

# GROUPS, RINGS AND GALOIS THEORY

PATRICK BROSANAN

## 1. SETS

**1.1. Prerequisites.** I have tried to assume as little as possible. However, I do assume basic facts about integers and congruences from **Math 312** or **Math 322**. I also work with sets in the Gödel-Bernays system. This means, for example, that I assume the existence of a class of all sets. The basic idea of this theory is that a class  $X$  is a set iff the relation  $X \in Y$  is true for some class  $Y$ . The class of all sets is then not a set. The reader interested in the Gödel-Bernays axioms can find them, for example, in Paul Cohen's book *Set theory and the continuum hypothesis*.

**1.2. General notation.** I write  $a := b$  to indicate that  $a$  is defined as being equal to  $b$ . If I am defining a new concept, I try to put the name of the concept in *italics*. I write  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  for the sets of integers, rationals, reals and complex numbers respectively. I write  $\mathbb{N} := \{n \in \mathbb{Z} : n \geq 0\}$  and call this the set of *natural numbers*. I write  $\mathbb{Z}_+ := \{n \in \mathbb{Z} : n > 0\}$ .

If  $a, b, d \in \mathbb{Z}$ , I write  $d|a$  to mean that  $d$  divides  $a$ , that is, there exists  $m \in \mathbb{Z}$  such that  $md = a$ . I write  $a \equiv b \pmod{d}$  to mean that  $d|(a-b)$ .

We begin with a few preliminaries about sets. In fact, our motivation for the entire class is to think of groups in terms of their actions on sets. We, therefore, review a little bit of elementary set theory to fix notation.

**1.3.** We write **Sets** for the class of all sets. If  $X, Y \in \mathbf{Sets}$ , we write  $\text{Hom}_{\mathbf{Sets}}(X, Y)$  for the set of all function  $f : X \rightarrow Y$  from  $X$  to  $Y$ . If  $f \in \text{Hom}_{\mathbf{Sets}}(X, Y)$  then  $f$  is *injective* (or *one-to-one*, a *monomorphism*, or simply *mono*) if the following statement holds:

$$(1.3.1) \quad \forall a, b \in X [f(a) = f(b) \Rightarrow a = b].$$

We say that  $f$  is *surjective* if

$$(1.3.2) \quad \forall y \in Y, \exists x \in X f(x) = y.$$

A function  $f : X \rightarrow Y$  is an *isomorphism of sets* if  $f$  is both injective and surjective. We write

$$\text{Isom}_{\mathbf{Sets}}(X, Y) := \{f \in \text{Hom}_{\mathbf{Sets}}(X, Y) : f \text{ is an isomorphism.}\}$$

We write  $\text{Aut}_{\mathbf{Sets}}(X) := \text{Isom}_{\mathbf{Sets}}(X, X)$ . These are the *automorphisms* of  $X$ .

**1.4.** If  $X \in \mathbf{Sets}$ , I write  $|X|$  to denote the cardinality of  $X$ . Recall that  $X$  is said to be *finite* if  $|X| \in \mathbb{N}$ .

**1.5.** If  $f \in \text{Hom}_{\text{Sets}}(X, Y)$ ,  $g \in \text{Hom}_{\text{Sets}}(Y, Z)$ , then we write  $g \circ f$  (or sometimes just  $gf$ ) for the composition of  $g$  with  $f$ . (Thus,  $g \circ f \in \text{Hom}_{\text{Sets}}(X, Z)$ .) For  $x \in X$ , we have, by definition,  $(g \circ f)(x) = g(f(x))$ . If  $h \in \text{Hom}_{\text{Sets}}(Y, Z)$ , then it is easy to see that

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

In other words, composition is *associative*.

**1.6.** Recall that a set is determined by its elements. (We take this as an axiom of set theory.) There is exactly one set with no elements, the empty set, written  $\emptyset$ . A set  $X$  is a *singleton* if it has exactly one element.

**1.7.** We sometimes call a function  $f \in \text{Hom}_{\text{Sets}}(X, Y)$  a *map* of sets. If  $f : X \rightarrow Y$  is injective (resp. surjective) we sometimes indicate this by writing  $f : X \hookrightarrow Y$  (resp.  $f : X \twoheadrightarrow Y$ ). If  $A \subset X$  and  $B \subset Y$ , then

$$f(A) := \{f(a) : a \in A\}, \quad f^{-1}(B) := \{x \in X : f(x) \in B\}.$$

The set  $f(A)$  is called the *image* of  $A$ , and the set  $B$  is called the *inverse image* of  $B$ . Clearly,  $f$  is surjective if and only if  $f(X) = Y$  and  $f$  is injective iff, for every  $y \in Y$ ,  $f^{-1}\{y\}$  is either empty or a singleton.

