-

Abstract Algebra

Paul Garrett

I covered this material in a two-semester graduate course in abstract algebra in 2004-05, rethinking the material from scratch, ignoring traditional prejudices.

I wrote proofs which are natural outcomes of the viewpoint. A viewpoint is good if taking it up means that there is less to remember. *Robustness*, as opposed to *fragility*, is a desirable feature of an argument. It is burdensome to be clever. Since it is non-trivial to arrive at a viewpoint that allows proofs to seem easy, such a viewpoint is revisionist. However, this is a *good* revisionism, as opposed to much worse, destructive revisionisms which are nevertheless popular, most notably the misguided impulse to logical perfection [sic]. Logical streamlining is not the same as optimizing for performance.

The worked examples are meant to be model solutions for many of the standard traditional exercises. I no longer believe that everyone is obliged to redo everything themselves. Hopefully it is possible to learn from others' efforts.

Paul Garrett
June, 2007, Minneapolis

Introduction

Abstract Algebra is not a conceptually well-defined body of material, but a conventional name that refers roughly to one of the several lists of things that mathematicians need to know to be competent, effective, and sensible. This material fits a two-semester beginning graduate course in abstract algebra. It is a *how-to* manual, not a monument to traditional icons. Rather than an encyclopedic reference, it tells a story, with plot-lines and character development propelling it forward.

The main novelty is that most of the standard exercises in abstract algebra are given here as *worked* examples. Some additional exercises are given, which are variations on the worked examples. The reader might contemplate the examples before reading the solutions, but this is not mandatory. The examples are given to *assist*, not necessarily *challenge*. The point is *not* whether or not the reader can do the problems on their own, since all of these are at least fifty years old, but, rather, whether the *viewpoint* is assimilated. In particular, it often happens that a logically correct solution is conceptually regressive, and should not be considered satisfactory.

I promote an efficient, abstract viewpoint whenever it is purposeful to abstract things, especially when letting go of appealing but irrelevant details is advantageous. Some things often not mentioned in an algebra course are included. Some naive set theory, developing ideas about ordinals, is occasionally useful, and the abstraction of this setting makes the set theory seem less farfetched or baffling than it might in a more elementary context. Equivalents of the Axiom of Choice are described. Quadratic reciprocity is useful in understanding quadratic and cyclotomic extensions of the rational numbers, and I give the proof by Gauss' sums. An economical proof of Dirichlet's theorem on primes in arithmetic progressions is included, with discussion of relevant complex analysis, since existence of primes satisfying linear congruence conditions comes up in practice. Other small enrichment topics are treated briefly at opportune moments in examples and exercises. Again, algebra is not a unified or linearly ordered body of knowledge, but only a rough naming convention for an ill-defined and highly variegated landscape of ideas. Further, as with all parts of the basic graduate mathematics curriculum, many important things are inevitably left out. For algebraic geometry or algebraic number theory, much more commutative algebra is useful than is presented here. Only vague hints of representation theory are detectable here.

Far more systematic emphasis is given to finite fields, cyclotomic polynomials (divisors of $x^n - 1$), and cyclotomic fields than is usual, and less emphasis is given to *abstract* Galois theory. Ironically, there are many more explicit Galois theory *examples* here than in sources that emphasize abstract Galois theory. After proving Lagrange's theorem and the Sylow theorem, the pure theory of finite groups is not especially emphasized. After all, the Sylow theorem is not interesting because it allows classification of groups of small order, but because its *proof* illustrates *group actions on sets*, a ubiquitous mechanism in mathematics. A strong and recurring theme is the characterization of objects by *(universal) mapping properties*, rather than by goofy constructions. Nevertheless, formal category theory does not appear. A greater emphasis is put on linear and multilinear algebra, while doing little with general commutative algebra apart from Gauss' lemma and Eisenstein's criterion, which are immediately useful.

Students need good role models for writing mathematics. This is a reason for the complete write-ups of solutions to many examples, since most traditional situations do *not* provide students with *any* models for solutions to the standard problems. This is bad. Even worse, lacking full solutions written by a practiced hand, inferior and regressive solutions may propagate. I do not always insist that students give solutions in the style I wish, but it is very desirable to provide beginners with good examples.

The reader is assumed to have *some* prior acquaintance with introductory abstract algebra and linear algebra, not to mention other standard courses that are considered preparatory for graduate school. This is not so much for specific information as for maturity.

Contents

1. The integers

1.1 *Unique factorization*

Let $\mathbb{Z}$ denote the integers. Say d **divides** m, equivalently, that m is a **multiple** of d, if there exists an integer q such that $m = qd$. Write $d|m$ if d divides m.

It is easy to prove, from the definition, that if $d|x$ and $d|y$ then $d|(ax + by)$ for any integers x, y, a, b: let $x = rd$ and $y = sd$, and

$$ax + by = a(rd) + b(sd) = d \cdot (ar + bs)$$

1.1.1 Theorem: Given an integer N and a non-zero integer m there are unique integers q and r, with $0 \leq r < |m|$ such that

$$N = q \cdot m + r$$

The integer r is the **reduction modulo** m of N.

