2. Groups I

---

1. *Groups*

The simplest, but not most immediately intuitive, object in abstract algebra is a *group*. Once introduced, one can see this structure nearly everywhere in mathematics. [1]

By definition, a **group** G is a set with an **operation** $g*h$ (formally, a function $G \times G \longrightarrow G$), with a special element e called **the identity**, and with properties:
• *The property of the identity*: for all $g \in G$, $e * g = g * e = g$.
• *Existence of* **inverses**: for all $g \in G$ there is $h \in G$ (the **inverse** of g) such that $h * g = g * h = e$.
• *Associativity*: for all $x, y, z \in G$, $x * (y * z) = (x * y) * z$.

If the operation $g * h$ is **commutative**, that is, if

$$g * h = h * g$$

then the group is said to be **abelian**. [2] In that case, often, but not necessarily, the operation is written as *addition*. And when the operation is written as addition, the identity is often written as 0 instead of e.

[1] Further, the notion of group proves to be more than a mere *descriptive* apparatus. It provides unification and synthesis for arguments and concepts which otherwise would need individual development. Even more, abstract structure theorems for groups provide *predictive* indications, in the sense that we know something in advance about groups we've not yet seen.

[2] After N.H. Abel, who in his investigation of the solvability by radicals of algebraic equations came to recognize

In many cases the group operation is written as multiplication or simply as juxtaposition

$$g * h = g \cdot h = gh$$

This does not *preclude* the operation being abelian, but only denies the *presumption* that the operation is abelian. If the group operation is written as multiplication, then often the identity is denoted as 1 rather than e. Unless written additively, the **inverse** [3] of an element g in the group is denoted

$$\text{inverse of } g = g^{-1}$$

If the group operation is written as *addition*, then the inverse is denoted

$$\text{inverse of } g = -g$$

Many standard mathematical items with natural operations are groups: The set $\mathbb{Z}$ of integers $\mathbb{Z}$ with addition $+$ is an abelian group. The set $n\mathbb{Z}$ of multiples of an integer n, with addition, is an abelian group. The set $\mathbb{Z}/m$ of integers mod m, with addition mod m as the operation is an abelian group. The set $\mathbb{Z}/m^\times$ of integers mod m *relatively prime to* m, with multiplication mod m as the operation is an abelian group.

The set $\mathbb{Z}$ of integers with operation being *multiplication* is *not* a group, because there are no inverses. [4] The closest we can come is the set $\{1, -1\}$ with multiplication.

Other things which we'll define formally only a bit later are groups: vector spaces with vector addition are abelian groups. The set $GL(2, \mathbb{R})$ of invertible 2-by-2 real matrices, with group law matrix multiplication, is a non-abelian group. Here the identity is the matrix

$$1_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The existence of inverses is part of the definition. The *associativity* of matrix multiplication is not entirely obvious from the definition, but can either be checked by hand or inferred from the fact that composition of functions is associative.

A more abstract example of a group is the set S_n of **permutations** of a set with n elements (n an integer), where *permutation* means *bijection to itself*. Here the operation is *composition* (as functions) of permutations. If there are more than two things in the set, S_n is non-abelian.

Some nearly trivial uniqueness issues should be checked: [5]
- *(Uniqueness of identity)* If $f \in G$ and $f * g = g * f = g$ for all g in G, then $f = e$.
- *(Uniqueness of inverses)* For given $g \in G$, if $a * g = e$ and $g * b = e$, then $a = b$.

Proof: For the first assertion,

$$\begin{array}{rcll} f & = & f * e & (\text{property of } e) \\ & = & e & (\text{assumed property of } e) \end{array}$$

---

the significance of commutativity many decades before the notion of *group* was formalized.

[3] once we prove its uniqueness!

[4] The fact that there are multiplicative inverses in the larger set $\mathbb{Q}^\times$ of non-zero rational numbers is beside the point, since these inverses are not inside the given set $\mathbb{Z}$.

[5] These are the sort of properties which, if they were *not* provable from the definition of group, would probably need to be added to the definition. We are fortunate that the innocent-looking definition does in fact yield these results.

which was claimed. For the second, similarly,

$$a = a * e = a * (g * b) = (a * g) * b = e * b = b$$

where we use, successively, the property of the identity, the defining property of b, associativity, the defining property of a, and then the property of the identity again. ///

[1.0.1] **Remark:** These uniqueness properties justify speaking of *the* inverse and *the* identity.

---

2. *Subgroups, Lagrange's theorem*

Subgroups are subsets of groups which are groups *in their own right*, in the following sense. A subset H of a group G is said to be a **subgroup** if, with the same operation and identity element as that used in G, it is a group.

That is, if H contains the identity element $e \in G$, if H contains inverses of all elements in it, and if H contains products of any two elements in it, then H is a subgroup.

Common terminology is that H is **closed under inverses** if for $h \in H$ the inverse h^{-1} is in H, and **closed under the group operation** if $h_1, h_2 \in H$ implies $h_1 * h_2$ is in H. [6]

Note that the associativity of the operation is assured since the operation was *assumed* associative for G itself to be a group.

The subset $\{e\}$ of a group G is always a subgroup, termed **trivial**. A subgroup of G other than the trivial subgroup and the group G itself is **proper**.

[2.0.1] **Proposition:** The intersection $\bigcap_{H \in S} H$ of any collection of subgroups of a group G is again a subgroup of G.

Proof: Since the identity e of G lies in each H, it lies in their intersection. If h lies in H for every $H \in S$, then h^{-1} lies in H for every $H \in S$, so h^{-1} is in the intersection. Similarly, if h_1, h_2 are both in H for every $H \in S$, so is their product, and then the product is in the intersection. ///

Given a set X of elements in a group G, the **subgroup generated by** [7] X is defined to be

$$\text{subgroup generated by } X \ = \langle X \rangle = \bigcap_{H \supset X} H$$

where H runs over *subgroups* of G containing X. The previous proposition ensures that this really is a subgroup. If $X = \{x_1, \ldots, x_n\}$ we may, by abuse of notation, write also

$$\langle X \rangle = \langle x_1, \ldots, x_n \rangle$$

and refer to the subgroup generated by $x_1, \ldots, x_n$ rather than by the subset X.

A **finite group** is a group which (as a set) is finite. The **order** of a finite group is the number of elements in it. Sometimes the order of a group G is written as $|G|$ or $o(G)$. The first real theorem in group theory is

[6] In reality, the very notion of *operation* includes the assertion that the output is again in the set. Nevertheless, the property is important enough that extra emphasis is worthwhile.

[7] Later we will see a constructive version of this notion. Interestingly, or, perhaps, disappointingly, the more constructive version is surprisingly complicated. Thus, the present quite non-constructive definition is useful, possibly essential.

[2.0.2] Theorem: *(Lagrange)* [8] Let G be a *finite* group. Let H be a subgroup of G. Then the order of H *divides* the order of G.

Proof: For $g \in G$, the **left coset** of H by g or **left translate** of H by g is

$$gH = \{gh : h \in H\}$$

(Similarly, the **right coset** of H by g or **right translate** of H by g is $Hg = \{hg : h \in H\}$.)

First, we will prove that the collection of all left cosets of H is a *partition* of G. Certainly $x = x \cdot e \in xH$, so every element of G lies in a left coset of H. Now suppose that $xH \cap yH \neq \phi$ for $x, y \in G$. Then for some $h_1, h_2 \in H$ we have $xh_1 = yh_2$. Multiply both sides of this equality on the right by h_2^{-1} to obtain

$$(xh_1)h_2^{-1} = (yh_2)h_2^{-1} = y$$

Let $z = h_1 h_2^{-1}$ for brevity. Since H is a *subgroup*, $z \in H$. Then

$$yH = \{yh : h \in H\} = \{(xz)h : h \in H\} = \{x(zh) : h \in H\}$$

Thus, $yH \subset xH$. Since the relationship between x and y is symmetrical, also $xH \subset yH$, and $xH = yH$. Thus, the left cosets of H in G partition G.

Next, show that the cardinalities of the left cosets of H are identical, by demonstrating a *bijection* from H to xH for any $x \in G$. Define

$$f(g) = xg$$

This maps H to yH, and if $f(g) = f(g')$, then

$$xg = xg'$$

from which left multiplication by x^{-1} gives $g = g'$. For *surjectivity*, note that the function f was arranged so that

$$f(h) = xh$$

Thus, all left cosets of H have the same number of elements as H.

So G is the disjoint union of the left cosets of H. From this, $|H|$ divides $|G|$. ///

The **index** $[G : H]$ of a subgroup H in a group G is the number of disjoint (left or right) cosets of H in G. Thus, Lagrange's theorem says

$$|G| = [G : H] \cdot |H|$$

For a single element g of a group G, one can verify that

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

where $g^0 = e$, and

$$g^n = \begin{cases} \underbrace{g * g * \ldots * g}_{n} & (0 < n \in Z) \\ \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{|n|} & (0 > n \in Z) \end{cases}$$

[8] Since the notion of abstract group did not exist until about 1890, Lagrange, who worked in the late 18^{th} and early 19^{th} centuries, could not have proven the result as it is stated. However, his work in number theory repeatedly used results of this sort, as did Gauss's of about the same time. That is, Lagrange and Gauss recognized the principle without having a formal framework for it.

One might do the slightly tedious induction proof of the fact that, for all choices of sign of integers m, n,

$$g^{m+n} = g^m * g^n$$

$$(g^m)n = g^{mn}$$

That is, the so-called *Laws of Exponents* are provable properties. And, thus, $\langle g\rangle$ really is a subgroup. For various reasons, a (sub)group which can be generated by a single element is called a **cyclic subgroup**. Note that a cyclic group is necessarily abelian.

