3 Groups

In this lecture we will study the basic properties of groups, we will define them following [1] and then interpret our results in the language of the previous lectures.

3.1 Definition (Alternative definition). A group is a set S together with a function $S \times S \to S$ ($s, t \mapsto s \cdot t$), called the *product* and an element $e \in S$ called the *identity*. satisfying the following axioms

a) $e \cdot t = t \cdot e = t$ for all $t \in S$.

b) $s \cdot (t \cdot r) = (s \cdot t) \cdot r$ for all $s, t, r \in S$.

c) For every $s \in S$ there exists $t \in S$ such that $s \cdot t = e$.

3.2. Let $s \cdot t = e$ and let s' be such that $t \cdot s' = e$. Then multiplying the first equation by s' on the right and using associativity and the identity we have

$$s' = (s \cdot t) \cdot s' = s \cdot (t \cdot s') = s \cdot e = s.$$

It follows that t is both a left and right inverse to s. It will be denoted by s^{-1}.

Similarly, if t and t' satisfy $s \cdot t = s \cdot t' = e$, multiplying on both sides by s on the right, by what we just proved we obtain $t = t'$. Hence inverses are unique.

3.3. This definition is equivalent to the definition we saw before. In fact given a group G defined as category with one object, we let $S = \mathrm{Hom}(*, *)$, $\cdot$ be the composition of morphisms and $e = \mathrm{Id}_*$. Conversely, given a group S as above, we consider the category with only one object $*$ and with morphisms given by elements of S. From now on when we refer to a group G and elements $g \in G$ I will mean either an element of the corresponding set or a morphism in the corresponding category, understanding that they are the same.

3.4 Definition (yet another definition). A group is a set G together with three maps

$$* \xrightarrow{e} G, \qquad G \times G \xrightarrow{\cdot} G, \qquad G \xrightarrow{(\cdot)^{-1}} G,$$

called the *identity*, the *multiplication* and the *inverse* maps. Such that the following diagrams commute:

$$\begin{tikzcd}
* \times G \arrow[r, "e \times \mathrm{Id}_G"] \arrow[dr, "\pi_2"'] & G \times G \arrow[d, "\cdot"'] & G \times * \arrow[l, "\mathrm{Id}_G \times e"'] \arrow[dl, "\pi_1"] \\
& G &
\end{tikzcd} \tag{3.4.1}$$

$$\begin{tikzcd}
G \times G \times G \arrow[r, "\cdot \times \mathrm{Id}_G"] \arrow[d, "\mathrm{Id}_G \times \cdot"'] & G \times G \arrow[d, "\cdot"] \\
G \times G \arrow[r, "\cdot"'] & G
\end{tikzcd} \tag{3.4.2}$$

$$\begin{tikzcd}
G \arrow[r, "\Delta"] \arrow[dr] & G \times G \arrow[r, "(\cdot)^{-1} \times \mathrm{Id}_G"] & G \times G \arrow[d, "\cdot"'] & G \times G \arrow[l, "\mathrm{Id}_G \times (\cdot)^{-1}"'] & G \arrow[l, "\Delta"'] \arrow[dl] \\
& * \arrow[r, "e"'] & G & * \arrow[l, "e"] &
\end{tikzcd} \tag{3.4.3}$$

Equation (3.4.1) is equivalent to e being the identity of the multiplication. Equation (3.4.2) is equivalent to the associativity property and (3.4.3) is equivalent to the existence of inverses for the multiplication.