Proof: Let S be the set of all non-negative integers expressible in the form $N - sm$ for some integer s. The set S is non-empty, so by well-ordering has a least element $r = N - qm$. Claim that $r < |m|$. If not, then still $r - |m| \geq 0$, and also

$$r - |m| = (N - qm) - |m| = N - (q \pm 1)m$$

(with the sign depending on the sign of m) is still in the set S, contradiction. For uniqueness, suppose that both $N = qm + r$ and $N = q'm + r'$. Subtract to find

$$r - r' = m \cdot (q' - q)$$

Thus, $r - r'$ is a multiple of m. But since $-|m| < r - r' < |m|$ we have $r = r'$. And then $q = q'$. ///

1.1.2 Remark: The conclusion of the theorem is that in $\mathbb{Z}$ one can divide and obtain a remainder *smaller* than the divisor. That is, $\mathbb{Z}$ is **Euclidean**.

As an example of nearly trivial things that can be proven about divisibility, we have:

A divisor d of n is **proper** if it is neither $\pm n$ nor ± 1. A positive integer p is **prime** if it has no proper divisors and if $p > 1$.

1.1.3 Proposition: A positive integer n is prime if and only if it is not divisible by any of the integers d with $1 < d \leq \sqrt{n}$.

Proof: Suppose that n has a proper factorization $n = d \cdot e$, where $d \leq e$. Then

$$d = \frac{n}{e} \leq \frac{n}{d}$$

gives $d^2 \leq n$, so $d \leq \sqrt{n}$. ///

1.1.4 Remark: The previous proposition suggests that to test an integer n for primality we attempt to divide n by all integers $d = 2, 3, \ldots$ in the range $d \leq \sqrt{n}$. If no such d divides n, then n is prime. This procedure is **trial division**.

Two integers are **relatively prime** or **coprime** or **mutually prime** if for every integer d if $d|m$ and $d|n$ then $d = \pm 1$.

An integer d is a **common divisor** of integers $n_1, \ldots, n_m$ if d divides each n_i. An integer N is a **common multiple** of integers $n_1, \ldots, n_m$ if N is a multiple of each. The following peculiar characterization of the greatest common divisor of two integers is fundamental.

1.1.5 Theorem: Let m, n be integers, not both zero. Among all *common* divisors of m, n there is a unique $d > 0$ such that for *every* other common divisor e of m, n we have $e|d$. This d is the *greatest common divisor* of m, n, denoted $\gcd(m, n)$. And

$$\gcd(mn) = \text{least positive integer of the form } xm + yn \text{ with } x, y \in \mathbb{Z}$$

Proof: Let $D = x_o m + y_o n$ be the least positive integer expressible in the form $xm + yn$. First, we show that any divisor d of both m and n divides D. Let $m = m'd$ and $n = n'd$ with $m', n' \in \mathbb{Z}$. Then

$$D = x_o m + y_o n = x_o(m'd) + y_o(n'd) = (x_o m' + y_o n') \cdot d$$

which presents D as a multiple of d.

On the other hand, let $m = qD + r$ with $0 \leq r < D$. Then

$$0 \leq r = m - qD = m - q(x_o m + y_o n) = (1 - qx_o) \cdot m + (-y_o) \cdot n$$

That is, r is expressible as $x'm + y'n$. Since $r < D$, and since D is the smallest positive integer so expressible, $r = 0$. Therefore, $D|m$, and similarly $D|n$. ///

Similarly:

1.1.6 Corollary: Let m, n be integers, not both zero. Among all *common* multiples of m, n there is a unique positive one N such that for *every* other common multiple M we have $N|M$. This multiple N is the *least common multiple* of m, n, denoted $\mathrm{lcm}(m, n)$. In particular,

$$\mathrm{lcm}(m, n) = \frac{mn}{\gcd(m, n)}$$

Proof: Let

$$L = \frac{mn}{\gcd(m,n)}$$

First we show that L is a multiple of m and n. Indeed, let

$$m = m' \cdot \gcd(m,n) \qquad n = n' \cdot \gcd(m,n)$$

Then

$$L = m \cdot n' = m' \cdot n$$

expresses L as an integer multiple of m and of n. On the other hand, let M be a multiple of both m and n. Let $\gcd(m,n) = am + bn$. Then

$$1 = a \cdot m' + b \cdot n'$$

Let $N = rm$ and $N = sn$ be expressions of N as integer multiples of m and n. Then

$$N = 1 \cdot N = (a \cdot m' + b \cdot n') \cdot N = a \cdot m' \cdot sn + b \cdot n' \cdot rm = (as + br) \cdot L$$

as claimed. ///

The innocent assertion and perhaps odd-seeming argument of the following are essential for what follows. Note that the key point is the peculiar characterization of the *gcd*, which itself comes from the Euclidean property of $\mathbb{Z}$.