The smallest positive integer n (if it exists) such that

$$g^n = e$$

is the **order** or **exponent** of g, often denoted by $|g|$ or $o(g)$. If there is no such n, say that the order of g is *infinite*. [9]

[2.0.3] **Proposition:** Let g be a finite-order element of a group G, with order n. Then the order of g (as group *element*) is equal to the order of $\langle g\rangle$ (as subgroup). In particular,

$$\langle g\rangle = \{g^0, g^1, g^2, \ldots, g^{n-1}\}$$

and, for arbitrary integers i, j,

$$g^i = g^j \quad \text{if and only if} \quad i = j \bmod n$$

Proof: The last assertion implies the first two. On one hand, if $i = j \bmod n$, then write $i = j + \ell n$ and compute

$$g^i = g^{j+\ell n} = g^j \cdot (g^n)^\ell = g^j \cdot e^\ell = g^j \cdot e = g^j$$

On the other hand, suppose that $g^i = g^j$. Without loss of generality, $i \le j$, and $g^i = g^j$ implies $e = g^{j-i}$. Let

$$j - i = q \cdot n + r$$

where $0 \le r < n$. Then

$$e = g^{j-i} = g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r$$

Therefore, since n is the least such that $g^n = e$, necessarily $r = 0$. That is, $n|j - i$. ///

[2.0.4] **Corollary:** *(of Lagrange's theorem)* The order $|g|$ of an element g of a finite group G divides the order of G. [10]

Proof: We just proved that $|g| = |\langle g\rangle|$, which, by Lagrange's theorem, divides $|G|$. ///

Now we can recover Euler's theorem as an example of the latter corollary of Lagrange's theorem:

[2.0.5] **Corollary:** *(Euler's theorem, again)* Let n be a positive integer. For $x \in \mathbb{Z}$ relatively prime to n,

$$x^{\varphi(n)} = 1 \bmod n$$

[9] Yes, this use of the term *order* is in conflict with the use for subgroups, but we immediately prove their compatibility.

[10] One can also imitate the direct proof of Euler's theorem, and produce a proof of this corollary at least for finite abelian groups.

Proof: The set $\mathbb{Z}/n^\times$ of integers mod n relatively prime to n is a group with $\varphi(n)$ elements. By Lagrange, the order k of $g \in \mathbb{Z}/n^\times$ divides $\varphi(n)$. Therefore, $\varphi(n)/k$ is an integer, and

$$g^{\varphi(n)} = (g^k)^{\varphi(n)/k} = e^{\varphi(n)/k} = e$$

as desired. ///

The idea of Euler's theorem can be abstracted. For a group G, the smallest positive integer ℓ so that for every $g \in G$

$$g^\ell = e$$

is the **exponent** of the group G. It is not clear from the definition that there really is such a positive integer ℓ. Indeed, for *infinite* groups G there may not be. But for *finite* groups the mere finiteness allows us to characterize the exponent:

[2.0.6] **Corollary:** *(of Lagrange's theorem)* Let G be a finite group. Then the exponent of G divides the order $|G|$ of G.

Proof: From the definition, the exponent is the least common multiple of the orders of the elements of G. From Lagrange's theorem, each such order is a divisor of $|G|$. The least common multiple of any collection of divisors of a fixed number is certainly a divisor of that number. ///

---

3. *Homomorphisms, kernels, normal subgroups*

Group homomorphisms are the maps of interest among groups.

A *function* (or *map*)

$$f : G \longrightarrow H$$

from one group G to another H is a **(group) homomorphism** if the *group operation is preserved* in the sense that

$$f(g_1 g_2) = f(g_1)\ f(g_2)$$

for all $g_1, g_2 \in G$. Let e_G be the identity in G and e_H the identity in H. The **kernel** of a homomorphism f is

$$\text{kernel of } f\ = \ker f = \{g \in G : f(g) = e_H\}$$

The **image** of f is just like the image of any function:

$$\text{image of } f\ = \text{im} f = \{h \in H :\ \text{there is } g \in G \text{ so that } f(g) = h\}$$

[3.0.1] **Theorem:** Let $f : G \longrightarrow H$ be a group homomorphism. Let e_G be the identity in G and let e_H be the identity in H. Then
• Necessarily f carries the identity of G to the identity of H: $f(e_G) = e_H$.
• For $g \in G$, $f(g^{-1}) = f(g)^{-1}$.
• The *kernel* of f is a subgroup of G.
• The *image* of f is a subgroup of H.
• Given a subgroup K of H, the *pre-image*

$$f^{-1}(K) = \{g \in G : f(g) \in K\}$$

of K under f is a subgroup of G.
• A group homomorphism $f : G \longrightarrow H$ is *injective* if and only if the kernel is *trivial* (that is, is the trivial subgroup $\{e_G\}$).

Proof: The image $f(e_G)$ has the property

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

Left multiplying by $f(e_G)^{-1}$ (whatever this may be),

$$f(e_G)^{-1} \cdot f(e_G) = f(e_G)^{-1} \cdot (f(e_G) \cdot f(e_G))$$

Simplifying,

$$e_H = (f(e_G)^{-1} \cdot f(e_G)) \cdot f(e_G) = e_H \cdot f(e_G) = f(e_G)$$

so the identity in G is mapped to the identity in H.

To check that the image of an inverse is the inverse of an image, compute

$$f(g^{-1}) \cdot f(g) = f(g^{-1} \cdot g) = f(e_G) = e_H$$

using the fact just proven that the identity in G is mapped to the identity in H.

Now prove that the kernel is a subgroup of G. The identity lies in the kernel since, as we just saw, it is mapped to the identity. If g is in the kernel, then g^{-1} is also, since, as just showed, $f(g^{-1}) = f(g)^{-1}$. Finally, suppose both x, y are in the kernel of f. Then

$$f(xy) = f(x) \cdot f(y) = e_H \cdot e_H = e_H$$

Let X be a subgroup of G. Let

$$f(X) = \{f(x) : x \in X\}$$

To show that $f(X)$ is a subgroup of H, we must check for presence of the identity, closure under taking inverses, and closure under products. Again, $f(e_G) = e_H$ was just proven. Also, we showed that $f(g)^{-1}) = f(g^{-1})$, so the image of a subgroup is closed under inverses. And $f(xy) = f(x)f(y)$ by the defining property of a group homomorphism, so the image is closed under multiplication.

Let K be a subgroup of H. Let x, y be in the pre-image $f^{-1}(K)$. Then

$$f(xy) = f(x) \cdot f(y) \in K \cdot K = K$$

$$f(x^{-1}) = f(x)^{-1} \in K$$

And already $f(e_G) = e_H$, so the pre-image of a subgroup is a group.

Finally, we prove that a homomorphism $f : G \longrightarrow H$ is injective if and only if its kernel is trivial. First, if f is injective, then at most one element can be mapped to $e_H \in H$. Since we know that at least e_G is mapped to e_H by such a homomorphism, it must be that *only* e_G is mapped to e_H. Thus, the kernel is trivial. On the other hand, suppose that the kernel is trivial. We will suppose that $f(x) = f(y)$, and show that $x = y$. Left multiply $f(x) = f(y)$ by $f(x)^{-1}$ to obtain

$$e_H = f(x)^{-1} \cdot f(x) = f(x)^{-1} \cdot f(y)$$

By the homomorphism property,

$$e_H = f(x)^{-1} \cdot f(y) = f(x^{-1}y)$$

Thus, $x^{-1}y$ is in the kernel of f, so (by assumption) $x^{-1}y = e_G$. Left multiplying this equality by x and simplifying, we get $y = x$. ///

If a group homomorphism $f : G \longrightarrow H$ is *surjective*, then H is said to be a **homomorphic image** of G. If a group homomorphism $f : G \longrightarrow H$ has an inverse homomorphism, then f is said to be an **isomorphism**, and G and H are said to be **isomorphic**, written

$$G \approx H$$

For groups, if a group homomorphism is a *bijection*, then it has an inverse which is a group homomorphism, so is an isomorphism.

[3.0.2] **Remark:** Two groups that are *isomorphic* are considered to be 'the same', in the sense that any *intrinsic* group-theoretic assertion about one is also true of the other.

A subgroup N of a group G is **normal** [11] or **invariant** [12] if, for every $g \in G$,

$$gNg^{-1} = N$$

where the notation is

$$gNg^{-1} = \{gng^{-1} : n \in N\}$$

This is readily seen to be equivalent to the condition that

$$gN = Ng$$

for all $g \in G$. Evidently in an abelian group G *every* subgroup is normal. It is not hard to check that *intersections of normal subgroups are normal.*

[3.0.3] **Proposition:** The kernel of a homomorphism $f : G \longrightarrow H$ is a normal subgroup.

Proof: For $n \in \ker f$, using things from just above,

$$f(gng^{-1}) = f(g)\, f(n)\, f(g^{-1}) = f(g)\, e_H\, f(g)^{-1} = f(g)\, f(g)^{-1} = e_H$$

as desired. ///

A group with no *proper* normal subgroups is **simple**. Sometimes this usage is restricted to apply only to groups *not* of orders which are prime numbers, since (by Lagrange) such groups have no proper subgroups whatsoever, much less normal ones.

---

4. *Cyclic groups*

Finite groups generated by a single element are easy to understand. The collections of all *subgroups* and of all *generators* can be completely understood in terms of elementary arithmetic, in light of the first point below. Recall that the set of integers modulo n is

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \{cosetsofn\mathbb{Z}in\mathbb{Z}\} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\}$$

[4.0.1] **Proposition:** Let $G = \langle g \rangle$, of order n. Then G is isomorphic to $\mathbb{Z}/n$ with addition, by the map

$$f(g^i) = i + n\mathbb{Z} \in \mathbb{Z}/n$$

Proof: The main point is the well-definedness of the map. That is, that $g^i = g^j$ implies $i = j \bmod n$, for $i, j \in \mathbb{Z}$. Suppose, without loss of generality, that $i < j$. Then $g^{j-i} = e$. Let

$$j - i = q \cdot n + r$$

[11] This is one of too many uses of this term, but it is irretrievably standard.

[12] The term *invariant* surely comes closer to suggesting the intent, but is unfortunately archaic.

with $0 \le r < n$. Then

$$e = e \cdot e = g^{j-i-qn} = g^r$$

and by the minimality of n we have $r = 0$. Thus, $n|j-i$, proving well-definedness of the map. The surjectivity and injectivity are then easy. The assertion that f is a homomorphism is just the well-definedness of addition modulo n together with properties of exponents:

$$f(g^i) + f(g^j) = (i + n\mathbb{Z}) + (j + n\mathbb{Z}) = (i + j) + n\mathbb{Z} = f(g^{i+j}) = f(g^i \cdot g^j)$$

This demonstrates the isomorphism. ///

[4.0.2] **Corollary:** Up to isomorphism, there is only one finite cyclic group of a given order. ///

The following facts are immediate corollaries of the proposition and elementary properties of $\mathbb{Z}/n$.