**1.8.** If  $X \in \text{Sets}$ , we write  $\text{End}_{\text{Sets}}(X) := \text{Hom}_{\text{Sets}}(X, X)$ . We write  $\text{id}_X$  for the identity function on  $X$ :  $\text{id}_X(x) = x$ . If  $f \in \text{Hom}_{\text{Sets}}(X, Y)$ , then  $g \in \text{Hom}_{\text{Sets}}(Y, X)$  is said to be a left (resp. right) inverse of  $f$  if  $g \circ f = \text{id}_X$  (resp.  $f \circ g = \text{id}_Y$ ). If  $X \neq \emptyset$ , then a function  $f : X \rightarrow Y$  is injective iff it has a left inverse. This is an elementary fact of set theory. Similarly, if  $X$  is any set, a map  $f : X \rightarrow Y$  is surjective iff it has a right inverse. This is a consequence of the axiom of choice. (In fact, is equivalent to the axiom of choice given the other usual axioms of set theory.) It is easy to see (without the axiom of choice) that  $f$  has both a left and a right inverse iff  $f$  is an isomorphism. Moreover, if  $f$  is an isomorphism,  $f$  has a unique left inverse  $g$  which is also the unique right inverse.

## 2. GROUPS

**Proposition 2.1.** *Suppose  $X \in \text{Sets}$ , then composition on the set  $\text{Aut}_{\text{Sets}}(X)$  has the following properties*

- (1) *If  $f, g, h \in \text{Aut}_{\text{Sets}} X$ , then  $f(gh) = (fg)h$ .*
- (2) *For all  $f \in \text{Aut}_{\text{Sets}} X$ ,  $\text{id}_X f = f \text{id}_X = f$ .*
- (3) *For all  $f$  in  $\text{Aut}_{\text{Sets}} X$ , there exist a unique  $g \in \text{Aut}_{\text{Sets}} X$  such that  $fg = gf = \text{id}_X$ .*

We abstract these properties to get the notion of a group.

**Definition 2.2.** A *group* is a set  $G$  and a binary operation  $G \times G \rightarrow G$  written  $(x, y) \mapsto xy$  such that

- (1) for all  $x, y, z \in G$ ,  $(xy)z = x(yz)$ ;
- (2) there exists  $1 \in G$  such that, for all  $x \in G$ ,  $x1 = 1x = x$ ;
- (3) for all  $x \in G$ , there exists  $x^{-1} \in G$  such that  $xx^{-1} = x^{-1}x = 1$ .

**Remark 2.3.** To be precise, we should consider a group to be a *ordered pair*  $(G, m)$  where  $G$  is a set and  $m : G \times G \rightarrow G$  is a map satisfying the properties enumerated in Definition 2.2. However, doing this is usually unweildy so we almost always abuse notation and write  $G$  for the group. When we need to

refer to the the set  $G$  in the pair  $(G, m)$  we refer to it as the *underlying set* of the group  $G$ . The map  $m : G \times G \rightarrow G$  is called the *multiplication*.

**2.4.** If  $G$  is a group then the element  $1$  is unique. It is called the *identity element*. Similarly, for each  $x \in G$ , the element  $x^{-1}$  is unique.

**Definition 2.5.** We say that a group  $G$  is *abelian* if, for every  $a, b \in G$ ,  $ab = ba$ .

Often if  $G$  is abelian the multiplication is written additively. For example, the set  $\mathbb{Z}$  of integers form an abelian group under addition.

**Exercise 2.6.** Show that the group  $\text{Aut}_{\text{Sets}}(X)$  is abelian iff  $|X| \leq 2$ .

**2.7.** A non-empty subset  $H \subset G$  of a group  $G$  is called a *subgroup* if it satisfies the following axiom

$$\forall a, b \in H, ab^{-1} \in H.$$

We say that a subgroup  $H$  of  $G$  is a *proper* subgroup if  $H \neq G$ . We write  $H \leq G$  (resp.  $H < G$ ) if  $H$  is a subgroup (resp. proper subgroup) of  $G$ .

**Exercise 2.8.** If  $G$  is a set, then a subset  $H \subset G$  is a subgroup if and only, for all  $a, b \in H$ ,  $ab \in H$ , and  $H$  with this product forms a group.