3.5 Examples.

a) The integers with the sum $(\mathbb{Z}, +)$, the non-zero rational numbers with the product $(\mathbb{Q}^\times, \cdot)$, the non-zero real numbers with the product $(\mathbb{R}^\times, \cdot)$ are examples of groups. These groups are all *Abelian or commutative*, in the sense that $a \cdot b = b \cdot a$ for all pairs $a, b \in G$. Notice that we need to take out the zero from $\mathbb{Q}$ in order to obtain a group, since it does not have a (multiplicative) inverse. In the case of $\mathbb{Z}$, even taking out the zero we would not obtain a group since there are no multiplicative inverses in $\mathbb{Z}$. Similarly for the natural numbers $\mathbb{N}$ with the addition, it is not a group since there are no additive inverses.

b) The group of *permutations* of n elements S_n is a group under composition, this is the group of bijective maps $\{1, \cdots, n\} \to \{1, \cdots, n\}$ where multiplication is the composition. More generally, for any set S, the set of bijective functions $f : S \to S$ is a group with composition as multiplication.

c) Let V be a vector space over the field k. The set of k-linear endomorphisms of V that are invertible is a group with composition as the multiplication. This group is not commutative if $\dim V > 1$. If we consider however all endomorphisms of V with addition as an operation, then we obtain a group.

   Suppose that $\dim V = n$ (in particular that it is finite). Then choosing a basis $\{e_1, \cdots, e_n\}$ for V we can express any linear automorphism of V as an invertible $n \times n$ matrix with coefficients in k. Conversely, any such matrix gives a linear automorphism of V. In other words, the set of invertible $n \times n$ matrices with coefficients in k is a group with multiplication of matrices as the operation. This group is typically denoted $GL_n(k)$.

d) These examples generalize as follows: let $\mathscr{C}$ be any category and a an object. Consider the set

$$\mathrm{Aut}(a) := \left\{\phi \in \mathrm{Hom}_{\mathscr{C}}(a, a),\ \phi \text{ is an isomorphism}\right\}.$$

   Then $\mathrm{Aut}(a)$ is a group with composition as the operation. *Homeomorphisms* of topological spaces, *diffeomorphisms* of smooth varieties, etc. fall into this class.

e) The group of 3×3 upper triangular matrices and entries in $\mathbb{R}$ with 1 on the diagonal is called the (real) Heisenberg group.

3.6 Definition. A *homomorphism* of groups is a function $f : G \to H$ such that $f(g \cdot g') = f(g) \cdot f(g')$. For a homomorphism f it follows that $f(e_G) = e_H$. Indeed we have

$$f(e) = f(e \cdot e) = f(e) \cdot f(e),$$

and multiplying by $f(e)^{-1}$ on both sides we obtain $f(e_G) = e_H$. It follows that the notion of *homomorphism* we have thus defined coincides with our previous definition as a functor.

3.7 Example. *A subset $H \subset G$ of a group G which is closed under the product and by taking inverses, is called a* subgroup. *For example, the set of all even integers is a subgroup of the integers with the addition. The set of all n-th roots of unit of $\mathbb{C}$, that is the set*

$$\left\{\zeta \in \mathbb{C} \,|\, \zeta^n = 1\right\},$$

is a subgroup of $(\mathbb{C}^\times, \cdot)$. In these cases, the inclusion $\iota : H \hookrightarrow G$ is a homomorphism of groups.

3.8. Let $f : H \to G$ be a morphism of groups. Then

$$\mathrm{im}(f) := f(H) \subset G, \qquad \ker(f) := f^{-1}(e_G) \subset H,$$

are subgroups. Indeed, for $a' = f(a)$, $b' = f(b)$ we have $a' \cdot b' = f(a \cdot b)$ hence $\mathrm{im}(f)$ is closed under products. Similarly from $e_G = f(e_H) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$ it follows that $\mathrm{im}(f)$ is closed under taking inverses.

As for $\ker(f)$ we notice that $e_H \in \ker(f)$ since $f(e_H) = e_G$, and if $a \cdot b \in \ker(f)$ we have $f(a) \cdot f(b) = f(a \cdot b) = e_G \cdot e_G = e_G$ hence $\ker(f)$ is closed under taking products and taking inverses (consider $b = a^{-1}$).

