Notes on Abstract Algebra

Alex Nelson

December 22, 2008

Contents

List of Figures

Introduction

Remark 1. Just a prefatory note, to indicate an example has ended I will use either 'QEF' or ■ and for the end of a proof, I will use an empty square; to show that a sketch of a proof has ended I will use a spade ♠.

1 Groups

1.1 Monoids

Let S be some set. A mapping

$$S \times S \to S \tag{1}$$

is sometimes called a **law of composition** (of S into itself). If x, y are elements of S, the image of the pair (x, y) under this mapping is also called their **product** under the law of composition. It will be denoted as xy.

Example 1. In $\mathbb{R}^3$, our favorite vector space from calculus 21 C, an example of a noncommutative law of composition is the **cross product**

$$\vec{u} \times \vec{v} = \begin{vmatrix} \hat{x} & \hat{y} & \hat{z} \\ u_x & u_y & u_z \\ v_x & v_y & v_z \end{vmatrix} \tag{2a}$$

$$= (u_y v_z - u_z v_y)\hat{x} + (u_z v_x - u_x v_z)\hat{y} + (u_x v_y - u_y v_x)\hat{z} \tag{2b}$$

Observe that the dot product does not really satisfy the criteria for the composition, because the dot product "takes in" two vectors and it "spits out" a scalar. But for

a composition, it needs to "take in" two of the same object, and it "spits out" the same object. The cross product does this, it "takes in" two 3-vectors and it "spits out" a 3-vector. ■

Example 2. Consider multiplication of complex numbers

$$(t + iu)(x + iy) = (xt - yu) + i(ux + ty) \tag{3}$$

It takes in two complex numbers, and it returns a complex number. It is commutative. ■

Example 3. Consider an arbitrary vector space V over some field $\mathbb{F}$. Given any two vectors $\vec{u}$, $\vec{v} \in V$, we have the commutative composition operation of vector addition

$$(\vec{u} + \vec{v}) \in V \tag{4}$$

which means that we have a law of composition for vector spaces. ■

Example 4. Let W be a vector space over the field $\mathbb{F}$. Consider two linear operators:

$$T, U : W \to W \tag{5}$$

then we may compose the linear operators into a new linear operator

$$V = T \circ U \tag{6}$$

so when acting on some element $\vec{w} \in W$ we have

$$V(\vec{w}) = T\Big(U(\vec{w})\Big) \tag{7}$$

which is also a linear operator. ■

Similarly, for more general (not necessarily commutative, but possibly commutative) operations, we use the symbol '$\cdot$' and write $x \cdot y$ (or more generally just xy).

Now in general, if the composition is commutative (so $xy = yx$) then we usually use the symbol '$+$' to indicate this and generically call it "**addition**" . So when $x + y = y + x$ (i.e. when the operation is commutative) we use the generic term "addition" and the symbol '$+$' to indicate this.

But to be fully general, a generic law of composition is dubbed "multiplication", and if it is commutative we call it "addition". We use the corresponding terminology (e.g. "the sum of x and y is $x + y$", "given u and v, their product is uv").

Now let us consider a set S with a law of composition. If x, y, z are elements of S, we can write their product in two ways: $(xy)z$ and $x(yz)$. If $(xy)z = x(yz)$ for all $x, y, z \in S$, then we say that their law of composition is "**associative**" .

Screw with the parenthese, i.e. order of operating doesn't matter, operation is associative

An element e of S such that

$$ex = xe = x \tag{8}$$

for all $x \in S$ is called a **unit element** . (When the law of composition is written additively, the unit element is denoted by 0, and is **zero element** .) A unit element is unique, suppose that there is another unit element e' distinct from e, then

$$e = ee' = e' \tag{9}$$

by assumption. In most cases, the unit element is written simply as 1 (instead of e). It is a generalization of the notion of the identity element with respect to some given "Law of Composition". For most of this section, we'll use e for clarity when specifying the basic properties.

Now, a **monoid** is a set G with a law of composition which is associative, and having a unit element (which implies that G is never empty). Note that there is nothing about being finite or infinite, nor is there any specification about the law of composition possessing an inverse.