• The *distinct* subgroups of G are exactly the subgroups $\langle g^d \rangle$ for all *divisors* d of N.
• For $d|N$ the order of the subgroup $\langle g^d \rangle$ is the order of g^d, which is N/d.
• The order of g^k with arbitrary integer $k \neq 0$ is $N/\gcd(k, N)$.
• For any integer n we have

$$\langle g^n \rangle = \langle g^{\gcd(n,N)} \rangle$$

• The distinct generators of G are the elements g^r where $1 \le r < N$ and $\gcd(r, N) = 1$. Thus, there are $\varphi(N)$ of them, where φ is Euler's phi function.
• The number of elements of order n in a finite cyclic group of order N is 0 unless $n|N$, in which case it is N/n.

[4.0.3] **Proposition:** A homomorphic image of a finite cyclic group is finite cyclic.

Proof: The image of a generator is a generator for the image. ///

Using the isomorphism of a cyclic group to some $\mathbb{Z}/n$, it is possible to reach definitive conclusions about the solvability of the equation $x^r = y$.

[4.0.4] **Theorem:** Let G be a cyclic group of order n with generator g. Fix an integer r, and define

$$f : G \longrightarrow G$$

by

$$f(x) = x^r$$

This map f is a group homomorphism of G to itself. If $\gcd(r, n) = 1$, then f is an *isomorphism*, and in that case every $y \in G$ has a unique r^{th} root. More generally,

$$\text{order of kernel of } f = \gcd(r, n)$$

$$\text{order of image of } f = n/\gcd(r, n)$$

If an element y has an r^{th} root, then it has exactly $\gcd(r, n)$ of them. There are exactly $n/\gcd(r, n)$ r^{th} powers in G.

Proof: Since G is abelian the map f is a homomorphism. Use the fact that G is isomorphic to $\mathbb{Z}/n$. Converting to the additive notation for $\mathbb{Z}/n$-with-addition, f is

$$f(x) = r \cdot x$$

If $\gcd(r,n) = 1$ then there is a multiplicative inverse r^{-1} to r mod n. Thus, the function

$$g(x) = r^{-1} \cdot x$$

gives an inverse function to f, so f is an isomorphism.

For arbitrary r, consider the equation

$$r \cdot x = y \bmod n$$

for given y. This condition is

$$n|(rx - y)$$

Let $d = \gcd(r,n)$. Then certainly it is *necessary* that $d|y$ or this is impossible. On the other hand, suppose that $d|y$. Write $y = dy'$ with integer y'. We want to solve

$$r \cdot x = dy' \bmod n$$

Dividing through by the common divisor d, this congruence is

$$\frac{r}{d} \cdot x = y' \bmod \frac{n}{d}$$

The removal of the common divisor makes r/d prime to n/d, so there is an inverse $(r/d)^{-1}$ to r/d mod n/d, and

$$x = (r/d)^{-1} \cdot y' \bmod (n/d)$$

That is, any integer x meeting this condition is a solution to the original congruence. Letting x_0 be one such solution, the integers

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + 2 \cdot \frac{n}{d},\ x_0 + 3 \cdot \frac{n}{d},\ \dots x_0 + (d-1) \cdot \frac{n}{d}$$

are also solutions, and are distinct mod n. That is, we have d distinct solutions mod n.

The kernel of f is the collection of x so that $rx = 0 \bmod n$. Taking out the common denominator $d = \gcd(r,n)$, this is $(r/d)x = 0 \bmod n/d$, or $(n/d)|(r/d)x$. Since r/d and n/d have no common factor, n/d divides x. Thus, mod n, there are d different solutions x. That is, the kernel of f has d elements. ///

---

5. *Quotient groups*

Let G be a group and H a subgroup. The **quotient set** G/H of G by H is the set of H-cosets

$$G/H = \{xH : x \in G\}$$

in G. In general, there is *no* natural group structure on this set. [13] But if H is *normal*, then we define a group operation $*$ on G/H by

$$xH * yH = (xy)H$$

Granting in advance that this works out, the **quotient map** $q : G \longrightarrow G/N$ defined by

$$q(g) = gN$$

will be a group homomorphism.

[13] The key word is *natural*: of course any set can have several group structures put on it, but, reasonably enough, we are interested in group structures on G/H that have some connection with the original group structure on G.

Of course, the same symbols can be written for non-normal H, *but will not give a well-defined operation.* That is, for well-definedness, one must verify that the operation does not depend upon the choice of coset representatives x, y in this formula. That is, one must show that if

$$xH = x'H \quad \text{and} \quad yH = y'H$$

then

$$(xy)H = (x'y')H$$

If H is *normal*, then $xH = Hx$ for all $x \in G$. Then, literally, as sets,

$$xH \cdot yH = x \cdot Hy \cdot H = x \cdot yH \cdot H = (xy)H \cdot H = (xy)H$$

That is, we can more directly define the group operation $*$ as

$$xH * yH = xH \cdot yH$$

[5.0.1] **Remark:** If H is *not* normal, take $x \in G$ such that $Hx \not\subset xH$. That is, there is $h \in H$ such that $hx \notin xH$. Then $hxH \neq H$, and, if the same definition were to work, supposedly

$$hH * xH = (hx)H \neq xH$$

But, on the other hand, since $hH = eH$,

$$hH * xH = eH * xH = (ex)H = xH$$

That is, if H is not normal, this apparent definition is in fact not well-defined.

[5.0.2] **Proposition:** *(Isomorphism Theorem)* Let $f : G \longrightarrow H$ be a *surjective* group homomorphism. Let $K = \ker f$. Then the map $\bar{f} : G/K \longrightarrow H$ by

$$\bar{f}(gK) = f(g)$$

is well-defined and is an isomorphism.

Proof: If $g'K = gK$, then $g' = gk$ with $k \in K$, and

$$f(g') = f(gk) = f(g)\, f(k) = f(g)\, e = f(g)$$

so the map $\bar{f}$ is well-defined. It is surjective because f is. For injectivity, if $\bar{f}(gK) = \bar{f}(g'K)$, then $f(g) = f(g')$, and

$$e_H = f(g)^{-1} \cdot f(g') = f(g^{-1}) \cdot f(g) = f(g^{-1}g')$$

Thus, $g^{-1}g' \in K$, so $g' \in gK$, and $g'K = gK$. ///

In summary, the normal subgroups of a group are exactly the kernels of surjective homomorphisms.

As an instance of a counting principle, we have

[5.0.3] **Corollary:** Let $f : G \longrightarrow H$ be a surjective homomorphism of finite groups. Let Y be a subgroup of H. Let

$$X = f^{-1}(Y) = \{x \in G : f(x) \in Y\}$$

be the **inverse image** of Y in G. Then

$$|X| = |\ker f| \cdot |Y|$$

Proof: By the isomorphism theorem, without loss of generality $Y = G/N$ where $N = \ker f$ is a normal subgroup in G. The quotient group is the set of cosets gN. Thus,

$$f^{-1}(Y) = \{xN : f(x) \in Y\}$$

That is, the inverse image is a disjoint union of cosets of N, and the number of cosets in the inverse image is $|Y|$. We proved earlier that X is a subgroup of G. ///

A variant of the previous corollary gives

[5.0.4] Corollary: Given a normal subgroup N of a group G, and given any other subgroup H of G, let $q : G \longrightarrow G/N$ be the quotient map. Then

$$H \cdot N = \{hn : h \in H, n \in N\} = q^{-1}(q(H))$$

is a subgroup of G. If G is finite, the order of this group is

$$|H \cdot N| = \frac{|H| \cdot |N|}{|H \cap N|}$$

Further,

$$q(H) \approx H/(H \cap N)$$

Proof: By definition the inverse image $q^{-1}(q(H))$ is

$$\{g \in G : q(g) \in q(H)\} = \{g \in G : gN = hN \text{ for some } h \in H\}$$

$$= \{g \in G : g \in hN \text{ for some } h \in H\} = \{g \in G : g \in H \cdot N\} = H \cdot N$$

The previous corollary already showed that the inverse image of a subgroup is a subgroup. And if $hN = h'N$, then $N = h^{-1}h'N$, and $h^{-1}h' \in N$. Yet certainly $h^{-1}h' \in H$, so $h^{-1}h' \in H \cap N$. And, on the other hand, if $h^{-1}h' \in H \cap N$ then $hN = h'N$. Since $q(h) = hN$, this proves the isomorphism. From above, the inverse image $H \cdot N = q^{-1}(q(H))$ has cardinality

$$\operatorname{card} H \cdot N = |\ker q| \cdot |q(H)| = |N| \cdot |H/(H \cap N)| = \frac{|N| \cdot |H|}{|H \cap N|}$$

giving the counting assertion. ///

6. *Groups acting on sets*

Let G be a group and S a set. A map $G \times S \longrightarrow S$, denoted by juxaposition

$$g \times s \longrightarrow gs$$

is an **action** of the group on the set if
• $es = s$ for all $s \in S$
• *(Associativity)* $(gh)s = g(hs)$ for all $g, h \in G$ and $s \in S$.

These conditions assure that, for example, $gs = t$ for $s, t \in S$ and $g \in G$ implies that $g^{-1}t = s$. Indeed,

$$g^{-1}t = g^{-1}(gs) = (g^{-1}g)s = es = s$$

Sometimes a set with an action of a group G on it is called a G-**set**.

The action of G on a set is **transitive** if, for all $s, t \in S$, there is $g \in G$ such that $gs = t$. This definition admits obvious equivalent variants: for example, the seemingly weaker condition that there is $s_o \in S$ such that for every $t \in S$ there is $g \in G$ such that $gs_o = t$ implies transitivity. Indeed, given $s, t \in S$, let $g_s s_o = s$ and $g_t s_o = t$. Then

$$(g_t g_s^{-1})s = g_t(g_s^{-1}s) = g_t(s_o) = t$$

For G acting on a set S, a subset T of S such that $g(T) \subset T$ is G-**stable**.