3.9. Let G be a group and $x \in G$ be any element. The *cyclic subgroup generated by x* is the set $H = \left\{\cdots, , x^{-2}, x^{-1}, e_G, x, x^2, \cdots\right\}$. It is the smallest subgroup of G containing x. There might be repetitions in this list. For example if there exists $n > 0$ such that $x^n = e_G$ then we will have $x^{kn} = e_G$ for every $k \in \mathbb{Z}$. Notice that if there are two different powers in this list that are equal, say $x^m = x^l$ for some $m \neq l \in \mathbb{Z}$. Then we will have $x^{m-l} = e_G$ and we are in the situation above. On the other hand, all the elements in that list are different we will call the group the "*infinite cyclic group*". Suppose that our subgroup H is not the infinite cyclic group. Then we have

Lemma. *The set $S = \left\{n \in \mathbb{Z} \mid x^n = e_G\right\}$ is a subgroup of $\mathbb{Z}$.*

Proof. Indeed this is simply the fact that the morphism $\mathbb{Z} \to G$ given by $n \mapsto x^n$ has S as a kernel. ☐

On the other hand we have

Lemma. *Every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer number n.*

Proof. The fact that $n\mathbb{Z}$ is a subgroup follows since the morphism $\mathbb{Z} \to \mathbb{Z}$, given by $m \mapsto n \cdot m$ has $n\mathbb{Z}$ as image. Conversely, let H be a subgroup of $\mathbb{Z}$. There are some cases to consider, if $H = 0$ then it is of the form required for $n = 0$. Conversely, there is some $0 < m \in H$ (pick any non-zero m and if it's negative consider it's inverse $-m$). There exists a smallest such m, call it n. I claim that $H = n\mathbb{Z}$. Indeed we have $n \in H$ and therefore $H' := n\mathbb{Z} \subset H$ since any element of H' can be written either as

$$\underbrace{n + \cdots + n}_{k\text{times}}, \qquad \text{or,} \quad \underbrace{n + \cdots + n}_{-k\text{times}}.$$

☐

On the other suppose that $H \supsetneq H'$ and let k be a positive integer in H and not in H'. Then since $-n \in H' \subset H$ we have $\{k - n \cdot l \mid l \in \mathbb{Z}\} \subset H$. In particular, there exists a minimal positive integer number r in this list with the property $0 \leq r < n$, namely the remainder in the division of k by n. By our assumptions that k was not in H' we have that $r > 0$ and since $r < n$ is in H we reach a contradiction.

Combining these two lemmas we see that if H is a cyclic group which is not the infinite cyclic group, nor the trivial group $\left\{e_G\right\}$ then there exists a minimal positive integer number m such that

$$H = \left\{e_G, x, x^2, \cdots, x^{m-1}\right\},$$

these powers are all distinct and $x^m = e_G$. This is called *a cyclic group of order m*.

3.10. We have a category **Grp** whose objects are groups and whose morphisms are homomorphisms of groups. Here are some properties of this category:

a) The trivial group $*$ with only one element is both an initial and a final object in this category. Indeed, given any group G there is a unique morphism $\pi : G \to *$ such that $\pi(g) = *$ for all $g \in G$. Similarly we have a unique morphism $* \to G$ by $* \mapsto e_G$.

b) Given a subgroup $H \subset G$ then the inclusion $\iota : H \hookrightarrow G$ is a *monomorphism* of groups. More generally, for any morphism $\phi : H \to G$ the inclusion $\ker(\phi) \hookrightarrow H$ is a *kernel* in the sense of the previous lecture (cf. Definition 2.11).

c) Given two groups G and H the product of sets $G \times H$ has a group structure defined by

$$(g,h) \cdot (g',h') := (g \cdot g', h \cdot h'), \qquad e_{G\times H} := (e_G, e_H).$$

