \subseteq \operatorname{End} X$. G-maps

Any set X can be considered to be a G-set by the *trivial action*: $gx := x$. The power set of a G-set X is naturally a G-set: $gS := \{gx \mid x \in S\}$. If X and Y are G-sets, then so is the set $\operatorname{Mor}(X, Y)$ of all maps from X to Y: $({}^g f)(x) := g(f(g^{-1}x))$. The space of functions on X (values being taken in a set Y on which G acts trivially) is naturally a right G-set: $(f^g)x = f(gx)$. Constructing new G-sets out of given ones

1.1.1. Examples.

- There are several ways in which G acts on itself: by left multiplication which makes it a left G-set; by right multiplication which makes it a right G-set; by the conjugation action ${}^g x := gxg^{-1}$ which makes it a left G-set.
- The set G/H of left cosets of a subgroup H is a G-set: $g \cdot xH := gxH$.
- The group $\operatorname{Bij} X$ of bijections of a set X clearly acts on X. Such an action serves to define the group in the first place and is called the *defining representation*. Groups often arise in this way along with their defining representations.

1.2. **Orbits, stabilizers, and fixed points.** [ss:orb] Let x be an element of a G-set X. Its *orbit* is $Gx := \{gx \mid g \in G\}$ and *stabilizer* $G_x := \{g \in G \mid gx = x\}$; it is *fixed by* G if $G_x = G$. The set of elements of X fixed by G is denoted X^G. The action of G is *transitive* if X is a single orbit (of any of its points). A transitive G-set is sometimes also called a *homogeneous space*.

An elementary but important observation is the following:

$$Gx \cong G/G_x \quad \text{as } G\text{-sets} \tag{1.1}$$

[1] The set X could possibly be empty. In this case too, as when X is a singleton, $\operatorname{Bij} X$ is the trivial group $\{1\}$. This is analogous to the well-known convention $0! = 1$.

[2] Given self-maps ϕ and ψ of a set X, we have a choice as to the meaning given to their composition $\phi\psi$: either ψ could act first and then ϕ, or vice-versa. In the first case, we let the maps *act on the left*, i.e., we write $\psi(x)$ or just ψx for the image of x under ψ; in the second case, we write $(x)\psi$ or just $x\psi$.

In particular:

(1.2) every transitive G-set is of the form G/H for some subgroup H;

(1.3) the number of elements in an orbit of a finite group divides the order of the group.

Another equally elementary and important observation is:

(1.4) The orbits form a partition of a G-set.

In particular, when X is finite:

$$|X| = |X^G| + \sum |\text{orbit}| \tag{1.5}$$

where the sum is over the non-singleton orbits. Taking X to be a finite group acted upon by itself by conjugation, we get the *class equation*:

class equation

$$|G| = |\mathfrak{z}(G)| + \sum |\text{class}| \tag{1.6}$$

where $\mathfrak{z}(G)$ denotes the centre of G and the sum is over the non-singleton classes. Combining (1.5) with (1.3), we get:

(1.7) $|X| \equiv |X^G| \bmod p$ when X is finite and G a p-group.

[ss:gsetapply]

1.3. **Some applications.** We discuss some applications of the above observations to finite group theory.

1.3.1. p-groups. Letting X in (1.7) be the p-group itself acted upon by conjugation:

(1.8) The centre of a p-group is non-trivial.

Suppose now that G is a group of order p^2. Then $G/\mathfrak{z}(G)$ is of order 1 or p, and so cyclic. It follows that G is abelian, for we have the following simple observation:

(1.9) A group which is cyclic modulo a central subgroup is abelian.

[sss:sylow]

1.3.2. Sylow subgroups. Let G be a finite group, p a prime, and p^n the highest exponent of p that divides $|G|$. A subgroup of G of order p^n is called a *Sylow p-subgroup*. We first show, by induction on the order of G, that they exist. If $[G{:}H]$ is prime to p for a proper subgroup H, then we are done by applying the induction hypothesis to H. If not, then p divides every term in the sum on the right side of (1.6). Since p also divides G (there being nothing to prove otherwise), it follows that p divides $|\mathfrak{z}(G)|$. Let N be a subgroup of order p of $\mathfrak{z}(G)$. By induction, a p-Sylow of G/N exists, and pulling this back to G gives us a p-Sylow of G.

Existence of Sylow subgroups

Let P be a Sylow p-subgroup and H any p-subgroup. Consider the set X of G-conjugates of P, as a H-set (by conjugation). Apply (1.7). Since $|X| = [G{:}N(P)]$ is coprime to p, we conclude that X^H is non-empty. Which means that H normalizes some conjugate Q of P. But then QH is a p-subgroup containing Q, so $QH = Q$ and $H \subseteq Q$. We've proved:

(1.10) Any p-subgroup can be conjugated into any Sylow p-subgroup.

Conjugacy of Sylow p-subgroups

In particular:

> Any two Sylow p-subgroups are conjugate. A Sylow p-subgroup is normal if and only if it is the only Sylow p-subgroup. A Sylow p-subgroup is the unique such one in its normalizer. The normalizer of a Sylow p-subgroup is its own normalizer.