1.1.7 Theorem: A prime p divides a product ab if and only if $p|a$ or $p|b$.

Proof: If $p|a$ we are done, so suppose p does not divide a. Since p is prime, and since $\gcd(p,a) \neq p$, it must be that $\gcd(p,a) = 1$. Let r, s be integers such that $1 = rp + sa$, and let $ab = kp$. Then

$$b = b \cdot 1 = b(rp + sa) = p \cdot (rb + sk)$$

so b is a multiple of p. ///

Granting the theorem, the proof of unique factorization is nearly an afterthought:

1.1.8 Corollary: *(Unique Factorization)* Every integer n can be written in an *essentially unique* way (up to reordering the factors) as $\pm$ a product of primes:

$$n = \pm\, p_1^{e_1}\, p_2^{e_2} \ldots p_m^{e_m}$$

with positive integer exponents and primes $p_1 < \ldots < p_m$.

Proof: For *existence,* suppose $n > 1$ is the least integer *not* having a factorization. Then n cannot be prime itself, or just '$n = n$' is a factorization. Therefore n has a proper factorization $n = xy$ with $x, y > 1$. Since the factorization is *proper*, both x and y are strictly smaller than n. Thus, x and y both can be factored. Putting together the two factorizations gives the factorization of n, contradicting the assumption that there exist integers lacking prime factorizations.

Now *uniqueness.* Suppose

$$q_1^{e_1} \ldots q_m^{e_m} = N = p_1^{f_1} \ldots p_n^{f_n}$$

where $q_1 < \ldots < q_m$ are primes, and $p_1 < \ldots < p_n$ are primes, and the exponents e_i and f_i are positive integers. Since q_1 divides the left-hand side of the equality, it divides the right-hand side. Therefore, q_1 must divide one of the factors on the right-hand side. So q_1 must divide some p_i. Since p_i is prime, it must be that $q_1 = p_i$.

If $i > 1$ then $p_1 < p_i$. And p_1 divides the left-hand side, so divides one of the q_j, so is some q_j, but then

$$p_1 = q_j \geq q_1 = p_i > p_1$$

which is impossible. Therefore, $q_1 = p_1$.

Without loss of generality, $e_1 \leq f_1$. Thus, by dividing through by $q_1^{e_1} = p_1^{e_1}$, we see that the corresponding exponents e_1 and f_1 must also be equal. Then do induction. ///

1.1.9 Example: The simplest meaningful (and standard) example of the failure of unique factorization into primes is in the collection of numbers

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

The relation

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$$

gives two different-looking factorizations of 6. We must verify that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are *primes* in R, in the sense that they cannot be further factored.

To prove this, we use *complex conjugation*, denoted by a bar over the quantity to be conjugated: for real numbers a and b,

$$\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}$$

For α, β in R,

$$\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$$

by direct computation. Introduce the **norm**

$$N(\alpha) = \alpha \cdot \overline{\alpha}$$

The multiplicative property

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

follows from the corresponding property of conjugation:

$$N(\alpha) \cdot N(\beta) = \alpha\overline{\alpha}\beta\overline{\beta} = (\alpha\beta) \cdot (\overline{\alpha}\,\overline{\beta})$$

$$= (\alpha\beta) \cdot (\overline{\alpha\beta}) = N(\alpha\beta)$$

Note that $0 \leq N(\alpha) \in \mathbb{Z}$ for α in R.

Now suppose $2 = \alpha\beta$ with α, β in R. Then

$$4 = N(2) = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

By unique factorization in $\mathbb{Z}$, $N(\alpha)$ and $N(\beta)$ must be $1, 4$, or $2, 2$, or $4, 1$. The middle case is impossible, since no norm can be 2. In the other two cases, one of α or β is ± 1, and the factorization is not *proper*. That is, 2 cannot be factored further in $\mathbb{Z}[\sqrt{-5}]$. Similarly, 3 cannot be factored further.

If $1 + \sqrt{-5} = \alpha\beta$ with α, β in R, then again

$$6 = N\left(1 + \sqrt{-5}\right) = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

Again, the integers $N(\alpha)$ and $N(\beta)$ must either be $1, 6$, $2, 3$, $3, 2$, or $6, 1$. Since the norm cannot be 2 or 3, the middle two cases are impossible. In the remaining two cases, one of α or β is ± 1, and the factorization is not *proper*. That is, $1 + \sqrt{-5}$ cannot be factored further in R. Neither can $1 - \sqrt{-5}$. Thus,

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{5}\right)$$

is a factorization of 6 in two different ways *into primes* in $\mathbb{Z}[\sqrt{-5}]$.