[6.0.1] **Proposition:** For a group G acting on a set S, and for a G-stable subset T of S, in fact $g(T) = T$ for all $g \in G$.

Proof: We have

$$T = eT = (gg^{-1})T = g(g^{-1}(T)) \subset g(T) \subset T$$

Thus, all the inclusions must be equalities. ///

A single element $s_o \in S$ such that $gs_o = s_o$ for *all* $g \in G$ is G-**fixed**. Given an element $s_o \in S$, the **stabilizer** of s_o in G, often denoted G_{s_o}, is

$$G_{s_o} = \{g \in G : gs_o = s_o\}$$

More generally, for a subset T of S, the **stabilizer** of T in G is

$$\text{stabilizer of } T \text{ in } G = \{g \in G : g(T) = T\}$$

The **point-wise fixer** or **istropy subgroup** of a subset T is

$$\text{isotropy subgroup of } T = \text{point-wise fixer of } T \text{ in } G = \{g \in G : gt = t \text{ for all } t \in T\}$$

For a subgroup H of G, the **fixed points** S^H of H on S are the elements of the set

$$\text{fixed point set of } H = \{s \in S : hs = s \text{ for all } h \in H\}$$

[6.0.2] **Remark:** In contrast to the situation of the previous proposition, if we attempt to define the stabilizer of a subset by the weaker condition $g(T) \subset T$, the following proposition can fail (for infinite sets S).

[6.0.3] **Proposition:** Let G act on a set S, and let T be a subset of S. Then both the stabilizer and point-wise fixer of T in G are *subgroups* of G.

Proof: We only prove that the stabilizer of T is stable under inverses. Suppose $gT = T$. Then

$$g^{-1}T = g^{-1}(g(T)) = (g^{-1}g)(T) = e(T) = T$$

since $g(T) = T$. ///

With an action of G on the set S, a G-**orbit** in S is a *non-empty* G-stable subset of S, on which G is *transitive*.

[6.0.4] **Proposition:** Let G act on a set S. For any element s_o in an orbit O of G on S,

$$O = G \cdot s_o = \{gs_o : g \in G\}$$

Conversely, for any $s_o \in S$, the set $G \cdot s_o$ is a G-orbit on S.

Proof: Since an orbit O is required to be non-empty, O contains an element s_o. Since O is G-stable, certainly $gs_o \in S$ for all $g \in G$. Since G is transitive on O, the collection of all images gs_o of s_o by elements $g \in G$ must be the whole orbit O. On the other hand, any set

$$Gs_o = \{gs_o : g \in G\}$$

is G-stable, since $h(gs_o) = (hg)s_o$. And certainly G is transitive on such a set. ///

Now we come to some consequences for counting problems. [14]

[6.0.5] **Proposition:** Let G act transitively on a (non-empty) set S, and fix $s \in S$. Then S is in bijection with the set G/G_s of cosets gG_s of the isotropy group G_s of s in G, by

$$gs \longleftrightarrow gG_s$$

Thus,

$$\operatorname{card} S = [G : G_s]$$

Proof: If $hG_s = gG_s$, then there is $x \in G_s$ such that $h = gx$, and $hs = gxs = gs$. On the other hand, if $hs = gs$, then $g^{-1}hs = s$, so $g^{-1}h \in G_s$, and then $h \in gG_s$. ///

[6.0.6] **Corollary:** *(Counting formula)* Let G be a finite group acting on a finite set S. Let X be the set of G-orbits in S. For $O \in X$ let $s_O \in O$. And

$$\operatorname{card} S = \sum_{O \in X} \operatorname{card} O = \sum_{O \in X} [G : G_{s_O}]$$

Proof: The set S is a disjoint union of the G-orbits in it, so the cardinality of S is the sum of the cardinalities of the orbits. The cardinality of each orbit is the index of the isotropy group of a chosen element in it, by the previous proposition. ///

Two fundamental examples of natural group actions are the following.

[6.0.7] **Example:** A group G acts on itself (as a set) by **conjugation**: [15] for $g, x \in G$,

$$\text{conjugate of } x \text{ by } g = gxg^{-1}$$

[14] Yes, these look boring and innocent, in this abstraction.

[15] It is obviously not wise to use the notation gh for ghg^{-1}.

It is easy to verify that for fixed $g \in G$, the map

$$x \longrightarrow gxg^{-1}$$

is an isomorphism of G to itself. For x and y elements of G in the same G-orbit under this action, say that x and y **are conjugate**. The orbits of G on itself with the conjugation action are **conjugacy classes** (of elements). The **center** of a group G is the set of elements z whose orbit under conjugation is just $\{z\}$. That is,

$$\text{center of } G = \{z \in G : gz = zg \text{ for all } g \in G\}$$

Either directly or from general principles (above), the center Z of a group G is a *subgroup* of G. Further, it is *normal*:

$$gZg^{-1} = \{gzg^{-1} : z \in Z\} = \{z : z \in Z\} = Z$$

And of course the center is itself an *abelian* group.

[6.0.8] **Example:** For a subgroup H of G and for $g \in G$, the **conjugate** subgroup gHg^{-1} is

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

Thus, G acts on the set of its own subgroups by conjugation. [16] As with the element-wise conjugation action, for H and K subgroups of G in the same G-orbit under this action, say that H and K **are conjugate**. The orbits of G on its subgroups with the conjugation action are **conjugacy classes** (of subgroups). The *fixed points* of G under the conjugation action on subgroups are just the *normal* subgroups. On the other hand, for a given subgroup H, the isotropy subgroup in G for the conjugation action is called the **normalizer** of H in G:

$$\text{normalizer of } H \text{ in } G = \{g \in G : gHg^{-1} = H\}$$

Either directly or from more general principles (above), the normalizer of H in G is a subgroup of G (containing H).

---

7. The Sylow theorem

There is not much that one can say about the subgroups of an arbitrary finite group. Lagrange's theorem is the simplest very general assertion. Sylow's theorem is perhaps the strongest and most useful relatively elementary result limiting the possibilities for subgroups and, therefore, for finite groups.

Let p be a prime. A p-**group** is a finite group whose order is a power of the prime p. Let G be a finite group. Let p^e be the largest power of p dividing the order of G. A p-**Sylow** subgroup (if it exists) is a subgroup of G of order p^e.

[7.0.1] **Remark:** By Lagrange's theorem, no larger power of p can divide the order of *any* subgroup of G.

[7.0.2] **Theorem:** Let p be a prime. Let G be a finite group. Let p^e be the largest power of p dividing the order of G. Then
- G has p-Sylow subgroups.
- Every subgroup of G with order a power of p lies inside a p-Sylow subgroup of G.
- The number n_p of p-Sylow subgroups satisfies

$$n_p | \text{order}(G) \qquad n_p = 1 \bmod p$$

[16] And, again, it is manifestly unwise to write gH for gH^{-1}.

• Any two p-Sylow subgroups P and Q are **conjugate**. [17]
• A group of order p^n has a non-trivial center.

It is convenient to prove a much weaker and simpler result first, which also illustrates a style of induction via subgroups and quotients:

[7.0.3] **Lemma:** Let A be a finite *abelian* group, and let p be a prime dividing the order of A. Then there is an element a of A of order exactly p. Thus, there exists a subgroup of A of order p.

Proof: (of lemma) Use induction on the order of A. If the order is p exactly, then any non-identity element is of order p. Since a prime divides its order, A is not the trivial group, so we can choose a non-identity element g of A. By Lagrange, the order n of g divides the order of A. If p divides n, then $g^{n/p}$ is of order exactly p and we're done. So suppose that p does *not* divide the order of g. Then consider the quotient

$$q(A) = B = A/\langle g\rangle$$

of A by the cyclic subgroup generated by g. The order of B is still divisible by p (since $|\langle g\rangle|$ is not), so by induction on order there is an element y in B of order exactly p. Let x be any element in A which maps to y under the quotient map $q : A \longrightarrow B$. Let N be the order of x. The prime p divides N, or else write $N = \ell p + r$ with $0 < r < p$, and

$$e_B = q(e_A) = q(x^N) = y^N = y^{\ell p + r} = y^r \neq e_B$$

contradiction. Then $x^{N/p}$ has order exactly p, and the cyclic subgroup generated by $x^{N/p}$ has order p.
///

Proof: Now prove the theorem. First, we prove *existence* of p-Sylow subgroups by induction on the exponent e of the power p^e of p dividing the order of G. (Really, the induction uses subgroups and quotient groups of G.) If $e = 0$ the p-Sylow subgroup is the trivial subgroup, and there is nothing to prove. For fixed $e > 1$, do induction on the order of the group G. If any proper subgroup H of G has order divisible by p^e, then invoke the theorem for H, and a p-Sylow subgroup of H is one for G. So suppose that *no* proper subgroup of G has order divisible by p^e. Then for any subgroup H of G the prime p divides $[G : H]$. By the *counting formula* above, using the conjugation action of G on itself,

$$\operatorname{card} G = \sum_x [G : G_x]$$

where x is summed over (irredundant) representatives for conjugacy classes. Let Z be the center of G. Then Z consists of G-orbits each with a single element. We rewrite the counting formula as

$$\operatorname{card} G = \operatorname{card} Z + \sum_x^{\text{non}-\text{central}} [G : G_x]$$

where now x is summed over representatives *not* in the center. For non-central x the isotropy group G_x is a proper subgroup, so by assumption, p divides $[G : G_x]$ for all x. Since p divides the order of G, we conclude from the counting formula that p divides the order of the center Z (but p^e does not divide the order of Z). Using the lemma above, let A be a subgroup of Z of order p. Since A is inside the center it is still normal. Consider the quotient group $H = G/A$, with quotient map $q : A \longrightarrow B$. The power of p dividing the order of H is p^{e-1}, strictly smaller than p^e. By induction, let Q be a p-Sylow subgroup of H, and let $P = q^{-1}(Q)$ be the inverse image of Q under the quotient map q. Then

$$|P| = |q^{-1}(Q)| = |\ker q| \cdot |Q| = p \cdot p^{e-1} = p^e$$

[17] This property is the sharpest and most surprising assertion here.

from the counting corollary of the isomorphism theorem (above). Thus, G does have a p-Sylow theorem after all.