The projections $G \times H \to G$ (resp. $G \times H \to H$) defined by $(g,h) \mapsto g$ (resp. $(g,h) \mapsto h$) are morphisms of groups. And by the universal property of products of sets, given any group K (in particular a set) with two homomorphisms $\pi_G : K \to G$, $\pi_H : K \to H$ there exists a unique map of sets[1] $\pi_{G\times H} : K \to G \times H$ given by $k \mapsto (\pi_K(g), \pi_H(h))$. Since each π_G and π_H are homomorphisms of groups it follows that $\pi_{G\times H}$ is a homomorphism of groups. Indeed we have

$$\pi_{G\times H}(k) \cdot \pi_{G\times H}(k') = \left(\pi_G(k), \pi_H(k)\right) \cdot (\pi_G(k'), \pi_H(k')) = \\ \left(\pi_G(k) \cdot \pi_G(k'), \pi_H(k) \cdot \pi_H(k')\right) = \left(\pi_G(k \cdot k'), \pi_H(k \cdot k')\right) = \pi_{G\times H}(k \cdot k').$$

We have proved thus:

Lemma. *The product $G \times H$ is a* product *in* **Grp** *in the sense of Example 2.5 d).*

d) Coproducts exists in the category of groups and their construction uses the notion of a *free product of groups* (cf. Exercise 3.28.1). In particular, products and coproducts are *not* isomorphic, hence the category of groups is not an additive category.

3.11 Isomorphisms. We say that two groups are isomorphic if there exists a bijective homorphism $\phi : H \to G$. Let $\phi^{-1} : G \to H$ be its inverse as a map of sets. Since ϕ is a morphism of groups we have

$$\phi\left(\phi^{-1}(a) \cdot \phi^{-1}(b)\right) = \phi\left(\phi^{-1}(a)\right) \cdot \phi\left(\phi^{-1}(b)\right) = a \cdot b = \phi(\phi^{-1}(a \cdot b)).$$

Applying ϕ^{-1} to this equation we get

$$\phi^{-1}(a) \cdot \phi^{-1}(b) = \phi^{-1}(a \cdot b),$$

hence ϕ^{-1} is also a homomorphism of groups and ϕ is an isomorphism in the sense of 1.4.

We may have non-trivial isomorphisms from G to itself: $\phi : G \to G$. These will be called *automorphisms* of G. Of course the identity map is such an automorphism. But for the cyclic group of order 3, $G = e, x, x^2$ such that $x^3 = e$, the following is an automorphism:

$$e \mapsto e, \qquad x \mapsto x^2, \qquad x^2 \mapsto x.$$

3.12 Conjugation. More generally, for any element $g \in G$ we have an automorphism Ad_g of G given by

$$h \mapsto \mathrm{Ad}_g(h) := ghg^{-1}.$$

It is indeed an automorphism as

$$\mathrm{Ad}_g(h \cdot h') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = \mathrm{Ad}_g(h) \cdot \mathrm{Ad}_g(h').$$

If G is Abelian, then for any $g \in G$ we have $\mathrm{Ad}_g = \mathrm{Id}_G$. More generally, consider the set $\mathrm{Aut}(G)$ of all automorphisms of G, this is a group with composition as the multiplication as in Example 3.5 d). Indeed, given two automorphisms ϕ, ψ of G, we have already noticed in 3.11 that ϕ^{-1} is an automorphism. As for the multiplication we have

$$\phi \circ \psi(g \cdot g') = \phi\left(\psi\left(g \cdot g'\right)\right) = \phi\left(\psi(g) \cdot \psi(g')\right) = \phi(\psi(g)) \cdot \phi\left(\psi(g')\right).$$

[1] Unique in the sense that it makes the diagram of 2.3 commute.

Lemma. *The map $G \to \operatorname{Aut}(G)$, $g \mapsto \operatorname{Ad}_g$ is a morphism of groups.*

Proof. This is simply the statement that

$$\operatorname{Ad}_{gg'} h = gg'h(gg')^{-1} = gg'h(g')^{-1}g^{-1} = \operatorname{Ad}_g \left(g'h(g')^{-1}\right) = \operatorname{Ad}_g \circ \operatorname{Ad}_{g'} h.$$

□

As with any homomorphism of groups, the kernel and the image of this map are subgroups. We call the *center* of G, and denote it by $Z(G)$ its kernel, and by *inner automorphisms* and denote it by $\operatorname{Inn}(G)$ the image.

3.13 Definition. A subgroup $H \subset G$ is called *normal* if it is stable by conjugation by G, that is, for every $h \in H$ and $g \in G$, $ghg^{-1} \in H$.