1.1.10 Example: The **Gaussian integers**

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

where $i^2 = -1$ do have a Euclidean property, and thus have unique factorization. Use the *integer-valued* norm

$$N(a + bi) = a^2 + b^2 = (a + bi) \cdot \overline{(a + bi)}$$

It is important that the notion of size be integer-valued and respect multiplication. We claim that, given $\alpha, \delta \in \mathbb{Z}[i]$ there is $q \in \mathbb{Z}[i]$ such that

$$N(\alpha - q \cdot \delta) < N(\delta)$$

Since N is *multiplicative* (see above), we can divide through by δ inside

$$\mathbb{Q}(i) = \{a + bi : a, b, \in \mathbb{Q}\}$$

(where $\mathbb{Q}$ is the rationals) to see that we are asking for $q \in \mathbb{Z}[i]$ such that

$$N(\frac{\alpha}{\delta} - q) < N(1) = 1$$

That is, given $\beta = \alpha/\delta$ in $\mathbb{Q}(i)$, we must be able to find $q \in \mathbb{Z}[i]$ such that

$$N(\beta - q) < 1$$

With $\beta = a + bi$ with $a, b \in \mathbb{Q}$, let

$$a = r + f_1 \qquad b = s + f_2$$

with $r, s \in \mathbb{Z}$ and f_1, f_2 rational numbers with

$$|f_i| \leq \frac{1}{2}$$

That this is possible is a special case of the fact that any *real* number is at distance at most $1/2$ from some integer. Then take

$$q = r + si$$

Then

$$\beta - q = (a + bi) - (r + si) = f_1 + if_2$$

and

$$N(\beta - q) = N(f_1 + if_2) = f_1^2 + f_2^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$

Thus, indeed $\mathbb{Z}[i]$ has the Euclidean property, and, by the same proof as above, has unique factorization.

1.2 *Irrationalities*

The usual proof that there is no square root of 2 in the rationals $\mathbb{Q}$ uses a little bit of unique factorization, in the notion that it is possible to put a fraction into lowest terms, that is, having relatively prime numerator and denominator.

That is, given a fraction a/b (with $b \neq 0$), letting $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$, one can and should show that $\gcd(a', b') = 1$. That is, $a'b/b'$ is **in lowest terms**. And

$$\frac{a'}{b'} = \frac{a}{b}$$

1.2.1 Example: Let p be a prime number. We claim that there is no $\sqrt{p}$ in the rationals $\mathbb{Q}$. Suppose, to the contrary, that $a/b = \sqrt{p}$. Without loss of generality, we can assume that $\gcd(a, b) = 1$. Then, squaring and multiplying out,

$$a^2 = pb^2$$

Thus, $p|a^2$. Since $p|cd$ implies $p|c$ or $p|d$, necessarily $p|a$. Let $a = pa'$. Then

$$(pa')^2 = pb^2$$

or

$$pa'^2 = b^2$$

Thus, $p|b$, contradicting the fact that $\gcd(a, b) = 1$. ///

The following example illustrates a possibility that will be subsumed later by *Eisenstein's criterion*, which is itself an application of *Newton polygons* attached to polynomials.

1.2.2 Example: Let p be a prime number. We claim that there is no rational solution to

$$x^5 + px + p = 0$$

Indeed, suppose that a/b were a rational solution, in lowest terms. Then substitute and multiply through by b^5 to obtain

$$a^5 + pab^4 + pb^5 = 0$$

From this, $p|a^5$, so, since p is prime, $p|a$. Let $a = pa'$. Then

$$(pa')^5 + p(pa')b^4 + pb^5 = 0$$

or

$$p^4a'^5 + p^2a'b^4 + b^5 = 0$$

From this, $p|b^5$, so $p|b$ since p is prime. This contradicts the lowest-terms hypothesis.

1.3 $\mathbb{Z}/m$, *the integers mod* m

Recall that a *relation* R on a set S is a subset of the cartesian product $S \times S$. Write

$$x \; R \; y$$

if the ordered pair (x, y) lies in the subset R of $S \times S$. An **equivalence relation** R on a set S is a relation satisfying
• **Reflexivity**: $x \; R \; x$ for all $x \in S$
• **Symmetry**: If $x \; R \; y$ then $y \; R \; x$
• **Transitivity**: If $x \; R \; y$ and $y \; R \; z$ then $x \; R \; z$

A common notation for an equivalence relation is

$$x \sim y$$

that is, with a tilde rather than R.

Let $\sim$ be an equivalence relation on a set S. For $x \in S$, the $\sim$ - **equivalence class** $\bar{x}$ containing x is the subset

$$\bar{x} = \{x' \in S : x' \sim x\}$$

The **set of equivalence classes** of $\sim$ on S is denoted by

$$S/\sim$$

(as a quotient). Every element $z \in S$ is contained in an equivalence class, namely the equivalence class $\bar{z}$ of all $s \in S$ so that $s \sim z$. Given an equivalence class A inside S, an x in the set S such that $\bar{x} = A$ is a **representative** for the equivalence class. That is, any element of the subset A is a representative.

A set $\mathcal{S}$ of non-empty subsets of a set S whose union is the whole S, and which are mutually disjoint, is a **partition** of S. One can readily check that the equivalence classes of an equivalence relation on a set S form a partition of S, and, conversely, any partition of S defines an equivalence relation by positing that $x \sim y$ if and only if they lie in the same set of the partition. ///

If two integers x, y differ by a multiple of a non-zero integer m, that is, if $m|(x-y)$, then x is **congruent to** y **modulo** m, written

$$x \equiv y \bmod m$$

Such a relation a **congruence** modulo m, and m is the **modulus**. When Gauss first used this notion 200 years ago, it was sufficiently novel that it deserved a special notation, but, now that the novelty has worn off, we will simply write

$$x = y \bmod m$$

and (unless we want special emphasis) simply say that x is **equal to** y modulo m.