If it happens that $|G| = p^e$, looking at that same formula

$$\operatorname{card} G = \operatorname{card} Z + \sum_x^{\text{non-central}} [G : G_x]$$

the left-hand side is p^e, and all the summands corresponding to non-central conjugacy classes are divisible by p, so the order of the center is divisible by p. That is, p-power-order groups have non-trivial centers.

Let X be *any* G-conjugation stable set of p-Sylow subgroups. Fix a p-power-order subgroup Q not necessarily in X, and let Q act on the set X by conjugation. The counting formula gives

$$\operatorname{card} X = \sum_x [Q : Q_x]$$

where x runs over representatives for Q-conjugacy classes in X. If Q normalized a p-Sylow subgroup x not containing Q, then

$$H = Q \cdot x$$

would be a subgroup of order

$$|Q \cdot x| = \frac{|Q| \cdot |x|}{|Q \cap x|} > |x|$$

and would be a power of p, contradicting the maximality of x. Thus, the only p-Sylow subgroups normalized by any p-power-order subgroup Q are those containing Q. Thus, except for x containing Q, all the indices $[Q : Q_x]$ are divisible by p. Thus,

$$|X| = |\{x \in X : Q \subset x\}| + \sum_x^{Q \not\subset x} [Q : Q_x]$$

In the case that Q itself is a p-Sylow subgroup, and X is *all* p-Sylow subgroups in G,

$$|\{x \in X : Q \subset x\}| = |\{Q\}| = 1$$

so the number of *all* p-Sylow subgroups is 1 mod p.

Next, let X consist of a single G-conjugacy class of p-Sylow subgroups. Fix $x \in X$. Since X is a single orbit,

$$|X| = [G : G_x]$$

and the latter index is *not* divisible by p, since the normalizer G_x of x contains x. Let a p-power-subgroup Q act by conjugation on X. In the counting formula

$$|X| = |\{x \in X : Q \subset x\}| + \sum_x^{Q \not\subset x} [Q : Q_x]$$

all the indices $[Q : Q_x]$ are divisible by p, but $|X|$ is *not*, so

$$|\{x \in X : Q \subset x\}| \neq 0$$

That is, given a p-power-order subgroup Q, *every* G-conjugacy class of p-Sylow subgroups contains an x containing Q. This is only possible if there is a *unique* G-conjugacy class of p-Sylow subgroups. That is, the conjugation action of G is *transitive* on p-Sylow subgroups.

Further, since Q was not necessarily maximal in this last discussion, we have shown that every p-power-order subgroup of G lies inside at least one p-Sylow subgroup.

And, fixing a single p-Sylow subgroup x, using the transitivity, the number of *all* p-Sylow subgroups is

$$\text{number } p\text{-Sylow subgroups} = [G : G_x] = |G|/|G_x|$$

This proves the divisibility property. ///

[7.0.4] **Remark:** For general integers d dividing the order of a finite group G, it is seldom the case that there is a subgroup of G of order d. By contrast, if G is *cyclic* there is a *unique* subgroup for every divisor of its order. If G is *abelian* there is *at least one* subgroup for every divisor of its order.

[7.0.5] **Remark:** About the proof of the Sylow theorem: once one knows that the proof uses the conjugation action on elements and on subgroups, there are not so many possible directions the proof could go. Knowing these limitations on the proof methodology, one could hit on a correct proof after a relatively small amount of trial and error.

---

8. *Trying to classify finite groups, part I*

Lagrange's theorem and the Sylow theorem allow us to make non-trivial progress on the project of classifying finite groups whose orders have relatively few prime factors. That is, we can prove that there are not many non-isomorphic groups of such orders, sometimes a single isomorphism class for a given order. This sort of result, proving that an abstraction miraculously allows fewer instances than one might have imagined, is often a happy and useful result.

Groups of prime order: Let p be a prime, and suppose that G is a group with $|G| = p$. Then by Lagrange's theorem there are no proper subgroups of G. Thus, picking any element g of G other than the identity, the (cyclic) subgroup $\langle g\rangle$ generated by g is necessarily the whole group G. That is, for such groups G, choice of a non-identity element g yields

$$G = \langle g\rangle \approx \mathbb{Z}/p$$

Groups of order pq, part I: Let $p < q$ be primes, and suppose that G is a group with $|G| = pq$. Sylow's theorem assures that there exist subgroups P and Q of orders p and q, respectively. By Lagrange, the order of $P \cap Q$ divides both p and q, so is necessarily 1. Thus,

$$P \cap Q = \{e\}$$

Further, the number n_q of q-Sylow subgroups must be 1 mod q and also divide the order pq of the group. Since $q = 0 \bmod q$, the only possibilities (since p is prime) are that either $n_q = p$ or $n_q = 1$. But $p < q$ precludes the possibility that $n_q = p$, so $n_q = 1$. That is, with $p < q$, the q-Sylow subgroup is necessarily *normal*.

The same argument, apart from the final conclusion invoking $p < q$, shows that the number n_p of p-Sylow subgroups is either $n_p = 1$ or $n_p = q$, and (by Sylow) is $n_p = 1 \bmod p$. But now $p < q$ does *not* yield $n_p = 1$. There are two cases, $q = 1 \bmod p$ and otherwise.

If $q \neq 1 \bmod p$, then we *can* reach the conclusion that $n_p = 1$, that is, that the p-Sylow subgroup is also normal. Thus, for $p < q$ and $q \neq 1 \bmod p$, we have a normal p-Sylow group P and a normal q-Sylow subgroup Q. Again, $P \cap Q = \{e\}$ from Lagrange.

How to reconstruct G from such facts about its subgroups?

We need to enrich our vocabulary: given two groups G and H, the **(direct) product** group $G \times H$ is the cartesian product with the operation

$$(g, h) \cdot (g', h') = (gg', hh')$$

(It is easy to verify the group properties.) For G and H abelian, with group operations written as addition, often the direct product is written instead as a **(direct) sum** [18]

$$G \oplus H$$

[8.0.1] **Proposition:** Let A and B be normal [19] subgroups of a group G, such that $A \cap B = \{e\}$. Then

$$f : A \times B \longrightarrow A \cdot B = \{ab : a \in A, b \in B\}$$

by

$$f(a, b) = ab$$

is an isomorphism. The subgroup $A \cdot B \approx A \times B$ is a normal subgroup of G. In particular, $ab = ba$ for all $a \in A$ and $b \in B$.

Proof: The trick is to consider **commutator** expressions

$$aba^{-1}b^{-1} = aba^{-1} \cdot b^{-1} = a \cdot ba^{-1}b^{-1}$$

for $a \in A$ and $b \in B$. Since B is normal, the second expression is in B. Since A is normal, the third expression is in A. Thus, the commutator $aba^{-1}b^{-1}$ is in $A \cap B$, which is $\{e\}$. [20] Thus, right multiplying by b

$$aba^{-1} = b$$

or, right multiplying further by a,

$$ab = ba$$

The fact that $ab = ba$ for all $a \in A$ and all $\underline{in}B$ allows one to easily show that f is a group homomorphism. Its kernel is trivial, since $ab = e$ implies

$$a = b^{-1} \in A \cap B = \{e\}$$

Thus, the map is injective, from earlier discussions. Now $|A \times B| = pq$, and the map is injective, so $f(A \times B)$ is a subgroup of G with order pq. Thus, the image is all of G. That is, f is an isomorphism. ///

[8.0.2] **Proposition:** Let A and B by cyclic groups of relatively prime orders m and n. Then $A \times B$ is cyclic of order mn. In particular, for a a generator for A and b a generator for B, (a, b) is a generator for the product.

Proof: Let N be the least positive integer such that $N(a, b) = (e_A, e_B)$. Then $Na = e_A$, so $|a|$ divides N. Similarly, $|b|$ divides N. Since $|a|$ and $|b|$ are relatively prime, this implies that their product divides N. ///

[8.0.3] **Corollary:** For $|G| = pq$ with $p < q$ and $q \neq 1 \bmod p$, G is cyclic of order pq. Hence, in particular, there is only *one* isomorphism class of groups of such orders pq. ///

---

[18] Eventually we will make some important distinctions between direct sums and direct products, but there is no need to do so just now.

[19] Unless at least one of the subgroups is normal, the set $A \cdot B$ may not even be a subgroup, much less normal.

[20] By Lagrange, again. Very soon we will tire of explicit invocation of Lagrange's theorem, and let it go without saying.

[8.0.4] **Remark:** Even without the condition $q \neq 1 \bmod p$, we do have the cyclic group $\mathbb{Z}/pq$ of order pq, but without that condition we cannot prove that there are no *other* groups of order pq. [21] We'll delay treatment of $|G| = pq$ with primes $p < q$ and $q = 1 \bmod p$ till after some simpler examples are treated.

[8.0.5] **Example:** Groups of order $15 = 3 \cdot 5$, or order $35 = 5 \cdot 7$, of order $65 = 5 \cdot 13$, etc., are necessarily cyclic of that order. By contrast, we reach no such conclusion about groups of order $6 = 2 \cdot 4$, $21 = 3 \cdot 7$, $55 = 5 \cdot 11$, etc. [22]

Groups G of order pqr with distinct primes p, q, r: By Sylow, there is a p-Sylow subgroup P, a q-Sylow subgroup Q, and an r-Sylow subgroup R. Without any further assumptions, we cannot conclude anything about the normality of any of these Sylow subgroups, by contrast to the case where the order was pq, wherein the Sylow subgroup for the larger of the two primes was invariably normal.