3.14 Lemma. *The kernel of a homomorphism $\varphi : H \to G$ is a normal subgroup.*

Proof. Let $h \in \ker(\varphi)$ and $g \in H$, we have

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e.$$

□

3.15. The image of a homomorphism might not be a normal subgroup (consider the inclusion of a non-normal subgroup). We have however:

Lemma. $\operatorname{Inn}(G) \subset \operatorname{Aut}(G)$ *is a normal subgroup*

Proof. Let $\phi \in \operatorname{Aut}(G)$ we have

$$\phi \operatorname{Ad}_g \phi^{-1}(h) = \phi\left(g\phi^{-1}(h)g^{-1}\right) = \phi(g)h\phi(g)^{-1} = \operatorname{Ad}_{\phi(g)}(h),$$

for all $h \in G$, therefore $\phi \operatorname{Ad}_g \phi^{-1} = \operatorname{Ad}_{\phi(g)} \in \operatorname{Inn}(G)$. □

3.16. Let $H \subset G$ be a subgroup, not necessarily normal. Consider the set

$$\operatorname{Ad}_g H = gHg^{-1} = \left\{ghg^{-1}, \| h \in H\right\} \subset G.$$

We have $ghg^{-1}gh'g^{-1} = ghh'g^{-1}$ so that gHg^{-1} is closed under the product and considering $g^{-1}h^{-1}g$ we see it is also closed under inverses, hence it is a subgroup of G. We will say that two subgroups H, H' of G are *conjugated* if there exits $g \in G$ such that $gHg^{-1} = H'$.

3.17 Group Actions. Recall that for any group G, we have another group G^{op} which is G as a set, but with the multiplication defined by $g \cdot^{op} h := h \cdot g$.

A *right action* of a group G on a set S is a homomorphism of groups $\rho : G^{op} \to \operatorname{Aut}(S)$. Equivalently, we may use Definition 3.4 replacing the leftmost copy of G in the diagrams by S, namely, a right action of a group G on a set S is a map $S \times G \xrightarrow{\cdot} S$ making the following diagrams commute:

$$\begin{tikzcd} S \times G \arrow[d, "\cdot"'] & S \times * \arrow[l, "\mathrm{Id}_S \times e"'] \arrow[dl, "\pi_1"] \\ S & \end{tikzcd} \tag{3.17.1}$$

$$
\begin{tikzcd}
S \times G \times G \arrow[r, "\cdot \times \mathrm{Id}_G"] \arrow[d, "\mathrm{Id}_S \times \cdot"'] & S \times G \arrow[d, "\cdot"] \\
S \times G \arrow[r, "\cdot"'] & S
\end{tikzcd}
\tag{3.17.2}
$$

The equivalence between this definition and the previous one is simply given by declaring $\rho(g)(s) = s \cdot g$. The first diagram says that the identity of e acts as the identity automorphism ($\rho(e) = \mathrm{Id}_S$), and the second diagram is equivalent to ρ being a group homomorphism: $\rho(g) \circ \rho(h) = \rho(hg)$

3.18 Examples.

a) Let $\phi : H \to G$ be a homomorphism of groups. Then H acts on the right of G by right multiplication, namely the action map is simply $g \cdot h := g \cdot \phi(h)$.

b) The group of permutations of n elements acts on the right on the set $1, \cdots, n$ as follows. For a permutation $\sigma \in S_n$, we let $\rho(\sigma)(i) = \sigma^{-1}(i)$ for $1 \leq i \leq n$.

c) The group G acts on itself on the right in two different ways. First as in a) taking $\phi = \mathrm{Id}_G$, that is by right multiplication. Second by *conjugation*. Indeed we may define $\rho(g) = \mathrm{Ad}_{g^{-1}}$ and by definition is a homomorphism $G^{op} \to \mathrm{Aut}(G)$.