**Proposition 2.9.** If  $\{H_i\}_{i \in I}$  is a collection of subgroups of a group  $G$ , then the intersection  $\bigcap_{i \in I} H_i$  is also a subgroup of  $G$ .

*Proof.* This is obvious from the definition. □

**Definition 2.10.** We write  $\mathbf{Gps}$  for the class of all groups. A map  $f : G \rightarrow H$  between groups (i.e. a map of their underlying sets) is a *homomorphism* if, for all  $a, b \in G$ ,  $f(ab) = f(a)f(b)$ . We write  $\text{Hom}_{\mathbf{Gps}}(G, H)$  for the set of all group homomorphism. Obviously,  $\text{Hom}_{\mathbf{Gps}}(G, H) \subset \text{Hom}_{\text{Sets}}(G, H)$ .

**2.11.** Note that, if  $f \in \text{Hom}_{\mathbf{Gps}}(G, H)$  then

$$f(1) = (f(1)^{-1}f(1))f(1) = f(1)^{-1}f(1) = 1.$$

Also note that, for  $g \in G$ ,

$$f(g)^{-1} = f(1)f(g)^{-1} = f(g^{-1})f(g)f(g)^{-1} = f(g^{-1}).$$

**2.12.** A homomorphism is injective (resp. surjective) if it is as a map of the underlying sets.

**Proposition 2.13.** Suppose  $f : G \rightarrow H$  is a homomorphism, and  $A \leq G$ ,  $B \leq H$  are subgroups. Then

- (1)  $f(A) \leq H$ ;
- (2)  $f^{-1}(B) \leq G$ .

*Proof.* (1) Suppose  $x, y \in A$ , then  $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(A)$ .

(2) Suppose  $x, y \in f^{-1}(B)$ , then

$$f(xy^{-1}) = f(x)f(y)^{-1} \in B.$$

□

**Definition 2.14.** If  $f : G \rightarrow H$  is a group homomorphism, then we write  $\ker f := f^{-1}(\{1\}) \leq G$ . This subgroup is called the *kernel* of  $f$ .

**Definition 2.15.** Suppose  $S \subset G$  is a set. The subgroups  $\langle S \rangle$  of  $G$  generated by  $S$  is the intersection of all subgroups of  $H$  of  $G$  containing  $S$ . We say that  $G$  is *cyclic* if it is generated by 1 element.

**2.16.** If  $n \in \mathbb{Z}$ , we write  $n\mathbb{Z} := \{nm : m \in \mathbb{Z}\}$ . This is clearly a subgroup of  $\mathbb{Z}$ . In fact, every subgroup of  $\mathbb{Z}$  is of this form. To see this, suppose  $H \leq \mathbb{Z}$ . If  $H = \{0\}$ , then clearly  $H = 0\mathbb{Z}$ . Otherwise, there exists a smallest positive element  $n$  of  $H$ . I claim that  $H = n\mathbb{Z}$ . In fact, this is a simple consequence of the long division algorithm: take  $m \in H$ . Then, we can write  $m = nd + r$  with  $0 \leq r < d$ . Therefore  $r = m - nd \in H$ . Thus  $r = 0$  by the minimality of  $n$ . Thus  $m \in n\mathbb{Z}$ .

**Definition 2.17.** Let  $G$  be a group and  $g \in G$ . If, for every positive integer  $n$ ,  $g^n \neq 1$ , then  $g$  is said to have order equal to  $+\infty$ . Otherwise, the order of  $g$  is the smallest positive integer  $n$  such that  $g^n = 1$ .

**Definition 2.18.** If  $G$  and  $H$  are groups then we define a multiplication on the product  $G \times H$  by  $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ . With this multiplication,  $G \times H$  is then a group. Note that  $G \cong G \times \{1\} \leq G \times H$  via the map  $g \rightarrow (g, 1)$  and  $H \cong \{1\} \times H$ . More generally, suppose  $(G_i)_{i \in I}$  is a collection of groups. Then the product  $\prod_{i \in I} G_i$  is a group with the multiplication given by  $(g_i)(g'_i) = (g_i g'_i)$ . The map  $G_i \rightarrow \prod_{i \in I} G_i$  given by sending  $g \in G_i$  to the element  $(g_j)_{j \in I}$  with  $g_j = g$  for  $j = i$  and  $g_j = 1$  otherwise is an injective homomorphism.