Consider the set X of all Sylow p-subgroups to be a P-set (under conjugation) and apply (1.7). Since P cannot normalize any other Sylow p-subgroup Q (if it did, QP would be a p-subgroup strictly containing P, a contradiction), it follows that $X^P = \{P\}$. We conclude:

The number of Sylow p-subgroups

(1.11) The number of Sylow p-subgroups is congruent to 1 modulo p. (It divides $|G|$ since the Sylow p-subgroups form an orbit of G.)

1.4. **Complements and exercises.** In the following, G is a group, H a subgroup, N a normal subgroup, X and Y are G-sets, and S is a subset of X. When an action of G on an element or subset of G is implied, it is the conjugation action.

The action of G on X is *faithful* if the only element of G that fixes every point of X is the identity; or, equilvalently, the kernel of the defining homomorphism $\rho : G \to \operatorname{Bij} X$ is trivial. Clearly $\operatorname{Ker} \rho = \cap_{x \in X} G_x$.

The *pointwise stabiliser* of S is the subgroup $G_S := \{g \in G \mid gs = s \ \forall\ s \in S\}$ and *(global) stabiliser* the subgroup $\operatorname{stab}_G S := \{g \in G \mid gS = S\}$. We call S a *G-subset* if $\operatorname{stab}_G S = G$.

1.4.1. $\operatorname{Mor}(X, Y)^G = \operatorname{Mor}_G(X, Y)$.

1.4.2. By *restricting* the action to H, we may consider X as a H-set.

1.4.3. If K is a group and $\pi : K \to G$ a group homomorphism, we can *pull back* the action on X to K: ${}^k x := {}^{\pi k} x$.

1.4.4. S is a $\operatorname{stab}_G S$-set in the obvious way. Being the kernel of the induced map $\operatorname{stab}_G S \to \operatorname{Bij} S$, the pointwise stabiliser G_S is normal in $\operatorname{stab}_G S$.

[sss:xn]

1.4.5. The set X^N of fixed points of N is a G-subset.

1.4.6. $G_{{}^g S} = {}^g G_S$ and $\operatorname{stab}_G {}^g S = {}^g \operatorname{stab}_G S$. Taking $S = \{x\}$, we see that elements that are in the same G-orbit have conjugate stabilisers.

1.4.7. If $G/H \cong G/K$ for a subgroup K of G, then H and K are conjugate.

1.4.8. Assume that G acts transitively on X and let x be an element of X.

- $\operatorname{Ker} \rho = \cap_{z \in X} G_z = \cap_{g \in G} G_{{}^g x} = \cap_{g \in G} {}^g G_x$, the largest normal subgroup of G contained in the stabiliser G_x.
- H too acts transitively on X if and only if $HG_x = G$ (here $HG_x := \{hz \mid h \in H, z \in G_x\}$).
- Let K a subgroup of the stabiliser G_x of x. Then the action of the normalizer $\mathrm{N}_G K$ on X^K (see 1.4.5) is transitive if and only if the only G-conjugates of K contained in G_x are the G_x-conjuagtes of K. Observe that the latter condition is satisfied when G_x is finite and K is a Sylow p-subgroup of G_x.

1.4.9. Prove without using the results of §1.3 Cauchy's theorem: a finite group whose order is divisible by a prime p contains an element of order p.

1.4.10. Let X be finite and p be a prime. Suppose that for every x in X, there is a p-subgroup P_x of G which fixes x but no other point. Then the action is transitive and $|X| \equiv 1 \bmod p$. Observe that this proves (1.10) and (1.11) once the existence of Sylow p-subgroups is known.

[ex:nnprime]

1.4.11. Assume G finite. If there is only one Sylow p-subgroup of G for every prime p, then G is a direct product of its Sylow p-subgroups. (Hint: Observe that if N and N' are normal subgroups with $N \cap N' = \{1\}$ then $NN' \cong N \times N'$.)

1.4.12. (Frattini argument) Let P be a Sylow p-subgroup of a finite normal subgroup N. Then $N \, \mathrm{N}_G \, P = G$. (Hint: See the second item in 1.4.8.) Slightly more generally, but still by the same argument, we have the following. Let E be a subset of a finite normal subgroup of N. Then $N \, \mathrm{N}_G \, E = G$ if and only if every G-conjugate of E is also an N-conjugate of E. Here $\mathrm{N}_G \, E := \{g \in G \mid E^g = E\}$.

1.4.13. Suppose that $|G| = p^n m$, where p is a prime, $(m, p) = 1$, and $p > m$. Then there is a unique Sylow p-subgroup in G. This subgroup is also normal.

1.4.14. Suppose that $|G| = pq^2$ with p and q being distinct primes. Then one of the following holds:

- $p > q$ and there is a normal Sylow p-subgroup.
- $q > p$ and there is a normal Sylow q-subgroup.
- $|G| = 12$ and there is a normal Sylow 2-subgroup.

1.4.15. Let $\mathbb{F}_q$ be the finite field of q elements where q is a power of a prime p. Let G be the group $\mathrm{GL}_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices with entries in $\mathbb{F}_q$. The subgroup of *unipotent* upper triangular matrices (i.e., upper triangular matrices that have all their diagonal entries equal to 1) is a Sylow p-subgroup of G. Its normalizer is the subgroup of all invertible upper triangular matrices.