1.3.1 Proposition: (For fixed modulus m) equality modulo m is an equivalence relation. ///

Compatibly with the general usage for equivalence relations, the **congruence class** (or **residue class** or **equivalence class**) of an integer x modulo m, denoted $\bar{x}$ (with only implicit reference to m) is the set of all integers equal to x mod m:

$$\bar{x} = \{y \in \mathbb{Z} : y = x \bmod m\}$$

The **integers mod** m, denoted $\mathbb{Z}/m$, is the collection of *congruence classes* of integers modulo m. For some $X \in \mathbb{Z}/m$, a choice of ordinary integer x so that $\bar{x} = X$ is a **representative** for the congruence class X.

1.3.2 Remark: A popular but unfortunate notation for $\mathbb{Z}/m$ is $\mathbb{Z}_m$. We will not use this notation. It is unfortunate because for primes p the notation $\mathbb{Z}_p$ is the *only* notation for the *p-adic integers*.

1.3.3 Remark: On many occasions, the bar is dropped, so that x-mod-m may be written simply as 'x'.

1.3.4 Remark: The traditionally popular collection of representatives for the equivalence classes modulo m, namely

$$\{\bar{0}, \bar{1}, \bar{2}, \dots \overline{m-2}, \overline{m-1}\}$$

is not the only possibility.

The benefit Gauss derived from the explicit notion of congruence was that congruences behave much like equalities, thus allowing us to benefit from our prior experience with equalities. Further, but not surprisingly with sufficient hindsight, congruences behave nicely with respect to the basic operations of addition, subtraction, and multiplication:

1.3.5 Proposition: Fix the modulus m. If $x = x' \bmod m$ and $y = y' \bmod m$, then

$$x + y = x' + y' \bmod m$$

$$xy = x'y' \bmod m$$

Proof: Since $m|(x'-x)$ there is an integer k such that $mk = x' - x$. Similarly, $y' = y + \ell m$ for some integer ℓ. Then

$$x' + y' = (x + mk) + (y + m\ell) = x + y + m \cdot (k + \ell)$$

Thus, $x' + y' = x + y \bmod m$. And

$$x' \cdot y' = (x + mk) \cdot (y + m\ell) = x \cdot y + xm\ell + mky + mk \cdot m\ell = x \cdot y + m \cdot (k + \ell + mk\ell)$$

Thus, $x'y' = xy \bmod m$. ///

As a corollary, congruences *inherit* many basic properties from ordinary arithmetic, simply because $x = y$ implies $x = y \bmod m$:
• *Distributivity:* $x(y + z) = xy + xz \bmod m$
• *Associativity of addition:* $(x + y) + z = x + (y + z) \bmod m$
• *Associativity of multiplication:* $(xy)z = x(yz) \bmod m$
• *Property of* 1*:* $1 \cdot x = x \cdot 1 = x \bmod m$
• *Property of* 0*:* $0 + x = x + 0 = x \bmod m$

In this context, a **multiplicative inverse mod** m to an integer a is an integer b (if it exists) such that

$$a \cdot b = 1 \bmod m$$

1.3.6 Proposition: An integer a has a multiplicative inverse modulo m if and only if $\gcd(a, m) = 1$.

Proof: If $\gcd(a, m) = 1$ then there are r, s such that $ra + sm = 1$, and

$$ra = 1 - sm = 1 \bmod m$$

The other implication is easy. ///

In particular, note that if a is invertible mod m then any a' in the residue class of a mod m is likewise invertible mod m, and any other element b' of the residue class of an inverse b is also an inverse. Thus, it makes sense to refer to elements of $\mathbb{Z}/m$ as being invertible or not. Notation:

$$(\mathbb{Z}/m)^\times = \{\bar{x} \in \mathbb{Z}/m : \gcd(x, m) = 1\}$$

This set $(\mathbb{Z}/m)^\times$ is the **multiplicative group** or **group of units** of $\mathbb{Z}/m$.

1.3.7 Remark: It is easy to verify that the set $(\mathbb{Z}/m)^\times$ is **closed under multiplication** in the sense that $a, b \in (\mathbb{Z}/m)^\times$ implies $ab \in (\mathbb{Z}/m)^\times$, and is **closed under inverses** in the sense that $a \in (\mathbb{Z}/m)^\times$ implies $a^{-1} \in (\mathbb{Z}/m)^\times$.

1.3.8 Remark: The superscript is not an 'x' but is a 'times', making a reference to multiplication and multiplicative inverses mod m. Some sources write $\mathbb{Z}/m^*$, but the latter notation is inferior, as it is too readily confused with other standard notation (for *duals*).