**Definition 2.19.** Let  $\{G_i\}_{i \in I}$  be a family of groups as above. We define the *direct sum* of the  $G_i$  to be the subset  $\bigoplus_{i \in I} G_i$  of  $\prod_{i \in I} G_i$  consisting of elements  $(g_i)_{i \in I}$  such that  $g_i = 1$  for all but finitely many  $i$ . It is easy to see that the direct sum is a subgroup of the direct product. (They are clearly equal if  $I$  is finite.) Moreover, it is the subgroup of the direct product generated by the  $G_i \subset \prod_{i \in I} G_i$ .

### 3. GROUP ACTIONS

**Definition 3.1.** An *action* of a group  $G$  on a set  $S$  is a homomorphism  $\varphi : G \rightarrow \text{Aut}_{\text{Sets}} S$ .

**3.2.** An action as above defines a map  $a : G \times S \rightarrow S$  given by  $(g, s) \mapsto \varphi(g)s$  known as the *action map*. Sometimes, when  $\varphi$  is understood, we simply write  $gs$  instead of  $\varphi(g)s$ .

**3.3.** If we let  $m : G \times G \rightarrow G$  denote the multiplication map, the diagram

$$(3.3.1) \quad \begin{array}{ccc} G \times G \times S & \xrightarrow{m \times \text{id}_S} & G \times S \\ \downarrow \text{id}_G \times a & & \downarrow a \\ G \times S & \xrightarrow{a} & S \end{array}$$

is commutative. (This means simply that  $a \circ (m \times \text{id}_S) = a \circ (\text{id}_G \times a)$ .) To see this, note that

$$\begin{aligned} a \circ (m \times \text{id}_S)(g_1, g_2, s) &= a(g_1g_2, s) \\ &= \varphi(g_1g_2)s \\ &= \varphi(g_1)\varphi(g_2)s = \varphi(g_1)a(g_2, s) = a(g_1, a(g_2, s)). \end{aligned}$$

Conversly, suppose  $a : G \times S \rightarrow S$  is a map of sets such that the diagram (3.3.1) is commuative. Then the map  $\varphi : G \rightarrow \text{Aut}_{\text{Sets}} S$  given by  $\varphi(g)(s) = a(g, s)$  is a group homomorphism. We leave the verification as an exercise.

**Definition 3.4.** If  $G$  is a group, we write  $G\text{-Sets}$  for the class of sets  $E$  equipped with  $G$ -actions  $\varphi : G \rightarrow \text{Aut}_{\text{Sets}} E$ . If  $E$  and  $F$  are two  $G$ -sets, we define

$$\text{Hom}_{G\text{-Sets}}(E, F) = \{f \in \text{Hom}_{\text{Sets}}(E, F) : \forall e \in E, f(ge) = gf(e)\}.$$

**Example 3.5.** Let  $\mathbb{R}$  denote the real numbers. For any non-negative integer  $n$ , we write  $\text{GL}_n(\mathbb{R})$  for the set of invertible linear transformations of  $\mathbb{R}^n$ . Clearly,  $\text{GL}_n(\mathbb{R}) \subset \text{Aut}_{\text{Sets}}(\mathbb{R}^n)$ . Moreover, if  $a, b \in \text{GL}_n(\mathbb{R})$ , then it is easy to see that  $a \circ b^{-1}$  is as well. Thus  $\text{GL}_n(\mathbb{R})$  is a subgroup of  $\text{Aut}_{\text{Sets}}(\mathbb{R}^n)$ . By definition, this defines an action of  $\text{GL}_n(\mathbb{R})$  on  $\mathbb{R}^n$ .

**Example 3.6.** Let  $\mathbb{R}\mathbb{P}^n$  denote the set of lines through the origin in  $\mathbb{R}^{n+1}$ . Then  $\text{GL}_{n+1}$  acts on  $\mathbb{R}\mathbb{P}^n$  because linear transformations preserves lines.

**Definition 3.7.** A map  $\varphi : G \rightarrow H$  between groups is an *anti-homomorphism* if  $\varphi(g_1 g_2) = \varphi(g_2) \varphi(g_1)$ . For example, if  $G$  is a group, the map  $\text{Inv} : G \rightarrow G$  given by  $g \mapsto g^{-1}$  is an anti-homomorphism.

The following proposition allows us to replace anti-homomorphisms with homomorphisms.