Monoid: a set of elements equipped with some law of composition, that is closed under said law of composition

Example 5. Consider the natural numbers with 0[1], that is $\mathbb{N} \cup \{0\}$. We have the law of composition defined by addition in the usual way (so $1 + 0 = 1$, $2 + 4 = 6$, etc.) and we have the additive identity 0. If we didn't have 0, we'd be a bit out of luck as there is no additive identity in $\mathbb{N}$. So all by itself, $\mathbb{N}$ is not a monoid, but the union $\mathbb{N} \cup \{0\}$ is a monoid as it has the additive identity. ■

Example 6. Let V be a vector space over the field $\mathbb{F}$. Let $\mathcal{L}(V)$ be the set of linear operators on ("endomorphisms of") V. Then $\mathcal{L}(V)$ is a monoid in two different ways: one is with the law of composition being matrix addition with the unit element being the zero matrix; the other is with the law of composition being matrix multiplication with the unit element being the identity matrix. ■

Let G be a monoid, and $x_1, \dots, x_n$ be elements of G (where $n > 1$ is some integer). We can define their product inductively:

Remember, we have the law of composition generically referred to as "multiplication"

$$\prod_{\nu=1}^{n} x_\nu = x_1 \cdots x_n = (x_1 \cdots x_{n-1}) x_n. \tag{10}$$

Now, don't jump to conclusions! It is very tempting to think of this as just the usual product series as we learned from analysis, but this is more general due to this just being a way to iterate the law of composition on a sequence of elements in G. Note that we did define it to be careful about the order of operating.

We can also observe that we have the following rule

Extended associativty for an arbitary number of elements

$$\prod_{\mu=1}^{m} x_\mu \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu \tag{11}$$

which essentially asserts *that we can insert parentheses in any manner in our product without changing its value.* This is actually relatively trivial since monoids have their law of composition be associative.

Sketch Of Proof. We can do this proof by induction on m. So for an arbitrary positive integer, we have **Base Case:** $m = 2$ Observe that

$$\prod_{\mu=1}^{m} x_\mu \cdot \prod_{\nu=1}^{n} x_{m+\nu} = (x_1 \cdot x_2) \cdot (x_3 \cdot (\cdots) \cdot x_{2+n}) \tag{12a}$$

$$= x_1 \cdot x_2 \cdot x_3 \cdot (\cdots) \cdot x_{2+n} \text{ (by Associativity)} \tag{12b}$$

$$= \prod_{\nu=1}^{2+n} x_\nu \tag{12c}$$

where we justify the last step by just grouping terms by associativity of the law of composition.

[1] The author, not being French, doesn't believe 0 is either natural or a number.

Inductive Hypthotesis: Assume this works for arbitrary m.
Inductive Case: For $m+1$ we have

$$\prod_{\mu=1}^{m+1} x_\mu \cdot \prod_{\nu=1}^{n} x_{\nu+m+1} = \left(\prod_{\mu=1}^{m} x_\mu\right) \cdot x_{m+1} \cdot \left(\prod_{\mu=1}^{n} x_{\mu+m+1}\right) \tag{13a}$$

$$= \left(\prod_{\mu=1}^{m} x_\mu\right) \cdot \left(\prod_{\mu=1}^{n} x_{\mu+m}\right) \tag{13b}$$

where we justify that last step by, again, the associativity of the law of composition, since we're using a monoid. Then we see that this is precisely the case for m which we assumed worked! So that concludes our proof by induction. ♠

Also note just a few standards we have with the product. For instance, we have

$$\prod_{m+1}^{m+n} x_\nu \text{ instead of } \prod_{\nu}^{n} x_{m+\nu} \tag{14}$$

and we *define*

$$\prod_{\nu=1}^{0} x_\nu = e. \tag{15}$$

It should be possible to define more general laws of composition, that is to say maps $S_1 \times S_2 \to S_3$ where S_1, S_2, S_3 are arbitrary sets. One can then express associativity and commutativity in any setting where they make sense to express them (it will make more sense that than sentence just written). For instance, to have commutativity we need the law of composition take the form of

$$f : S \times S \to T \tag{16}$$

where the two sets that are "eaten" by f are necessarily the same. **Commutativity** then means that $f(x,y) = f(y,x)$ (or omitting f, $xy = yx$).