1.4 *Fermat's Little Theorem*

1.4.1 Theorem: Let p be a prime number. Then for any integer x

$$x^p = x \bmod p$$

Proof: First, by the Binomial Theorem

$$(x + y)^p = \sum_{0 \le i \le p} \binom{p}{i} x^i \, y^{p-i}$$

In particular, the binomial coefficients are *integers*. Now we can show that the prime p divides the binomial coefficients

$$\binom{p}{i} = \frac{p!}{i!\ (p-i)!}$$

with $1 \leq i \leq p-1$. We have

$$\binom{p}{i} \cdot i! \cdot (p-i)! = p!$$

(Since we know that the binomial coefficient is an integer, the following argument makes sense.) The prime p divides the right-hand side, so divides the left-hand side, but does not divide $i!$ nor $(p-i)!$ (for $0 < i < p$) since these two numbers are products of integers smaller than p and (hence) not divisible by p. Again using the fact that $p|ab$ implies $p|a$ or $p|b$, p does not divide $i! \cdot (p-i)!$, so p must divide the binomial coefficient.

Now we prove Fermat's Little Theorem for *positive* integers x by induction on x. Certainly $1^p = 1 \bmod p$. Now suppose that we know that

$$x^p = x \bmod p$$

Then

$$(x+1)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i\, 1^{p-i} = x^p + \sum_{0<i<p} \binom{p}{i} x^i + 1$$

All the coefficients in the sum in the middle of the last expression are divisible by p, so

$$(x+1)^p = x^p + 0 + 1 = x + 1 \bmod p$$

This proves the theorem for positive x. ///

1.4.2 Example: Let p be a prime with $p = 3 \bmod 4$. Suppose that a is a **square modulo** p, in the sense that there exists an *integer* b such that

$$b^2 = a \bmod p$$

Such b is a **square root modulo** p of a. Then we claim that $a^{(p+1)/4}$ is a square root of $a \bmod p$. Indeed,

$$\left(a^{(p+1)/4}\right)^2 = \left((b^2)^{(p+1)/4}\right)^2 = b^{p+1} = b^p \cdot b = b \cdot b \bmod p$$

by Fermat. Then this is $a \bmod p$. ///

1.4.3 Example: Somewhat more generally, let q be a prime, and let p be another prime with $p = 1 \bmod q$ but $p \neq 1 \bmod q^2$.

$$r = q^{-1} \bmod \frac{p-1}{q}$$

Then if a is a q^{th} power modulo p, a q^{th} root of $a \bmod p$ is given by the formula

$$q^{th} \text{ root of } a \bmod p = a^r \bmod p$$

If a is *not* a q^{th} power mod p then this formula does *not* product a q^{th} root.

1.4.4 Remark: For prime q and prime $p \neq 1 \bmod q$ there is an even simpler formula for q^{th} roots, namely let

$$r = q^{-1} \bmod p - 1$$

and then

$$q^{th} \text{ root of } a \bmod p = a^r \bmod p$$

Further, as can be seen from the even-easier proof of this formula, *everything* mod such p is a q^{th} power.

For a positive integer n, the **Euler phi-function** $\varphi(n)$ is the number of integers b so that $1 \le b \le n$ and $\gcd(b, n) = 1$. Note that

$$\varphi(n) = \text{cardinality of } (\mathbb{Z}/n)^\times$$

1.4.5 Theorem: *(Euler)* For x relatively prime to a positive integer n,

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

1.4.6 Remark: The special case that n is prime is Fermat's Little Theorem.

Proof: Let $G = (\mathbb{Z}/m)^\times$, for brevity. First note that the product

$$P = \prod_{g \in G} g = \text{product of all elements of } G$$

is again in G. Thus, P has a multiplicative inverse mod n, although we do not try to identify it. Let x be an element of G. Then we claim that the map $f : G \longrightarrow G$ defined by

$$f(g) = xg$$

is a bijection of G to itself. First, check that f really maps G to itself: for x and g both invertible mod n,

$$(xg)(g^{-1}x^{-1}) = 1 \bmod n$$

Next, injectivity: if $f(g) = f(h)$, then $xg = xh \bmod n$. Multiply this equality by $x^{-1} \bmod n$ to obtain $g = h \bmod n$. Last, surjectivity: given $g \in G$, note that $f(x^{-1}g) = g$.

Then

$$P = \prod_{g \in G} g = \prod_{g \in G} f(g)$$

since the map f merely permutes the elements of G. Then

$$P = \prod_{g \in G} f(g) = \prod_{g \in G} xg = x^{\varphi(n)} \prod_{g \in G} g = x^{\varphi(n)} \cdot P$$

Since P is invertible mod n, multiply through by $P^{-1} \bmod n$ to obtain

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

This proves Euler's Theorem. ///

1.4.7 Remark: This proof of Euler's theorem, while subsuming Fermat's Little Theorem as a special case, strangely uses fewer specifics. There is no mention of binomial coefficients, for example.