**Proposition 3.8.** *Suppose  $G, H$  and  $K$  are groups and  $a : G \rightarrow H$ ,  $b : H \rightarrow K$  are maps of sets.*

- (1) *If  $a$  and  $b$  are both either homomorphisms or anti-homomorphisms, then  $b \circ a$  is a homomorphism;*
- (2) *If  $a$  is an anti-homomorphism and  $b$  is a homomorphism or  $a$  is a homomorphism and  $b$  an anti-homomorphism, then  $b \circ a$  is an anti-homomorphism;*
- (3) *The map  $a \mapsto a \circ \text{Inv}$  sets up an isomorphism between  $\text{Hom}_{\text{Gps}}(G, H)$  and the set of anti-homomorphisms from  $G$  to  $H$  whose inverse is given by  $a \mapsto a \circ \text{Inv}$ .*
- (4) *Iff  $a \in \text{Hom}_{\text{Sets}}(G, H)$  is either a homomorphism or an anti-homomorphism, then  $\text{Inv} \circ a = a \circ \text{Inv}$ .*

*Proof.* Statements (1) and (2) are very easy to prove and I leave them to the reader. For (3), the important point is to note is that  $\text{Inv}^2 = \text{id}_G$ . Therefore,  $a \circ \text{Inv} \circ \text{Inv} = a$ . For (4), suppose that  $a$  is a homomorphism and  $g \in G$ . Then  $a(g^{-1}) = a(g)^{-1}$ . That is,  $a \circ \text{Inv} = \text{Inv} \circ a$ . Now suppose  $a$  is an anti-homomorphism. Then

$$\begin{aligned} a \circ \text{Inv} &= (a \circ \text{Inv}) \circ (\text{Inv} \circ \text{Inv}) \\ &= ((a \circ \text{Inv}) \circ \text{Inv}) \circ \text{Inv} \\ &= (\text{Inv} \circ (a \circ \text{Inv})) \circ \text{Inv} \\ &= (\text{Inv} \circ a \circ \text{Inv}) \circ \text{Inv} \\ &= \text{Inv} \circ a. \end{aligned}$$

□

**3.9.** A *right action* of a group  $G$  on a set  $S$  is an anti-homomorphism  $\varphi : G \rightarrow \text{Aut}_{\text{Sets}} S$ . Given a right action, the *associated action on  $S$*  is the action given by  $\varphi \circ \text{Inv} : G \rightarrow \text{Aut}_{\text{Sets}} S$ .

**3.10.** A right action defines a map  $a : S \times G \rightarrow S$  given by  $(s, g) \mapsto sg := \phi(g)s$ . This is called the associated right action map. Note that  $s(gh) = \varphi(gh)s = \varphi(h)\varphi(g)s = \varphi(h)(sg) = (sg)h$ . This explains the term “right” action. Moreover, giving a right action is equivalent to giving a map  $a : S \times G \rightarrow S$  such that  $a(s, gh) = a(a(s, g), h)$ .

**Remark 3.11.** We will often use the technique of 3.9 to turn right actions into left actions.

**Example 3.12.** Let  $G$  be a group. Then  $G$  acts on itself from both the left and the right. One way to package this information is to say that there is an action  $A : G \times G \rightarrow \text{Aut}_{\text{Sets}}(G)$  given by

$$A(g, h)(k) = gkh^{-1}.$$

From this, we deduce three important examples of actions of  $G$  on itself:

- (1) We set  $L(g) := A(g, 1)$ . So  $L(g)k = gk$ .
- (2) We have  $R(g) := A(1, g)$ . So  $R(g)k = kg^{-1}$ .
- (3) We set  $I(g) := A(g, g)$ . So  $I(g)k = gkg^{-1}$ . This is called the action of  $G$  on itself by *inner automorphisms*.

Note that  $I(G) \subset \text{Aut}_{\text{Gps}}(G) \subset \text{Aut}_{\text{Sets}}(G)$ : we have  $I(g)(ab) = g(ab)g^{-1} = gag^{-1}gbg^{-1} = I(g)(a)I(g)(b)$ .

**3.13.** Suppose  $H$  and  $K$  are subgroups of a group  $G$ . We say that  $H$  and  $K$  *commute with each other* if  $\forall h \in H, \forall k \in K \quad hk = kh$ .

**Proposition 3.14.** Let  $G$  be a group and  $\{H_i\}_{i \in I}$  a family of subgroups. If  $H_i$  commutes with  $H_j$  for any  $i \neq j \in I$ , then there is a homomorphism  $f : \bigoplus_{i \in I} H_i \rightarrow G$  such that  $\phi(H_i) = H_i$ . Conversely, if there is a homomorphism  $f : \bigoplus_{i \in I} H_i \rightarrow G$  with  $\phi(H_i) = H_i$ , then  $H_i$  commutes with  $H_j$  for  $i \neq j$ .