For associativity, when would it make sense? There are 8 possible cases one can imagine

$$\begin{array}{lll} S \times S \to S & S \times T \to S & T \times S \to S \\ T \times T \to T & S \times T \to T & T \times S \to T \\ S \times S \to T & T \times T \to S & \end{array}$$

To have associativity, we need to have

$$f(f(a,b),c) = f(f(a,c),b) \text{ or } f(a,f(b,c)) = f(b,f(a,c)) \tag{17}$$

so that means that b, c are both elements of the same set. That automatically rules out two possibilities

$$S \times S \to T \quad \text{and} \quad T \times T \to S.$$

By symmetry, we can see that if $S \times S \to S$ is associative, then $T \times T \to T$ is also associative. Similarly, if $S \times T \to S$ is associative, then $T \times S \to T$ is also associative. Commuting the position of the arguments doesn't change anything either, so if $S \times T \to S$ is associative then $T \times S \to S$ is also associative. So the only cases that can be associative are

When associativity could make sense

$$\begin{array}{lll} S \times S \to S & S \times T \to S & T \times S \to S \\ T \times T \to T & S \times T \to T & T \times S \to T \end{array} \tag{18}$$

and all others cannot be associative.

Now, if the law of composition of G is commutative, we say that G is **commutative** (or more often **Abelian**).

Proposition 1. Let G be a commutative monoid, and x_1, ..., x_n be elements of G. Let ψ be a bijection of the set of integers $(1, \ldots, n)$ onto itself (in other words, it's a permutation of $(1, \ldots, n)$). Then

$$\prod_{\nu=1}^{n} x_{\psi(\nu)} = \prod_{\nu=1}^{n} x_\nu \tag{19}$$

Proof. First let us show by induction that we can reorder a product of a sequence of elements in arbitrary order. **Base Case:** $n = 2$ So

$$xy = yx \tag{20}$$

which is trivially true from the definition of a commutative monoid.

Inductive Hypothesis: Assume this works for arbitrary n.

Inductive Step: We can show that since the law of composition maps $G \times G \to G$ that

$$\prod_{\nu=1}^{n} x_{\psi(\nu)} = y \tag{21}$$

and by the inductive hypothesis we have

$$\prod_{\nu=1}^{n} x_\nu = y \tag{22}$$

thus

$$yx_{n+1} = x_{n+1}y \tag{23}$$

by commuting x_{n+1} through all of the elements in the product. Thus we cover arbitrary permutations of $(1, \ldots, n+1)$ onto itself. □

Let G be a commutative monoid, let I be a set, and let $f : I \to G$ be a mapping such that $f(i) = e$ for almost all $i \in I$. (Here and thereafter, **almost all** means *all but a finite number.*) Let I_0 be the subset of I consisting of those i such that $f(i) \neq e$. By

$$\prod_{i \in I} f(i) \tag{24}$$

we shall mean the product

$$\prod_{i \in I_0} f(i) \tag{25}$$

taken in any order.

(When G is written additively, then instead of a product sign, we write the sum $\sum$ instead of the product $\prod$.)

We can continue rattling off a grocery list of properties that the product has. But it would be a pain in the rear to do, and not all that educational. We will, out of laziness, write *note notation*

$$\prod f(i) \tag{26}$$

omitting the $i \in I$ bit, since we have just seen the order doesn't matter. Another matter of convention, we use the exponent to indicate the number of times the operation of a set is used on a given element. So

$$x^n = \prod_{i=1}^{n} x$$

This allows us to have $x^0 = e$ and $x^1 = x$. We are content with this convention, since it allows us to use familiar notation making anything to the zeroeth power be the identity element.

Example 7. Consider the set of all invertibe matrices of a given vector space V on a field $\mathbb{F}$. This is typically denoted as $GL(V)$, and for an arbitrary element $X \in GL(V)$ we have

$$X^0 = I \tag{27}$$

where I is the identity matrix. ■

Let S, and S' be two subsets of a monoid G, then we define SS' to be the subset consisting of all elements xy with $x \in S$ and $y \in S'$. Inductively, we can define the product of a finite number of subsets, and we have associativity. Why? How can we see this assertion? Well, consider three subsets S, S', S'' of G. Then we can write $(SS')S'' = S(S'S'')$. Observe that we can say $GG = G$ since G has a unit element. If $x \in G$, then we can define xS to be $\{x\}S$ where $\{x\}$ is the set with a single element x (this is sort of like a coset). Thus xS consists of all elements xy with $y \in S$.