3.19. Let G be a group acting on the right on S. We then have an equivalence relation on S by declaring $s \sim t$ if there exists $g \in G$ such that $s \cdot g = t$. Indeed we have

reflexivity $s \sim s$ by taking $g = e$.

symmetry Let $s \sim t$ so that we have $s \cdot g = t$. Then $t \cdot g^{-1} = s$ and $t \sim s$.

transitivity Let $s \sim t$ and $t \sim u$, that is we have g and h in G with $s \cdot g = t$ and $t \cdot h = u$. Then $(s \cdot g) \cdot h = s \cdot (g \cdot h) = u$ and $s \sim u$.

The set of equivalence classes $S/$ is typically denoted by S/G. We have the map of sets $S \to S/G$, $s \mapsto [s]$, which assigns to each element $s \in S$ its equivalence class.

3.20 Example (Cosets). *One of the most important examples will be the quotient G/H where $H \subset G$ is a subgroup. The action here is defined as in Example 3.18 a). The equivalence classes are called the* right H-cosets of G.

3.21. Let G be a group acting on the right on the set S. The action is said to be *transitive* if the set $S/G \simeq *$, that is, for every pair $s, t \in S$ there exists $g \in G$ such that $s \cdot g = t$.

For each element $s \in S$, the subset

$$
G_s := \{g \in G | s \cdot g = s\},
$$

is a subgroup of G called the *stabilizer* or the *isotropy* of s. Indeed the identity element belongs to G_s for any s. Also if $g, h \in G_s$ then we have $(s \cdot g) \cdot h = s \cdot (gh) = s$ hence $gh \in G_s$. Finally if $g \in G_s$ we have $s \cdot g^{-1} = (s \cdot g) \cdot g^{-1} = s \cdot e = s$ hence $g^{-1} \in G_s$.

Let $h \in G_s$ and $g \in G$ be arbitrary. Define $t = s \cdot g^{-1}$.

$$
t \cdot (g \cdot h \cdot g^{-1}) = s \cdot h \cdot g^{-1} = t.
$$

Hence it follows that $gG_s g^{-1} = G_{s \cdot g^{-1}}$. In other words, for any two representatives of the same class $[s] \in S/G$, the isotropy groups are conjugated.

When G acts on itself by multiplication on the right, the isotropy group is trivial, that is $G_g = \{e\}$ for all g. On the other hand when G acts on itself by conjugation as in 3.18 c) the isotropy group of g is called the *centralizer of* g.

3.22. If G is a finite group, we have an equality $|G/H| = |G|/|H|$ since for each coset gH we have a bijection $H \simeq gH$ given by $h \mapsto g \cdot h$ (the stabilizer of any g is trivial). Since the whole set G is the disjoint union of its equivalence classes and each equivalence class has $|H|$ elements, we obtain the result. In particular we see that the order of a subgroup divides the order of a group. We define the *index* of H in G, $[G : H]$ as that quotient.

For infinite groups we may still make sense of the index as the number of elements in G/H, allowing this number to be infinite.

3.23 Commuting Actions. Sometimes the same set has *two commuting actions* of the group G (or even different groups) in a natural way. Suppose H and G are two groups such that H acts on the left and G acts on the right of S. We say that these actions *commute* if for every $s \in S$, $h \in H$ and $g \in G$ we have $(h \cdot s) \cdot g = h \cdot (s \cdot g)$. For example the group G has two commuting actions of G on itself. Or if G is a group and H, K are two subgroups, the actions of H by left multiplication and of K by right multiplication on G commute.

Let S be a set with two commuting actions of H and G as above. Then we have the set $H\backslash S$ (defined in the same way as for right cosets) of equivalence classes for the H action. The group G still acts on this set. Indeed let $[s]$ be a class, we define

$$[s] \cdot g := [s \cdot g].$$

This action is well defined since if t is another representative of the same class, namely $[t] = [s]$ then we have $h \in H$ such that $h \cdot s = t$ and $t \cdot g = (h \cdot s) \cdot g = h \cdot (s \cdot g)$, hence $[t \cdot g] = [s \cdot g]$. I leave it to you to check that this is indeed an action!