*Proof.* Suppose  $H_i$  commutes with  $H_j$  for  $i \neq j$ . Define a map  $f : \bigoplus_{i \in I} H_i \rightarrow G$  by  $(h_i)_{i \in I} \mapsto \prod_{i \in I} h_i$  here the product is taken over elements  $i$  such that  $h_i \neq 1$ ; therefore, it is a finite product. Note also that the order in which the product is taken does not matter as  $H_i$  commutes with  $H_j$ . Now,  $f$  is easily seen to be a homomorphism. Also  $f(H_i)$  is clearly equal to  $H_i$ . The converse is clear because the  $H_i \leq \bigoplus_{i \in I} H_i$  commute with each other.  $\square$

**3.15.** Suppose  $H$  and  $K$  are two groups acting on a set  $E$  (from the left). Let  $\varphi_H : H \rightarrow \text{Aut}_{\text{Sets}} E$  and  $\varphi_K : K \rightarrow \text{Aut}_{\text{Sets}} E$  denote the two actions. We say that the actions of  $H$  and  $K$  on  $E$  *commute* if the subgroups  $\varphi_H(H)$  and  $\varphi_K(K)$  of  $\text{Aut}_{\text{Sets}} E$  commute. Clearly, this is equivalent to saying that  $\forall e \in E, \forall h \in H, \forall k \in K \quad hke = khe$ . By 3.13, the actions of  $H$  and  $K$  on  $E$  iff they come by restriction from an action of  $H \times K$  on  $E$ . In particular, the actions  $L$  and  $R$  a group  $G$  on itself discussed in Example 3.12 commute.

#### 4. ORBITS AND QUOTIENTS

**4.1.** Let  $G$  be a group acting (on the left) on a set  $S$ . For each  $s \in S$ , we define the orbit of  $s$  under  $G$ , to be the set  $Gs = \{gs : g \in G\}$ . A subset  $T \subset S$  is a  $G$ -orbit if there exists  $s \in S$  such that  $T =Gs$ .

**Lemma 4.2.** *If a group  $G$  acts on a set  $S$ , then*

- (a) *Every element of  $S$  is in a  $G$ -orbit;*
- (b) *any two distinct  $G$ -orbits are disjoint.*

*Proof.* (a) is trivial as, for  $s \in S$ , we clearly have  $s \in Gs$ . (Since  $s = 1s$ .) To prove (b), suppose  $s_1, s_2 \in G$  and  $t \in Gs_1 \cap Gs_2$ . Then, we have elements  $g_1, g_2 \in G$ , such that  $t = g_1s_1 = g_2s_2$ . Then  $s_1 = g_1^{-1}g_2s_2$ . Hence, for  $g \in G$ , we have  $gs_1 = gg_1^{-1}g_2s_2 \in Gs_2$ . Thus  $Gs_1 \subset Gs_2$ . Switching the roles of  $s_1$  and  $s_2$ , we see that  $Gs_2 \subset Gs_1$ . Thus  $Gs_1 = Gs_2$ .  $\square$

**4.3.** If  $X$  is a set and  $(X_i)_{i \in I}$  is a family of non-empty subsets of  $X$ , then we say that  $X$  is the *disjoint union* of the  $X_i$  if  $X = \cup_{i \in I} X_i$  and  $X_i \cap X_j = \emptyset$  for  $i \neq j$ . By the Lemma,  $S$  is a disjoint union of its orbits under  $G$ . We write  $G \backslash S$  for the set of  $G$ -orbits when  $G$  acts on  $S$  from the left. If  $G$  acts on  $S$  on the right, then the right  $G$  orbit of  $s$  in  $G$  is the set  $sG = \{sg : g \in G\} \subset S$ . Clearly the lemma generalizes to right  $G$  orbits:  $S$  is the disjoint union of its right  $G$  orbits. (One cheap way to see this is to use the technique of 3.9 to convert the right action into a left action.) We write  $S/G$  for the set of right  $G$ -orbits of  $S$ .

**Example 4.4.** As in Example 3.5, let  $\mathbf{GL}_n(\mathbb{R})$  act on  $\mathbb{R}^n$  from the left. There are two orbits,  $\mathbf{GL}_n(\mathbb{R})0 = \{0\}$  and  $\mathbf{GL}_n(\mathbb{R})e = \mathbb{R}^n \setminus \{0\}$  where  $e \in \mathbb{R}^n$  is any non-zero vector.