Remember law of compositions map $G \times G \to G$

Example 8. Consider all the square matrices on the vector space $V = \mathbb{C}^2$ over the scalar field $\mathbb{C}$. Let

$$z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{28}$$

and let S be the set of all traceless operators acting on V. Then

$$zS = \{zy : y \in S\} = \left\{ \begin{bmatrix} 0 & \beta \\ -\alpha & 0 \end{bmatrix} : \alpha, \beta \in \mathbb{C} \right\} \tag{29}$$

is the, uh, "comonoid".■

We can specify a monoid which is a subset of a given monoid. We call it a **submonoid** of G. To be fully clear, a submonoid of G is a subset H of G containing the unit element e, and such that – if $x, y \in H$ then $xy \in H$ – or in other words, H is **closed** under the law of composition. Well, by the definition of a monoid, we see that H is also a monoid.

We can see a trivial example of a submonoid given a monoid is just the powers of an arbitrary element. What does this mean? Well, choose some element x. What can we do with this? Well, we have the law of composition, so we can multiply it to itself to get x^2. We can then multiply this by x again to get x^3. We can keep going and going for arbitrary $n \in \mathbb{N}$ have the set of x^n. But this alone is not a monoid. Why? There is no identity element, which isn't nice. So we copy the French, and have $n \in \{0\} \cup \mathbb{N}$, then $\{x^n : n \in \{0\} \cup \mathbb{N}\}$ is a monoid and its closed under the law of composition. We see that it is commutative and associative. So it's a really nice monoid!

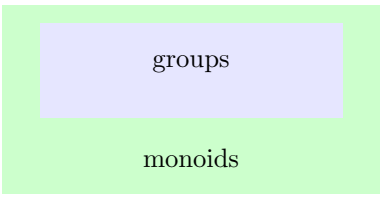

Figure 1: A Venn Diagram to illustrate the relation of the monoids and the groups. Observe all groups are monoids, but not all monoids are groups. Similarly, all trout are fish, but not all fish are trouts.

1.2 Groups

A **group** G is a monoid with some extra structure. Namely, for each element $x \in G$ there is an element $y \in G$ such that

$$xy = yx = e. \tag{30}$$

This element y is called an **inverse** for x. Such an inverse is unique, a simple proof to illustrate this: suppose that there are two inverses y, y' of x, then

$$y' = y'e = y'(xy) = (y'x)y = ey = y. \tag{31}$$

For multiplication, we denote the inverse of x by x^{-1}, and for addition the inverse of x is denoted by $-x$. The **order** of a group is the number of elements in the group, the size of the set so to speak.

It is probably worth going on without saying that e is its own inverse. But if we have (an identity e) an element x and its inverse x^{-1} and a given law of composition, then we can create a group consisting of the elements

$$G = \{(x^{-1})^n : n \in \mathbb{N}\} \cup \{(x)^n : n \in \mathbb{N}\} \cup \{e\} \tag{32}$$

which is trivial.

Example 9. Consider the matrix

$$z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{33}$$

observe that $z^2 = I$. That tells us that $\{I, z\}$ is a matrix group under matrix multiplication. ■

Notice we are being a bit ambiguous here in specifying "inverses" and "unit elements". E.g. with matrices, it makes a difference if we multiply by the right or by the left (e.g. X multiplied on the right by Y is XY but multiplied on the left is YX, and in general $XY - YX \neq 0$ – if it is zero, then X, Y are diagonal matrices). But we have been sufficiently general so left inverses and left identity elements are also inverses and identity elements. We can be precise in specification and prove it too:

Proposition 2. Let G be a set with an associative law of composition, let e be a left unit for that law, and assume that every element has a left inverse. Then e is a unit and each left inverse is also an inverse. In particular, G is a group.