One set of hypotheses which allows a simple conclusion is

$$\begin{array}{lll} q \neq 1 \bmod p & r \neq 1 \bmod p & qr \neq 1 \bmod p \\ p \neq 1 \bmod q & r \neq 1 \bmod q & pr \neq 1 \bmod q \\ p \neq 1 \bmod r & q \neq 1 \bmod r & pq \neq 1 \bmod r \end{array}$$

These conditions would suffice to prove that all of P, Q, and R are normal. Then the little propositions above prove that $P \cdot Q$ is a normal cyclic subgroup of order pq, and then (since still pq and r are relatively prime) that $(PQ) \cdot R$ is a cyclic subgroup of order pqr, so must be the whole group G. That is, G is cyclic of order pqr.

Groups of order pq, part II: Let $p < q$ be primes, and now treat the case that $q = 1 \bmod p$, so that a group G of order pq need *not* be cyclic. Still, we know that the q-Sylow subgroup Q is *normal*. Thus, for each x in a fixed p-Sylow subgroup P, we have a map $a_x : Q \longrightarrow Q$ defined by

$$a_x(y) = xyx^{-1}$$

Once the normality of Q assures that this really does map back to Q, it is visibly an isomorphism of Q to itself. This introduces:

An isomorphism of a group to itself is an **automorphism**. [23] The **group of automorphisms** of a group G is

$$\mathrm{Aut}(G) = \mathrm{Aut}G = \{\text{isomorphisms } G \longrightarrow G\}$$

It is easy to check that $\mathrm{Aut}(G)$ is indeed a group, with operation being the composition of maps, and identity being the identity map 1_G defined by [24]

$$1_G(g) = g \quad (\text{for any } g \text{ in } G)$$

In general it is a non-trivial matter to determine in tangible terms the automorphism group of a given group, but we have a simple case:

[8.0.6] **Proposition:**

$$\mathrm{Aut}(\mathbb{Z}/n) \approx (\mathbb{Z}/n)^\times$$

by defining, for each $z \in (\mathbb{Z}/n)^\times$, and for $x \in \mathbb{Z}/n$,

$$f_z(x) = zx$$

[21] And, indeed, there *are* non-cyclic groups of those orders.

[22] And, again, there *are* non-cyclic groups of such orders.

[23] A homomorphism that is not necessarily an isomorphism of a group to itself is an *endomorphism*.

[24] This should be expected.

On the other hand, given an automorphism f, taking $z = f(1)$ gives $f_z = f$.

Proof: For z multiplicatively invertible mod n, since the addition and multiplication in $\mathbb{Z}/n$ enjoy a distributive property, f_z is an automorphism of $\mathbb{Z}/n$ to itself. On the other hand, given an automorphism f of $\mathbb{Z}/n$, let $z = f(1)$. Then, indeed, identifying x in $\mathbb{Z}/n$ with an ordinary integer,

$$f(x) = f(x \cdot 1) = f(\underbrace{1 + \ldots + 1}_{x}) = \underbrace{f(1) + \ldots + f(1)}_{x} = \underbrace{z + \ldots + z}_{x} = zx$$

That is, *every* automorphism is of this form. ///

Given two groups H and N, with a group homomorphism

$$f : H \longrightarrow \mathrm{Aut}(N) \quad \text{denoted} \quad h \longrightarrow f_h$$

the **semi-direct product** group

$$H \times_f N$$

is the set $H \times N$ with group operation intending to express the idea that

$$hnh^{-1} = f_h(n)$$

But since H and N are not literally subgroups of anything yet, we must say, instead, that we want

$$(h, e_N)(e_H, n)(h^{-1}, e_N) = (e_H, f_h(n))$$

After some experimentation, one might decide upon the definition of the operation

$$(h, n) \cdot (h', n') = (hh', f_{h'^{-1}}(n)\, n')$$

Of course, when f is the trivial homomorphism (sending everything to the identity) the semi-direct product is simply the direct product of the two groups.

[8.0.7] **Proposition:** With a group homomorphism $f : H \longrightarrow \mathrm{Aut}(N)$, the semi-direct product $H \times_f N$ is a group. The maps $h \longrightarrow (h, e_N)$ and $n \longrightarrow (e_H, n)$ inject H and N, respectively, and the image of N is normal.

Proof: [25] The most annoying part of the argument would be proof of associativity. On one hand,

$$((h, n)(h', n'))\ (h'', n'') = (hh', f_{h'^{-1}}(n)n')\,(h'', n'') = (hh'h'', f_{h''^{-1}}\,(f_{h'^{-1}}(n)n')\,n'')$$

The H-component is uninteresting, so we only look at the N-component:

$$f_{h''^{-1}}\,(f_{h'^{-1}}(n)n')\,n'' = f_{h''^{-1}} \circ f_{h'^{-1}}(n) \cdot f_{h''^{-1}}(n') \cdot n'' = f_{(h'h'')^{-1}}(n) \cdot f_{h''^{-1}}(n') \cdot n''$$

which is the N-component which would arise from

$$(h, n)\ ((h', n')(h'', n''))$$

This proves the associativity. The other assertions are simpler. ///

[25] There is nothing surprising in this argument. It amounts to checking what must be checked, and there is no obstacle other than bookkeeping. It is surely best to go through it oneself rather than watch someone else do it, but we write it out here just to prove that it is possible to force oneself to carry out some of the details.

Thus, in the $|G| = pq$ situation, because Q is normal, we have a group homomorphism

$$\mathbb{Z}/p \approx P \longrightarrow \mathrm{Aut}(Q) \approx (\mathbb{Z}/q)^\times$$

The latter is of order $q-1$, so unless $p|(q-1)$ this homomorphism must have trivial image, that is, P and Q commute, giving yet another approach to the case that $q \neq 1 \bmod p$. But for $p|(q-1)$ there is at least one non-trivial homomorphism to the automorphism group: $(\mathbb{Z}/q)^\times$ is an abelian group of order divisible by p, so there exists [26] an element z of order p. Then take $f : \mathbb{Z}/p \longrightarrow \mathrm{Aut}(\mathbb{Z}/q)$ by

$$f(x)(y) = z^x \cdot y \in \mathbb{Z}/q$$

This gives a semi-direct product of $\mathbb{Z}/p$ and $\mathbb{Z}/q$ which cannot be abelian, since elements of the copy P of $\mathbb{Z}/p$ and the copy Q of $\mathbb{Z}/q$ do not all commute with each other. That is, there is at least one non-abelian [27] group of order pq if $q = 1 \bmod p$.

How many different semi-direct products are there? [28] Now we must use the non-trivial fact that $(\mathbb{Z}/q)^\times$ is *cyclic* for q prime. [29] That is, granting this cyclicness, there are *exactly* $p-1$ elements in $(\mathbb{Z}/q)^\times$ of order p. Thus, given a fixed element z of order p in $(\mathbb{Z}/q)^\times$, any other element of order p is a power of z.

Luckily, this means that, given a choice of isomorphism $i : \mathbb{Z}/p \approx P$ to the p-Sylow group P, and given non-trivial $f : P \longrightarrow \mathrm{Aut}(Q)$, whatever the image $f(i(1))$ may be, we can alter the choice of i to achieve the effect that

$$f(i(1)) = z$$

Specifically, if at the outset

$$f(i(1)) = z'$$

with some other element z' of order p, use the cyclicness to find an integer ℓ (in the range $1, 2, \ldots, p-1$) such that

$$z' = z^\ell$$

Since ℓ is prime to p, it has an inverse modulo k mod p. Then

$$f(i(k)) = f(k \cdot i(1)) = f(i(1))^k = (z')^k = (z^\ell)^k = z$$

since $\ell k = 1 \bmod p$ and z has order p.

In summary, with primes $q = 1 \bmod p$, up to isomorphism there is a *unique* non-abelian group of order pq, and it is a semi-direct product of $\mathbb{Z}/p$ and $\mathbb{Z}/q$. [30]

Groups of order p^2, with prime p: A different aspect of the argument of the Sylow theorem is that a p-power-order group G necessarily has a non-trivial center Z. If $Z = G$ we have proven that G is abelian. Suppose Z is proper. Then [31] it is of order p, thus [32] necessarily *cyclic*, with generator z. Let x be any

[26] Existence follows with or without use of the fact that there are primitive roots modulo primes. For small numerical examples this cyclicness can be verified directly, without necessarily appealing to any theorem that guarantees it.

[27] So surely non-cyclic.

[28] As usual in this context, *different* means *non-isomorphic*.

[29] This is the existence of *primitive roots* modulo primes.

[30] The argument that showed that seemingly different choices yield isomorphic groups is an ad hoc example of a wider problem, of classification up to isomorphism of *group extensions*.

[31] Lagrange

[32] Lagrange

other group element *not* in Z. It cannot be that the order of x is p^2, or else $G = \langle x\rangle$ and $G = Z$, contrary to hypothesis. Thus, [33] the order of x is p, and [34]

$$\langle x\rangle \cap \langle z\rangle = \{e\}$$

Abstracting the situation just slightly:

[8.0.8] Proposition: [35] Let G be a finite group with center Z and a subgroup A of Z. Let B be another abelian subgroup of G, such that $A \cap B = \{e\}$ and $A \cdot B = G$. Then the map

$$f : A \times B \longrightarrow A \cdot B$$

by

$$a \times b \longrightarrow ab$$

is an isomorphism, and $A \cdot B$ is abelian.

Proof: If $a \times b$ were in the kernel of f, then $ab = e$, and

$$a = b^{-1} \in A \cap B = \{e\}$$

And

$$f((a,b)\cdot(a',b')) = f(aa',bb') = aa'bb'$$

while

$$f(a,b)\cdot f(a',b') = ab \cdot a'b' = aa'bb'$$

because $ba' = a'b$, because elements of A commute with everything. That is, f is a homomorphism. Since both A and B are abelian, certainly the product is. ///

That is, any group G of order p^2 (with p prime) is abelian. So our supposition that the center of such G is of order only p is false.

Starting over, but knowing that G of order p^2 is abelian, if there is no element of order p^2 in G (so G is not cyclic), then in any case there is an element z of order p. [36] And take x not in $\langle z\rangle$. Necessarily x is of order p. By the same clichéd sort of argument as in the last proposition, $\langle x\rangle \cap \langle z\rangle = \{e\}$ and

$$\mathbb{Z}/p \times \mathbb{Z}/p \approx \langle x\rangle \times \langle z\rangle \approx \langle x\rangle \cdot \langle z\rangle = G$$

That is, *non-cyclic* groups of order p^2 are isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$.