1.4.8 Remark: The argument above is a prototype example for the basic Lagrange's Theorem in basic group theory.

1.5 Sun-Ze's theorem

The result of this section is sometimes known as the **Chinese Remainder Theorem**. Indeed, the earliest results (including and following Sun Ze's) were obtained in China, but such sloppy attribution is not good. Sun Ze's result was obtained before 850, and the statement below was obtained by Chin Chiu Shao about 1250. Such results, with virtually the same proofs, apply much more generally.

1.5.1 Theorem: *(Sun-Ze)* Let m and n be relatively prime positive integers. Let r and s be integers such that

$$rm + sn = 1$$

Then the function

$$f : \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$$

defined by

$$f(x, y) = y \cdot rm + x \cdot sn$$

is a bijection. The inverse map

$$f^{-1} : \mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$$

is

$$f^{-1}(z) = (x\text{-mod-}m, y\text{-mod-}n)$$

Proof: First, the peculiar characterization of $\gcd(m, n)$ as the smallest positive integer expressible in the form $rm + sn$ assures (since here $\gcd(m, n) = 1$) that integers r and s exist such that $rm + sn = 1$. Second, the function f is well-defined, that is, if $x' = x + am$ and $y' = y + bn$ for integers a and b, then still

$$f(x', y') = f(x, y)$$

Indeed,

$$f(x', y') = y'rm + x'sn = (y + an)rm + (x + am)sn$$
$$= yrm + xsn + mn(ar + bs) = f(x, y) \bmod mn$$

proving the well-definedness.

To prove surjectivity of f, for any integer z, let $x = z$ and $y = z$. Then

$$f(x, y) = zrm + zsn = z(rm + sn) = z \cdot 1 \bmod mn$$

(To prove injectivity, we *could* use the fact that $\mathbb{Z}/m \times \mathbb{Z}/n$ and $\mathbb{Z}/mn$ are finite sets of the same size, so a surjective function is necessarily injective, but a more direct argument is more instructive.) Suppose

$$f(x', y') = f(x, y)$$

Then modulo m the yrm and $y'rm$ are 0, so

$$xsn = x'sn \bmod m$$

From $rm + sn = 1 \bmod mn$ we obtain $sn = 1 \bmod m$, so

$$x = x' \bmod m$$

Symmetrically,

$$y = y' \bmod n$$

giving injectivity.

Finally, by the same reasoning,

$$f(x,y) = yrm + xsn = y \cdot 0 + x \cdot 1 \bmod m = x \bmod m$$

and similarly

$$f(x,y) = yrm + xsn = y \cdot 1 + x \cdot 0 \bmod n = y \bmod n$$

This completes the argument. ///

1.5.2 Remark: The above result is the simplest prototype for a very general result.

1.6 *Worked examples*

1.6.1 Example: Let D be an integer that is not the square of an integer. Prove that there is no $\sqrt{D}$ in $\mathbb{Q}$.

Suppose that a, b were integers ($b \neq 0$) such that $(a/b)^2 = D$. The fact/principle we intend to invoke here is that fractions can be put in *lowest terms*, in the sense that the numerator and denominator have greatest common divisor 1. This follows from *existence* of the *gcd*, and from the fact that, if $\gcd(a,b) > 1$, then let $c = a/\gcd(a,b)$ and $d = b/\gcd(a,b)$ and we have $c/d = a/b$. Thus, still $c^2/d^2 = D$. One way to proceed is to prove that c^2/d^2 is still in lowest terms, and thus cannot be an integer unless $d = \pm 1$. Indeed, if $\gcd(c^2, d^2) > 1$, this *gcd* would have a prime factor p. Then $p|c^2$ implies $p|c$, and $p|d^2$ implies $p|d$, by the critical proven property of primes. Thus, $\gcd(c,d) > 1$, contradiction.

1.6.2 Example: Let p be prime, $n > 1$ an integer. Show (directly) that the equation $x^n - px + p = 0$ has no rational root (where $n > 1$).

Suppose there were a rational root a/b, without loss of generality in lowest terms. Then, substituting and multiplying through by b^n, one has

$$a^n - pb^{n-1}a + pb^n = 0$$

Then $p|a^n$, so $p|a$ by the property of primes. But then p^2 divides the first two terms, so must divide pb^n, so $p|b^n$. But then $p|b$, by the property of primes, contradicting the lowest-common-terms hypothesis.

1.6.3 Example: Let p be prime, b an integer not divisible by p. Show (directly) that the equation $x^p - x + b = 0$ has no rational root.

Suppose there were a rational root c/d, without loss of generality in lowest terms. Then, substituting and multiplying through by d^p, one has

$$c^p - d^{p-1}c + bd^p = 0$$

If $d \neq \pm 1$, then some prime q divides d. From the equation, $q|c^p$, and then $q|c$, contradiction to the lowest-terms hypothesis. So $d = 1$, and the equation is

$$c^p - c + b = 0$$

By Fermat's Little Theorem, $p|c^p - c$, so $p|b$, contradiction.