Proof. Let $b \in G$ and let $a \in G$ be such that $ba = e$. Then

$$bab = eb = b. \tag{34}$$

This much should be trivial, it's just substitution. We can see that

$$abab = a(ba)b = aeb = ab \tag{35}$$

which is equivalent to

$$(ab)^2 = ab. \tag{36}$$

We can multiply both sides by $(ab)^{-1}$ on the left to see that

$$(ab) = e \tag{37}$$

which implies that a is the left inverse for b, or equivalently that b is the right inverse for a. We then see that

$$aba = a(e) = (e)a \tag{38}$$

which implies the left identity e is a "bi"-identity (i.e. both a left and right identity). □

Example 10. Let G be a group, and S be some nonempty set. The set of maps from S to G, denoted $M(S, G)$, is itself a group. That is, for two maps $f, g : S \to G$, we define fg to be the map such that

$$(fg)(x) = f(x)g(x) \tag{39}$$

The inverse f^{-1} multiplied by f is equal to the identity element in the group $\mathbb{1}$. That means, $f^{-1}(x) = f(x)^{-1}$. If $f(x)^{-1}$ is well defined, meaning that $f(x)$ – an element of the group G – has an inverse, which is necessarily true because that's the definition of a group, then each element of $M(S, G)$ has an inverse under the law of composition defined by Eq (39). We also have for arbitrary $f \in M(S, G)$ the product of it well defined too since $f(x)$ is an element in the group, so $f(x)^n$ is an element in the group raised to the n^{th} power – which is well defined because it's a monoid! So it is a group.■

Example 11. Let S be a non-empty set. Let G be the set of bijections from S to S. Then we see that, making the composition of mappings the law of composition, G is a group. (Remember a bijection is invertible, so each map has an inverse and we have the identity defined in the obvious way as the identity map of S.) The elements of G are called **permutations** of S. We denote G by $\mathrm{Perm}(S)$. ■

Example 12. Consider the group $\mathbb{Z}_2$, which consists of two elements 0 and 1. One can imagine this as a "bit" or a binary digit. It has the operation of addition

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1 \tag{40}$$

which is commutative. It is a cyclic group. We can further generalize this to $\mathbb{Z}_3$ with 3 elements: 0, 1, and 2. It has the laws of addition

$$0{+}0 = 1{+}2 = 2{+}1 = 0, \quad 0{+}1 = 1{+}0 = 2{+}2 = 1, \quad 0{+}2 = 2{+}0 = 1{+}1 = 2 \tag{41}$$

which is also commutative. We have inverses well defined, etc. etc. etc. We can generalize this to $\mathbb{Z}_n$ where $n \in \mathbb{N}$. This is a family of finite groups. ■

Remark 2. Typically we "represent" a number p in a cyclic group $\mathbb{Z}_n$ (where $0 \leq p < n$ is some integer) by $\exp[i2\pi(p/n)]$. In this "representation", we have instead of addition simple multiplication. Note that the "generator" of the group (the only element we really need that we can subject to the law of composition of the group to) is the primitive n^{th} root of unity $\exp[i2\pi/n]$. So p"="$(\exp[i2\pi/n])^p$.

Example 13. Let G_1, G_2 be groups. Let $G_1 \times G_2$ be the **direct product** which is similar to the direct product of sets, so $G_1 \times G_2$ is the set of all pairs (x_1, x_2) with $x_1 \in G_1$ and $x_2 \in G_2$. We define the product componentwise by

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2). \tag{42}$$

We see that $G_1 \times G_2$ is a group, with unit element (e_1, e_2) (where e_1 is the unit of G_1, and e_2 is the unit of G_2). We can do this for n groups, with componentwise multiplication. ■

Let G be a group. A **subgroup** H of G is a subset of G containing theunit element, and such that H is closed under the law of composition and inverse (or equivalently, it is a submonoid such that if $x \in H$ then $x^{-1} \in H$). A subgroup is **trivial** if it consists of the unit element alone. And trivially, the intersection of an arbitrary non-empty family of subgroups is a subgroup.

Let G be a group and $S \subset G$ be a subset. We say that S **generates** G or that S is a set of **generators** for G if every element of G can be expressed as a product of elements of S or inverses of elements of S, i.e. as a product $x_1 \cdots x_n$ where each x_i or x_i^{-1} is in S. It is clear that the set of al such products is a subgroup of G (remember, $x^0 = e$) and is the smallest subgroup of G containing S. What the hell does this mean? Well, S generates G if and only if the smallest subgroup of G containing S is G itself.