Automorphisms of groups of order q^2: Anticipating that we'll look at groups of order pq^2 with normal subgroups of order q^2, to understand semi-direct products $P \times_f Q$ with P of order p and Q of order q^2 we must have *some* understanding of the automorphism groups of groups of order q^2, since $f : P \longrightarrow \mathrm{Aut}\, Q$ determines the group structure. For the moment we will focus on merely the *order* of these automorphism groups. [37]

---

[33] Lagrange

[34] Lagrange

[35] This is yet another of an endless stream of variations on a theme.

[36] For example, this follows from the lemma preparatory to the Sylow theorem.

[37] After some further preparation concerning finite fields and linear algebra we can say more definitive structural things.

For Q cyclic of order q^2, we know that $Q \approx \mathbb{Z}/q^2$, and from above

$$\mathrm{Aut}\, Q \approx \mathrm{Aut}(\mathbb{Z}/q^2) \approx (\mathbb{Z}/q^2)^\times$$

In particular, the *order* is [38]

$$|\mathrm{Aut}\, Q| = \mathrm{card}\,(\mathbb{Z}/q^2)^\times = \varphi(q^2) = q(q-1)$$

This is easy.

For Q non-cyclic of order q^2, we saw that

$$Q \approx \mathbb{Z}/q \oplus \mathbb{Z}/q$$

where we write direct sum to emphasize the abelian-ness of Q. [39] For the moment we only aim to *count* these automorphisms. Observe that [40]

$$(\bar{x}, \bar{y}) = x \cdot (\bar{1}, \bar{0}) + y \cdot (\bar{0}, \bar{1})$$

for any $x, y \in \mathbb{Z}$, where for the moment the bars denotes residue classes modulo q. Thus, for any automorphism α of Q

$$\alpha(\bar{x}, \bar{y}) = x \cdot \alpha(\bar{1}, \bar{0}) + y \cdot \alpha(\bar{0}, \bar{1})$$

where multiplication by an integer is repeated addition. Thus, the images of $(\bar{1}, \bar{0})$ and $(\bar{0}, \bar{1})$ determine α completely. And, similarly, *any* choice of the two images gives a group homomorphism of Q to itself. The only issue is to avoid having a proper kernel. To achieve this, $\alpha(\bar{1}, \bar{0})$ certainly must not be $e \in Q$, so there remain $q^2 - 1$ possible choices for the image of $(\bar{1}, \bar{0})$. Slightly more subtly, $\alpha(\bar{0}, \bar{1})$ must not lie in the cyclic subgroup generated by $\alpha(\bar{1}, \bar{0})$, which excludes exactly q possibilities, leaving $q^2 - q$ possibilities for $\alpha(\bar{0}, \bar{1})$ for each choice of $\alpha(\bar{1}, \bar{0})$. Thus, altogether,

$$\mathrm{card}\ \mathrm{Aut}(\mathbb{Z}/q \oplus \mathbb{Z}/q) = (q^2 - 1)(q^2 - q)$$

We will pursue this later.

Groups of order pq^2: As in the simpler examples, the game is to find some mild hypotheses that combine with the Sylow theorem to limit the possibilities for the arrangement of Sylow subgroups, and then to look at direct product or semi-direct product structures that can arise. Let G be a group of order pq^2 with p, q distinct primes.

As a preliminary remark, if G is assumed abelian, then G is necessarily the direct product of a p-Sylow subgroup and a q-Sylow subgroup (both of which are necessarily norml), and by the classification of order q^2 groups this gives possibilities

$$G = P \cdot Q \approx P \times Q \approx \mathbb{Z}/p \times Q \approx \begin{cases} \mathbb{Z}/p \oplus \mathbb{Z}/q^2 & \approx & \mathbb{Z}/pq^2 \\ \mathbb{Z}/p \oplus \mathbb{Z}/q \oplus \mathbb{Z}/q & \approx & \mathbb{Z}/q \oplus \mathbb{Z}/pq \end{cases}$$

in the two cases for Q, writing direct sums to emphasize the abelian-ness. So now we consider non-abelian possibilities, and/or hypotheses which force a return to the abelian situation.

---

[38] Using Euler's totient function φ.

[39] Thus, in fact, Q is a two-dimensional vector space over the finite field $\mathbb{Z}/q$. We will more systematically pursue this viewpoint shortly.

[40] Yes, this is linear algebra.

The first and simplest case is that neither $p = 1 \bmod q$ nor $q^2 = 1 \bmod p$. Then, by Sylow, there is a unique q-Sylow subgroup Q and a unique p-Sylow subgroup P, both necessarily normal. We just saw that the group Q of order q^2 is necessarily [41] abelian. Since both subgroups are normal, elements of Q commute with elements of P. [42] This returns us to the abelian case, above.

A second case is that $p|(q-1)$. This implies that $p < q$. The number n_q of q-Sylow subgroups is $1 \bmod q$ and divides pq^2, so is either 1 or p, but $p < q$, so necessarily $n_q = 1$. That is, the q-Sylow subgroup Q is normal. But this does not follow for the p-Sylow subgroup, since now $p|(q-1)$. The Sylow theorem would seemingly allow the number n_p of p-Sylow subgroups to be 1, q, or q^2. Thus, we should consider the possible semi-direct products

$$\mathbb{Z}/p \times_f Q$$

for

$$f : \mathbb{Z}/p \longrightarrow \mathrm{Aut}\, Q$$

If f is the trivial homomorphism, then we obtain a direct product, returning to the abelian case. For $Q \approx \mathbb{Z}/q^2$ its automorphism group has order $q(q-1)$, which is divisible by p (by hypothesis), so [43] has an element of order p. That is, there does exist a non-trivial homomorphism

$$f : P \approx \mathbb{Z}/p \longrightarrow \mathrm{Aut}\, \mathbb{Z}/q^2$$

That is, there do exist non-abelian semi-direct products

$$\mathbb{Z}/p \times_f \mathbb{Z}/q^2$$

Distinguishing the isomorphism classes among these is similar to the case of groups of order pq with $p|(q-1)$, and we would find just a single non-abelian isomorphism class. For $\mathbb{Q} \approx \mathbb{Z}/q \oplus \mathbb{Z}/q$, we saw above that

$$|\mathrm{Aut}(\mathbb{Z}/q \oplus \mathbb{Z}/q)| = (q^2-1)(q^2-q) = (q-1)^2\, q\, (q+1)$$

Thus, there is at least one non-abelian semi-direct product

$$\mathbb{Z}/p \times_f (\mathbb{Z}/q \oplus \mathbb{Z}/q)$$

Attempting to count the isomorphism classes would require that we have more information on the automorphism group, which we'll obtain a little later.

A third case is that $p|(q+1)$. This again implies that $p < q$, except in the case that $q = 2$ and $p = 3$, which we'll ignore for the moment. The number n_q of q-Sylow subgroups is $1 \bmod q$ and divides pq^2, so is either 1 or p, but $p < q$, so necessarily $n_q = 1$. That is, the q-Sylow subgroup Q is normal. But this does not follow for the p-Sylow subgroup, since now $p|(q+1)$. The Sylow theorem would seemingly allow the number n_p of p-Sylow subgroups to be 1 or q^2. Thus, we should consider the possible semi-direct products

$$\mathbb{Z}/p \times_f Q$$

for

$$f : \mathbb{Z}/p \longrightarrow \mathrm{Aut}\, Q$$

---

[41] As a different sort of corollary of Sylow.

[42] The earlier argument is worth repeating: for a in one and b in another of two normal subgroups with trivial intersection, $(aba^{-1})b^{-1} = a(ba^{-1})b^{-1}$ must lie in both, so is e. Then $ab = ba$.

[43] By the lemma preceding the Sylow theorem, for example. In fact, all primes q the group $(\mathbb{Z}/q^2)^\times$ is *cyclic*, so will have *exactly one* subgroup of order p.

If f is the trivial homomorphism, then we obtain a direct product, returning to the abelian case. For $Q \approx \mathbb{Z}/q^2$ its automorphism group has order $q(q-1)$, which is not divisible by p, since $p|(q+1)$. That is, for $Q \approx \mathbb{Z}/q^2$ and $p|(q+1)$ and $q > 2$, there is *no* non-trivial homomorphism

$$f : P \approx \mathbb{Z}/p \longrightarrow \mathrm{Aut}\,\mathbb{Z}/q^2$$

That is, in this case there is *no* non-abelian semi-direct product

$$\mathbb{Z}/p \times_f \mathbb{Z}/q^2$$

For $\mathbb{Q} \approx \mathbb{Z}/q \oplus \mathbb{Z}/q$, we saw above that

$$|\mathrm{Aut}(\mathbb{Z}/q \oplus \mathbb{Z}/q)| = (q^2-1)(q^2-q) = (q-1)^2\, q\, (q+1)$$

Thus, there is at least one non-abelian semi-direct product

$$\mathbb{Z}/p \times_f (\mathbb{Z}/q \oplus \mathbb{Z}/q)$$

Again, attempting to count the isomorphism classes would require that we have more information on the automorphism group.

A fourth case is that $q|(p-1)$. Thus, by the same arguments as above, the p-Sylow subgroup P is normal, but the q-Sylow subgroup Q might not be. There are non-trivial homomorphisms in both cases

$$f : \begin{cases} \mathbb{Z}/p \oplus \mathbb{Z}/q^2 & \approx & \mathbb{Z}/pq^2 \\ \mathbb{Z}/p \oplus \mathbb{Z}/q \oplus \mathbb{Z}/q & \approx & \mathbb{Z}/q \oplus \mathbb{Z}/pq \end{cases} \longrightarrow \mathrm{Aut}\,\mathbb{Z}/p \approx (\mathbb{Z}/p)^\times$$

so either type of q-Sylow subgroup Q of order q^2 can give non-trivial automorphisms of the normal p-Sylow group P. Again, determining isomorphism classes in the first case is not hard, but in the second requires more information about the structure of $\mathrm{Aut}(\mathbb{Z}/q \oplus \mathbb{Z}/q)$.