**Example 4.5.** Let  $\mathbb{R}^*$  denote  $\mathbb{R} \setminus \{0\}$  viewed as a group under multiplication. The group  $\mathbb{R}^*$  acts on  $\mathbb{R}^{n+1} \setminus \{0\}$  by the action  $a : \mathbb{R}^* \times \mathbb{R}^{n+1} \setminus \{0\} \rightarrow \mathbb{R}^{n+1} \setminus \{0\}$  given by  $(\lambda, v) \mapsto \lambda v$ . The set  $\mathbb{R}^* \backslash (\mathbb{R}^{n+1} \setminus \{0\})$  is the set of lines through the origin (with the origin itself removed).

**Proposition 4.6.** *Suppose  $H$  and  $K$  are two groups acting on a set  $E$  (from the left). Suppose further that the actions commute. Let  $Ke$  be the  $K$  orbit (of an element  $e \in E$ ). Then, for any  $h \in H$ , multiplication by  $h$  maps  $Ke$  isomorphically onto the  $K$ -orbit  $Khe$ .*

*Proof.* This is obvious. If  $ke \in Ke$  then  $hke = khe \in Khe$ . This shows that multiplication by  $h$  maps  $Ke$  into  $Khe$ . The inverse map is clearly given by multiplication by  $h^{-1}$ .  $\square$

**Definition 4.7.** We say that a group  $G$  acts *transitively* on a  $G$  set  $E$  if  $G \backslash E$  is a singleton.

**4.8.** Let  $E$  be a  $G$ -set and  $e \in E$ . We say that the *stabilizer*  $\text{Stab}_G e$  of  $e$  in  $G$  is the set

$$\text{Stab}_G e = \{g \in G \mid ge = e\}.$$

Suppose  $g, h \in \text{Stab}_G e$ . Then  $gh^{-1}e = gh^{-1}he = ge = e$ . Therefore  $gh^{-1} \in \text{Stab}_G e$ . Thus  $\text{Stab}_G e \leq G$ .

**4.9.** Let  $H \leq G$  be a subgroup of a group  $G$ . Then  $H$ , since the left action of  $G$  on itself commutes with the right action of  $H$  on  $G$ , we see that  $G$  acts on the  $G/H$ . Explicitly, we have

$$g(g'H) = (gg')H.$$

Clearly  $G$  acts transitively on  $G/H$  because the orbit of  $H \in G/H$  is clearly  $G/H$ .

**Proposition 4.10.** *Let  $E$  be a  $G$ -set and  $e \in E$ . The map  $\phi : G/\text{Stab}_G e \rightarrow E$  given by  $g\text{Stab}_G e \mapsto ge$  is a well-defined homomorphism of  $G$ -sets.*

*Proof.* To check that it is well-defined, suppose  $g' = gh$  for  $h \in \text{Stab}_G e$ . Then  $g'e = ghe = ge$ . Therefore  $\phi(g') = \phi(g)$ . It is obvious that  $\phi$  is a homomorphism of  $G$ -sets.  $\square$

## 5. SYLOW THEOREMS

In this section we prove the Sylow theorems as an application of the study of group actions on sets. I use a version of the proof that from the book by Alperin-Bell.

**5.1.  $p$ -groups.** If  $p$  is a positive prime integer, then a  $p$ -group is a group  $P$  whose order is equal to  $p^r$  for some  $r \in \mathbb{Z}_{\geq 0}$ . The term  $p$ -group, when the prime  $p$  is unspecified, always refers to a group of *prime power order*.

**Lemma 5.2.** *Let  $G$  be a finite cyclic group. Then*

- (1) *the subgroups of  $G$  are all cyclic of order dividing  $|G|$ ;*
- (2) *for every non-negative divisor  $d$  of  $G$  there is exactly one subgroup  $H$  of  $G$  of order  $d$ .*

*Proof.* Let  $g$  be a generator of  $G$  and let  $\varphi : \mathbb{Z} \rightarrow G$  denote the map given by  $n \mapsto g^n$ . Then, by definition,  $\varphi$  is surjective. If  $H \leq G$  then,  $\varphi^{-1}H = r\mathbb{Z}$  for some  $r \in \mathbb{Z}_{\geq 0}$ . Since  $\varphi$  is surjective,  $H = \varphi(r\mathbb{Z})$  and, thus,  $H$  is cyclic. Moreover  $H \cong r\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(n/r)\mathbb{Z}$ . Thus  $H$  has order  $n/r$ . Thus  $r = n/|H|$ , and, therefore  $H$ , are determined by  $|H|$ .  $\square$

**5.3.** For  $n \in \mathbb{Z} \setminus \{0\}$  and  $p$  prime, let  $\ell_p(n)$  denote the largest power of  $p$  dividing  $n$ .