Let's stop and reiterate what we have just introduced. We have a subgroup S of a group G is a submonoid that is a group. So the submonoid contains inverses for each element. We have some finite subset S' of a group G which is such that any element of G can be written as a product of any finite number of elements of S'. This is a bit vague, so perhaps an example is needed.

Example 14. Consider the quaternions, which have elements

$$i^2 = j^2 = k^2 = ijk = -1 \tag{43}$$

We see that

$$\begin{aligned} i(ijk) &= i(-1) \\ \Rightarrow jk &= i \\ \Rightarrow (jk)k &= ik \\ \Rightarrow -j &= ik \\ \Rightarrow ij &= k \end{aligned}$$

So from i and j, we can get $1 = (-1)^2 = (i)^4 = (j)^4$ as well as $k = ij$. All we need are two elements to have the rest of the quaternions. ■

Note typically, if G is a group, and S is a set of generators, then we write $G = \langle S \rangle$. By definition, a cyclic group is a group which has one generator. *cyclic group has one generator*

Example 15. There are two non-abelian groups of order 8. One is the quaternions which we already say, the other is the **symmetries of the square**, generated by two elements σ, τ such that

$$\sigma^4 = \tau^2 = e, \quad \text{and } \tau\sigma\tau^{-1} = \sigma^3 \tag{44}$$

We see that

$$\begin{aligned}(\tau\sigma\tau^{-1})\tau &= \sigma^3\tau \\ &= \tau\sigma\end{aligned}$$

but also that

$$\sigma^{-1} = \sigma^3 \Rightarrow \sigma^{-1}\sigma = e = \sigma^4 \tag{45}$$

and

$$\tau^{-1} = \tau \Rightarrow \tau\sigma\tau = \sigma^3. \tag{46}$$

So that means that

$$\tau\sigma\tau = \sigma^{-1} \tag{47}$$

and

$$\tau\sigma^{-1}\tau = \sigma. \tag{48}$$

But doesn't this imply

$$\tau = \sigma\tau\sigma \tag{49}$$

by multiplying by the right by $\tau\sigma$. So we can write the inverses in terms of σ and τ alone. ■

Example 16. The quaternion group is more generally the group generated by two elements i, j and setting $ij = k$ and $m = i^2$, we have

$$i^4 = j^4 = k^4 = e, \quad \text{and } i^2 = j^2 = k^2 = m,\ ij = mji \tag{50}$$

but observe that as we introduced it before, it works perfectly fine setting $m = -1$ and $e = 1$. ■

Let G, G' be monoids. A **monoid-homomorphism** (or simply **homomorphism**) of G into G' is a mapping $f : G \to G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$ and mapping the unit element of G into that of G'. If additionally G, G' are groups, the mapping is given a special name called a **group-homomorphism**.

Example 17. Consider the monoid $\mathbb{N}$, a map

$$f : \mathbb{N} \to \mathbb{Z}_2 \tag{51}$$

is a homomorphism defined such that

$$f(n) = \begin{cases} 0 & n \text{ is even} \\ 1 & \text{otherwise} \end{cases} \tag{52}$$

Then f is a homomorphism. It maps the 0 element to the 0 element, and it maps

$$f(m + n) = f(m) + f(n)$$

trivially (odd+odd=even, even+even=even, even+odd=odd, and 1+1=0, 0+0=0, 0+1=1 respectively). ■

Example 18. Let V, W be arbitrary vector spaces. Let

$$f : V \to W \tag{53}$$

be a linear transformation. Trivially it is a homomorphism, as

$$f(u+v) = f(u) + f(v) \tag{54}$$

and by the definition of a linear transformation, we have

$$f(0) = 0. \tag{55}$$

Why? Well, it's trivial, observe

$$f(0+0) = f(0) + f(0) = f(0) \Rightarrow f(0) = 0. \tag{56}$$

So it preserves vector addition, and it maps the identity of vector addition to the identity of vector addition. ■

Observe that for a group homomorphism $f : G \to G'$, we have

$$\begin{aligned} f(xx^{-1}) &= f(e) \text{ since } xx^{-1} = e \\ &= f(x)f(x^{-}1) \text{ since } f \text{ is a homomorphism} \\ &= e' \text{ since } f \text{ is a homomorphism} \\ \Rightarrow (f(x))^{-1} f(e) &= f(x^{-1}) \\ &= f(x)^{-1}. \end{aligned}$$

It's trivial.