[8.0.9] **Remark:** The above discussion is fast approaching the limit of what we can deduce about finite groups based only on the prime factorization of their order. The cases of prime order and order pq with distinct primes are frequently genuinely useful, the others less so.

9. Worked examples

[2.1] Let G, H be finite groups with relatively prime orders. Show that any group homomorphism $f : G \longrightarrow H$ is necessarily trivial (that is, sends every element of G to the identity in H.)

The isomorphism theorem implies that

$$|G| = |\ker f| \cdot |f(G)|$$

In particular, $|f(G)|$ divides $|G|$. Since $f(G)$ is a subgroup of H, its order must also divide $|H|$. These two orders are relatively prime, so $|f(G)| = 1$.

[2.2] Let m and n be integers. Give a formula for an isomorphism of abelian groups

$$\frac{\mathbb{Z}}{m} \oplus \frac{\mathbb{Z}}{n} \longrightarrow \frac{\mathbb{Z}}{\gcd(m,n)} \oplus \frac{\mathbb{Z}}{\mathrm{lcm}(m,n)}$$

Let r, s be integers such that $rm + sn = \gcd(m, n)$. Let $m' = m/\gcd(m, n)$ and $n' = n/\gcd(m, n)$. Then $rm' + sn' = 1$. We claim that

$$f(a + m\mathbb{Z}, b + n\mathbb{Z}) = ((a - b) + \gcd(m,n)\mathbb{Z},\ (b \cdot rm' + a \cdot sn') + \mathrm{lcm}(m,n)\mathbb{Z})$$

is such an isomorphism. To see that it is well-defined, observe that

$$(a + m\mathbb{Z}) - (b + n\mathbb{Z}) = (a - b) + \gcd(m,n)\mathbb{Z}$$

since

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}$$

which itself follows from the facts that

$$\gcd(m,n) = rm + sn \in m\mathbb{Z} + n\mathbb{Z}$$

and (by definition) $m\mathbb{Z} \subset \gcd(m,n)\mathbb{Z}$ and $n\mathbb{Z} \subset \gcd(m,n)\mathbb{Z}$. And, similarly

$$sn' \cdot m\mathbb{Z} + rm' \cdot n\mathbb{Z} = \mathrm{lcm}(m,n)\mathbb{Z}$$

so the second component of the map is also well-defined.

Now since these things are finite, it suffices to show that the kernel is trivial. That is, suppose $b = a + k\gcd(m,n)$ for some integer k, and consider

$$b \cdot rm' + a \cdot sn'$$

The latter is

$$(a + k\gcd(m,n))rm' + a \cdot sn' = a \cdot rm' + a \cdot sn' = a \bmod m$$

since $\gcd(m,n)m' = m$ and $rm' + sn' = 1$. Symmetrically, it is $b \bmod n$. Thus, if it is $0 \bmod \mathrm{lcm}(m,n)$, $a = 0 \bmod m$ and $b = 0 \bmod n$. This proves that the kernel is trivial, so the map is injective, and, because of finiteness, surjective as well.

[9.0.1] **Remark:** I leave you the fun of guessing where the $a - b$ expression (above) comes from.

[2.3] Show that every group of order $5 \cdot 13$ is cyclic.

Invoke the Sylow theorem: the number of 5-Sylow subgroups is 1 mod 5 and also divides the order $5 \cdot 13$, so must be 1 (since 13 is not 1 mod 5). Thus, the 5-Sylow subgroup is normal. Similarly, even more easily, the 13-Sylow subgroup is normal. The intersection of the two is trivial, by Lagrange. Thus, we have two normal subgroups with trivial intersection and the product of whose orders is the order of the whole group, and conclude that the whole group is isomorphic to the (direct) product of the two, namely $\mathbb{Z}/5 \oplus \mathbb{Z}/13$. Further, this is isomorphic to $\mathbb{Z}/65$.

[2.4] Show that every group of order $5 \cdot 7^2$ is abelian.

From the classification of groups of prime-squared order, we know that there are only two (isomorphism classes of) groups of order 7^2, $\mathbb{Z}/49$ and $\mathbb{Z}/7 \oplus \mathbb{Z}/7$. From the Sylow theorem, since the number of 7-Sylow subgroups is 1 mod 7 and also divides the group order, the 7-Sylow subgroup is normal. For the same reason the 5-Sylow subgroup is normal. The intersection of the two is trivial (Lagrange). Thus, again, we have two normal subgroups with trivial intersection the product of whose orders is the group order, so the group is the direct product. Since the factor groups are abelian, so is the whole.

[2.5] Exhibit a non-abelian group of order $3 \cdot 7$.

We can construct this as a semi-direct product, since there exists a non-trivial homomorphism of $\mathbb{Z}/3$ to $\mathrm{Aut}(\mathbb{Z}/7)$, since the latter automorphism group is isomorphic to $(\mathbb{Z}/7)^\times$, of order 6. Note that we are assured of the *existence* of a subgroup of order 3 of the latter, whether or not we demonstrate an explicit element.

[2.6] Exhibit a non-abelian group of order $5 \cdot 19^2$.

We can construct this as a semi-direct product, since there exists a non-trivial homomorphism of $\mathbb{Z}/5$ to $\mathrm{Aut}(\mathbb{Z}/19 \oplus \mathbb{Z}/19)$, since the latter automorphism group has order $(19^2 - 1)(19^2 - 19)$, which is divisible by 5. Note that we are assured of the *existence* of a subgroup of order 5 of the latter, whether or not we demonstrate an explicit element.

[2.7] Show that every group of order $3 \cdot 5 \cdot 17$ is cyclic.

Again, the usual divisibility trick from the Sylow theorem proves that the 17-group is normal. Further, since neither 3 nor 5 divides $17 - 1 = |\mathrm{Aut}(\mathbb{Z}/17)|$, the 17-group is *central*. But, since $3 \cdot 17 = 1 \bmod 5$, and $5 \cdot 17 = 1 \bmod 3$, we cannot immediately reach the same sort of conclusion about the 3-group and 5-group. But if *both* the 3-group and 5-group were *not* normal, then we'd have at least

$$1 + (17 - 1) + (5 - 1) \cdot 3 \cdot 17 + (3 - 1) \cdot 5 \cdot 17 = 391 > 3 \cdot 5 \cdot 17 = 255$$

elements in the group. So at least one of the two is normal. If the 5-group is normal, then the 3-group acts trivially on it by automorphisms, since 3 does not divide $5 - 1 = |\mathrm{Aut}(\mathbb{Z}/5)|$. Then we'd have a *central* subgroup of order $5 \cdot 17$ group, and the whole group is abelian, so is cyclic by the type of arguments given earlier. Or, if the 3-group is normal, then for the same reason it is is central, so we have a central (cyclic) group of order $3 \cdot 17$, and again the whole group is cyclic.

[2.8] Do there exist 4 primes p, q, r, s such that every group of order $pqrs$ is necessarily abelian?

We want to arrange that all of the p, q, r, s Sylow subgroups P, Q, R, S are normal. Then, because the primes are distinct, still

$$P \cap Q = \{e\}$$

$$P \cdot Q \cap R = \{e\}$$

$$P \cdot Q \cdot R \cap S = \{e\}$$

(and all other combinations) so these subgroups commute with each other. And then, as usual, the whole group is the direct product of these Sylow subgroups.

One way to arrange that all the Sylow subgroups are normal is that, mod p, none of q, r, s, qr, qs, rs, qrs is 1, and symmetrically for the other primes. Further, with none of q, r, s dividing $p-1$ the p-group is *central*. For example, after some trial and error, plausible $p < q < r < s$ has $p = 17$. Take $q, r, s \bmod 11 = 2, 3, 5$ respectively. Take $q = 13$, so $p = -2 \bmod 13$, and require $r, s = 2, 5 \bmod q$. Then $r = 3 \bmod 11$ and $r = 2 \bmod 13$ is $80 \bmod 143$, and 223 is the first prime in this class. With $s = 5 \bmod 223$, none of the 7 quantities is 1 mod r.. Then $s = 5 \bmod 11 \cdot 13 \cdot 223$ and the first prime of this form is

$$s = 5 + 6 \cdot 11 \cdot 13 \cdot 223 = 191339$$

By this point, we know that the p, q, and r-sylow groups are central, so the whole thing is cyclic.

Exercises

2.[9.0.1] Classify groups of order 7 or less, up to isomorphism.

2.[9.0.2] Find two different non-abelian groups of order 8.

2.[9.0.3] Classify groups of order 9 and 10.

2.[9.0.4] Classify groups of order 12.

2.[9.0.5] Classify groups of order 21.

2.[9.0.6] Classify groups of order 27.

2.[9.0.7] Classify groups of order 30.

2.[9.0.8] Classify groups of order 77.

2.[9.0.9] Let G be a group with just two subgroups, G and $\{e\}$. Prove that either $G = \{e\}$ or G is cyclic of prime order.

2.[9.0.10] Let N be a normal subgroup of a group G, and let H be a subgroup of G such that $G = H \cdot N$, that is, such that the collection of all products $h \cdot n$ with $h \in H$ and $n \in N$ is the whole group G. Show that $G/N \approx H/(H \cap N)$.

2.[9.0.11] (*Cayley's theorem*) Show that every finite group is isomorphic to a subgroup of a permutation group. (*Hint*: let G act on the *set* G by left multiplication.)

2.[9.0.12] Let G be a group in which $g^2 = 1$ for every $g \in G$. Show that G is abelian.

2.[9.0.13] Let H be a subgroup of index 2 in a finite group G. Show that H is normal.

2.[9.0.14] Let p be the smallest prime dividing the order of a finite group G. Let H be a subgroup of index p in G. Show that H is normal.

2.[9.0.15] Let H be a subgroup of finite index in a (not necessarily finite) group G. Show that there is a *normal* subgroup N of G such that $N \subset H$ and N is of finite index in G.

2.[9.0.16] Find the automorphism group $\mathrm{Aut}\mathbb{Z}/n$ of the additive group $\mathbb{Z}/n$.