**Definition 5.4.** Let  $G$  be a finite group, and let  $p$  be a prime. A  $p$ -Sylow subgroup of  $G$  is a  $p$ -group of order  $\ell_p(|G|)$ . We write  $\text{Syl}_p(G)$  for the set of  $p$ -Sylow subgroups of  $G$ . Note that this is a  $G$ -set under the action of conjugation.

**Theorem 5.5 (Sylow).** *Let  $G$  be a finite group and let  $p$  be a prime.*

- (1) *The number of distinct  $p$ -Sylow subgroups of  $G$  is congruent to 1 modulo  $p$ . In particular,  $\text{Syl}_p(G)$  is non-empty.*
- (2) *All  $p$ -Sylow subgroups of  $G$  are conjugate. In other words,  $\text{Syl}_p(G)$  is a homogenous  $G$ -set.*

We are going to prove the theorem in several steps by studying the action of  $G$  on a  $G$ -set  $X$ . Before we define  $X$ , we set  $r = \log_p(\ell_p(|G|))$  and  $m := |G|/p^r$  so that  $|G| = p^r m$  with  $(p, m) = 1$ .

**5.6.** Let  $X$  denote the set of all subsets of  $G$  such that  $|S| = p^r$ . We regard  $X$  as a  $G$ -set with  $G$  acting by multiplication from the left. Note that

$$|X| = \binom{|G|}{\ell_p(|G|)} = \binom{p^r m}{p^r}.$$

Clearly, this number depends only on  $|G|$  and not on the group structure of  $G$ .

**5.7.** Let  $S \in X$ . Then  $S$  is the disjoint union of  $G_S$  orbits. Thus  $|G_S| \mid p^r$  with equality ( $|G_S| = p^r$ ) occurring iff  $S$  is a single  $G_S$  orbit, i.e, a left coset of  $G_S$ . Thus, for any  $P \in \text{Syl}_p(G)$ , there are exactly  $m$  elements of  $X$  stabilized by  $P$ : the  $m$  left cosets of  $P$ .

**5.8.** We have

$$\binom{p^r m}{p^r} = |X| = \sum_{S \in G \setminus X} [G : G_S] \equiv m |\text{Syl}_p(G)| \pmod{p}.$$

*Proof of (5.8).* The first two lines are clear. For the last use (5.7) and the obvious fact that  $p \nmid [G : G_S]$  if  $G_S$  is not a  $p$ -Sylow.  $\square$

**5.9.** We have

$$\binom{p^r m}{p^r} \equiv 1 \pmod{p}.$$

To see this, set  $G = \mathbb{Z}/p^r m$ . Then there is exactly one  $p$ -Sylow. Therefore  $m |\text{Syl}_p(G)| = m$ .

*Proof of Theorem 5.5 (1).* We have  $m |\text{Syl}_p(G)| \equiv m \pmod{p}$ . Since  $(m, p) = 1$ , this implies  $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$ .

## 6. ELEMENTARY GROUP REPRESENTATION THEORY

**6.1.** Let  $G$  be a group. A *representation* (or sometimes *linear representation*) of  $G$  over a field  $F$  is a group homomorphism  $G \xrightarrow{\rho} \text{Aut}_F V$  where  $V \in \mathbf{Vect}_F$ . Since  $\text{Aut}_F V \subset \text{Aut}_{\text{Sets}} V$ , a group representation is, in particular, a  $G$ -set. As with  $G$ -sets, we often abuse notation and write  $V$  instead of  $\rho$  for the representation. We write  $a : G \times V \rightarrow V$  for the map given by  $(g, v) \mapsto gv := \rho(g)v$ . We sometimes call a representation of  $G$  over  $F$ , a  *$G$ -representation* or a  *$G$ -rep*.

**6.2.** We write  $\mathbf{Rep}_F G$  for the class of all  $G$ -reps. over  $F$ . If  $V, W \in \mathbf{Rep}_F G$ , then

$$\begin{aligned} \text{Hom}_{\mathbf{Rep}_F G}(V, W) &:= \{f \in \text{Hom}_{\mathbf{Vect}_F}(V, W) : \forall g \in G, \forall v \in V, gf(v) = f(gv)\} \\ &= \text{Hom}_{\mathbf{Vect}_F}(V, W) \cap \text{Hom}_{G\text{-Sets}}(V, W). \end{aligned}$$

(Brosnan) DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, VANCOUVER, B.C., CANADA V6T 1Z2

*E-mail address*, Brosnan: brosnan@math.ubc.ca