Example 19. Let G be a commutative group. Then for $x \in G$,

$$x \mapsto x^n \tag{57}$$

for some fixed integer n, is a homomorphism called the **n-th power map** . ■

Example 20. Let G_i be some collection of groups, and $i \in I$ be an element of some indexing set. Let

$$G = \prod G_i \tag{58}$$

be direct product of all G_i, for all $i \in I$. So an element of G would be a tuple consisting of components from each of the G_i. Let

$$p_i : G \to G_i \tag{59}$$

be the projection of the i^{th} factor. It selects the component of the tuples in G which corresponds to the contribution from the group G_i. Then p_i is a homomorphism. ■

Theorem 1. Let G, G' be groups, and S be a set of generators of G. Let

$$f : S \to G' \tag{60}$$

be a map. If there exists a homomorphism $\widetilde{f} : G \to G'$ such that when we restrict G to be S, $\widetilde{f} = f$, then there exists only one $\widetilde{f}$.

In other words, f has at most one extension to a homomorphism of G into G'.

Let $f : G \to G'$ and $g : G' \to G''$ be two group-homomorphisms. Then the composition $g \circ f$ is also a group homomorphism. If f, g are isomorphisms then so is $g \circ f$. Further, $f^{-1} : G' \to G$ is also an isomorphism. In particular, the set of all automorphisms of G is itself a group, denoted as $\mathrm{Aut}(G)$.

Definition 2. Let $f : G \to G'$ be a group homomorphism. Let e, e' be the respective unit elements of G, G'. We can then define the **kernel** of f to be the subset of G consisting of all elements x such that $f(x) = e'$.

We immediately see that the kernel forms a subgroup of G, since for any two $x, y \in \mathrm{Ker}(f)$, we have

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ &= e' + e' \\ &= e'. \end{aligned}$$

Furthermore, since f is a homomorphism, we have $f(e) = e'$ and

$$f(e) = f(xx^{-1}) = f(x)f(x)^{-1} = e'f(x^{-1}) = e' \tag{61}$$

which implies $f(x^{-1}) = e'$. So x^{-1} is in $\mathrm{Ker}(f)$.

Proposition 3. Let $f : G \to G'$ be a group homomorphism. Let H' be the **image** of f. Then H' is a subgroup of G'.

Proof. Observe that for $x, y \in G$, that

$$f(xy) = f(x)f(y) \in H'. \tag{62}$$

Further, since $f(e) = e' \in H'$ (so H' has an identity element), we see

$$f(xx^{-1}) = f(x)f(x^{-1}) = e' \Rightarrow f(x^{-1}) \in H'. \tag{63}$$

So the inverse of an arbitrary element is in H', as is the identity element, which is sufficient for H' to be a subgroup. □

Remark 3. The kernel and image of f are denoted by $\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$ respectively.

2 Examples of Character Tables

NOTE! We will be working with irreps over a finite dimensional vector space V over the field $\mathbb{C}$ of complex numbers.

2.1 The Character Table for D_3

Consider the group D_3 the symmetries of a regular triangle. It has 6 elements, and the presentation

$$\langle x, y | x^3 = y^2 = 1, yx = x^{-1}y \rangle. \tag{64}$$

It has, as mentioned, 6 elements

$$D_3 = \{1, x, x^2, y, yx, yx^2\}. \tag{65}$$

It has the multiplication table

$\times$	1	x	x^2	y	yx	yx^2
1	1	x	x^2	y	yx	yx^2
x^2	x^2	1	x	yx	yx^2	y
x	x	x^2	1	yx^2	y	yx
y	y	yx	yx^2	1	x	x^2
yx	yx	yx^2	y	x^2	1	x
yx^2	yx^2	y	yx	x	x^2	1

(66)