3.24 Definition. Let S and T be two sets with G-actions on the right. We define a *homomorphism* of sets with a right G-action to be a map of sets $\phi : S \to T$ such that

$$\phi(s \cdot g) = \phi(s) \cdot g, \qquad \forall s \in S, t \in T, g \in G.$$

With this definition, we obtain a category $\mathbf{G-Set}$ of sets with right G-actions.

3.25 Orbits. Let G be a group acting on S. Let $s \in S$ and consider the set

$$s \cdot G = \{s \cdot g | g \in G\} \subset S.$$

It is called the *right G-orbit* of s. It is clear that G acts transitively on $s \cdot G$. Moreover, we have a map of sets

$$G \to s \cdot G, \qquad g \mapsto s \cdot g.$$

The isotropy subgroup $G_s \subset G$ is sent to s by this map. Moreover, suppose there are two $g, h \in G$ such that $s \cdot g = s \cdot h$, then $hg^{-1} \in G_s$ and therefore there exists $f \in G_s$ such that $f \cdot g = h$. Indeed consider G with the two commuting actions of the subgroup G_s on the left and G on the right. As in 3.23, the set $G_s\backslash G$ has a right action of G. The map above descends to an isomorphism in $\mathbf{G-Set}$

$$\varphi : G_s\backslash G \xrightarrow{\sim} s \cdot G. \tag{3.25.1}$$

We have already checked that φ is injective. Surjectivity is clear, as is the compatibility with the right G-actions.

3.26 Corollary. *Suppose S and G are finite sets, then for any $s \in S$ we have an equality*

$$|G| = |G_s| \cdot |s \cdot G|.$$

Proof. By the isomorphism (3.25.1) this is equivalent to checking $|G_s \backslash G| = |G|/|G_s|$ which in turn is the statement in 3.22. □

3.27 Corollary. *Let G be a finite group $g \in G$ be any element. Let $C(g)$ be the set of elements in G conjugated to g, C_g be the centralizer of g in G, then*

$$|G| = |C(g)||C_g|,$$

in particular both numbers on the right divide the order of the group G.

Proof. Applying the previous Corollary to the case when $S = G$ with the action by conjugation, $s = g \in G$ and G_s is the centralizer of g while $s \cdot G$ is the conjugation class of g. □

3.28 Exercises

3.28.1. Let G, H be two groups. And consider the set consisting on all finite sequences $\{a_1, a_2, a_3, \cdots\}$ where a_i either belongs to G or H. We *reduce* the sequence by applying the following operations.

a) We remove any appearance of the identity element from either group.

b) Replace any pair of consecutive $a_i a_{i+1}$ by their product if both are elements from the same group.

Then every *reduced word* is an alternating sequence (possibly empty) $\{g_1, h_1, g_2, h_2, \cdots\}$ of elements in G and H. The free group $G * H$ is the group whose elements are the reduced words with the operation of concatenation (and then reduction).

Prove that $G * H$ is a coproduct in the category of groups.

3.28.2. Check that the two given definitions of a right action of G on S given in 3.17 are equivalent. Give the corresponding definitions for a *left action* of G on S.

3.28.3. Let $GL_n(k)$ be the group of invertible $n \times n$ matrices with entries in k. Let $Gr(r, n)$ be the set of r-dimensional sub-vector spaces of $k^{\oplus n}$. Show that $GL_n(k)$ naturally acts transitively on $Gr(r, n)$. What is the stabilizer of a given sub-vector space?

3.28.4. Show that the relation $H \sim H'$ if H and H' are conjugated subgroups of G is an equivalence relation on the set of all subgroups.

3.28.5. Prove that two commuting actions of H and G on S as in 3.23 is equivalent to a homomorphism of groups $H \times G^{op} \to \mathrm{Aut}(S)$.

3.28.6. Let S be a set with two commuting actions of H and G. Show that $H \backslash S$ has a right action of G and S/G has a left action of H.

References

[1] Michael Artin. *Algebra.* Englewood Cliffs, N.J., 1991.