We find the cosets of the group

$$C(x) = \{x^k x x^{-k} = x, yxy = x^{-1}, yx^k xyx^k = x^{-1}\} \tag{67a}$$
$$= \{x, x^2\} \tag{67b}$$
$$C(y) = \{x^k y x^{-k} = yx^{-2k}, yyy = y, yx^k yyx^k = x^{-k}yx^k = yx^{2k}\} \tag{67c}$$
$$= \{y, yx, yx^2\} \tag{67d}$$

Observe that $(x^2)^2 = x^4 = x$ in our group. Refer to the multiplication table if in doubt. We can set up the character table. We expect there to be some number of irreducible representations k such that the sum of the squares of the dimensions of the irrep ρ_k is the size of the group. That is to say,

$$d_1^2 + d_2^2 + \cdots + d_k^2 = 6 \tag{68}$$

How many ways are there to do this? Well, observe $1^2 = 1 < 6$, so d_i can be at least 1. Further, $2^2 = 4 < 6$, so 2 is a possible dimension. But $3^2 = 9 > 6$, so we can only have 1 or 2 dimensional irreps. How many different combinations are there to write this? Trivially, two different ways

$$1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 = 6, \quad \text{or } 1^2 + 1^2 + 2^2 = 6. \tag{69}$$

Those are the only two ways to write it! Further, we expect the character table to be a square matrix, we have three cosets: $C(1)$ (or as I denote it $C(e)$), $C(x)$, and $C(y)$. That means we expect there to be three terms in our sum of squares, and the only formula with three terms is

$$1^2 + 1^2 + 2^2 = 1 + 1 + 4 = 6. \tag{70}$$

So we have a good idea of how many irreps there are for D_3. Let us now construct the character table:

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1			
χ_2			
χ_3			

(71)

Observe that we have the number of elements, which is *not standard* in character tables. I just like to add them in as a reminder for quick reference. Now the first column is the character of the irrep ρ_i. The first irrep ρ_1 is always the trivial representation, it maps everything to the identity in 1 dimension.

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1	1	1	1
χ_2			
χ_3			

(72)

Now we should remember that the character of the identity is always the number of dimensions of the irrep. So we can fill in the second column.

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1	1	1	1
χ_2	1		
χ_3	2		

(73)

We also have orthogonality of the rows (in a weighted inner product), and orthonormality of the columns. So we can **guess** the second row will be something of the form

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1	1	1	1
χ_2	1	a	b
χ_3	2		

(74)

where $a, b \in \mathbb{C}$ are to be determined. We know that the inner product between two characters is

$$\langle \chi_i, \chi_j \rangle = \frac{1}{n} \sum_g \overline{\chi_j(g)} \chi_i(g) = \delta_{ij} \tag{75}$$

where g is a coset representative and δ_{ij} is the Kronecker delta, χ_i is the character for the irrep ρ_i. So we have

$$\langle \chi_1, \chi_2 \rangle = 1(1 \cdot 1) + 2(1 \cdot \bar{a}) + 3(1 \cdot \bar{b}) = 0 \tag{76a}$$

$$\langle \chi_2, \chi_1 \rangle = 1(1) + 2(a) + 3(b) = 0 \tag{76b}$$

$$\langle \chi_2, \chi_2 \rangle = 1(1 \cdot 1) + 2(a \cdot \bar{a}) + 3(b \cdot \bar{b}) = 6. \tag{76c}$$

So from the first two of these equations, we find a, b are real. We know that characters of irreps of finite groups are integer combinations of roots of unity, so that means that $a, b \in \mathbb{Z}$. From the condition that

$$1 + 2a + 3b = 0 \tag{77}$$

we find that

$$a = 1, \quad b = -1. \tag{78}$$

So, we plug these into our character table

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2		

(79)

The orthonormality of the columns then demand that the rest of the character table is trivially

size of coset	(1)	(2)	(3)
coset rep	1	x	y
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

(80)

How do we see this? Take the first two columns and take their inner product

$$1 \cdot 1 + 1 \cdot 1 + 2 \cdot (-1) = 0 \tag{81}$$

and similarly for the first and third column

$$1 \cdot 1 - 1 \cdot 1 + 0 \cdot 2 = 1 - 1 = 0. \tag{82}$$

The second and third column are trivially orthogonal.

This is then the full character table for D_3.

References

[1] S. Lang, "Algebra. Revised," *Graduate Texts in Mathematics* **211** (2002) .