1.6.4 Example: Let r be a positive integer, and p a prime such that $\gcd(r, p-1) = 1$. Show that every b in $\mathbb{Z}/p$ has a unique r^{th} root c, given by the formula

$$c = b^s \bmod p$$

where $rs = 1 \bmod (p-1)$. [*Corollary of Fermat's Little Theorem.*]

1.6.5 Example: Show that $R = \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean.

First, we consider $R = \mathbb{Z}[\sqrt{-D}]$ for $D = 1, 2, \ldots$. Let $\omega = \sqrt{-D}$. To prove Euclidean-ness, note that the Euclidean condition that, given $\alpha \in \mathbb{Z}[\omega]$ and non-zero $\delta \in \mathbb{Z}[\omega]$, there exists $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q \cdot \delta| < |\delta|$$

is equivalent to

$$|\alpha/\delta - q| < |1| = 1$$

Thus, it suffices to show that, given a complex number α, there is $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q| < 1$$

Every complex number α can be written as $x + y\omega$ with real x and y. The simplest approach to analysis of this condition is the following. Let m, n be integers such that $|x - m| \leq 1/2$ and $|y - n| \leq 1/2$. Let $q = m + n\omega$. Then $\alpha - q$ is of the form $r + s\omega$ with $|r| \leq 1/2$ and $|s| \leq 1/2$. And, then,

$$|\alpha - q|^2 = r^2 + Ds^2 \leq \frac{1}{4} + \frac{D}{4} = \frac{1+D}{4}$$

For this to be strictly less than 1, it suffices that $1 + D < 4$, or $D < 3$. This leaves us with $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$.

In the second case, consider $Z[\omega]$ where $\omega = (1 + \sqrt{-D})/2$ and $D = 3 \bmod 4$. (The latter condition assures that $\mathbb{Z}[x]$ works the way we hope, namely that everything in it is expressible as $a + b\omega$ with $a, b \in \mathbb{Z}$.) For D=3 (the Eisenstein integers) the previous approach still works, but fails for $D = 7$ and for $D = 11$. Slightly more cleverly, realize that first, given complex α, integer n can be chosen such that

$$-\sqrt{D}/4 \leq \text{imaginary part}(\alpha - n\omega) \leq +\sqrt{D}/4$$

since the imaginary part of ω is $\sqrt{D}/2$. *Then* choose integer m such that

$$-1/2 \leq \text{ real part}(\alpha - n\omega - m) \leq 1/2$$

Then take $q = m + n\omega$. We have chosen q such that $\alpha - q$ is in the *rectangular* box of complex numbers $r + s\sqrt{-7}$ with

$$|r| \leq 1/2 \quad \text{and} \quad |s| \leq 1/4$$

Yes, 1/4, not 1/2. Thus, the size of $\alpha - q$ is at most

$$1/4 + D/16$$

The condition that this be strictly less than 1 is that $4 + D < 16$, or $D < 12$ (and $D = 1 \bmod 4$). This gives $D = 3, 7, 11$.

1.6.6 Example: Let $f : X \longrightarrow Y$ be a function from a set X to a set Y. Show that f has a left inverse if and only if it is injective. Show that f has a right inverse if and only if it is surjective. (Note where, if anywhere, the Axiom of Choice is needed.)

1.6.7 Example: Let $h : A \longrightarrow B$, $g : B \longrightarrow C$, $f : C \longrightarrow D$. Prove the associativity

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

Two functions are equal if and only if their values (for the same inputs) are the same. Thus, it suffices to evaluate the two sides at $a \in A$, using the definition of composite:

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

1.6.8 Example: Show that a set is infinite if and only if there is an injection of it to a proper subset of itself. Do not set this up so as to trivialize the question.

The other definition of *finite* we'll take is that a set S is finite if there is a surjection to it from one of the sets

$$\{\},\ \{1\},\ \{1,2\},\ \{1,2,3\},\ \dots$$

And a set is *infinite* if it has no such surjection.

We find a denumerable subset of an infinite set S, as follows. For infinite S, since S is not empty (or there'd be a surjection to it from $\{\}$), there is an element s_1. Define

$$f_1 : \{1\} \longrightarrow S$$

by $f(1) = s_1$. This cannot be surjective, so there is $s_2 \neq s_1$. Define

$$f_2 : \{1,2\} \longrightarrow S$$

by $f(1) = s_1$, $f(2) = s_2$. By induction, for each natural number n we obtain an injection $f_n : \{1,\dots\} \longrightarrow S$, and distinct elements $s_1, 2_2, \dots$. Let S' be the complement to $\{s_1, s_2, \dots\}$ in S. Then define $F : S \longrightarrow S$ by

$$F(s_i) = s_{i+1} \quad F(s') = s' \text{ (for } s' \in S')$$

This is an injection to the proper subset $S - \{s_1\}$.

On the other hand, we claim that no set $\{1,\dots,n\}$ admits an injection to a proper subset of itself. If there were such, by Well-Ordering there would be a least n such that this could happen. Let f be an injection of $S = \{1,\dots,n\}$ to a proper subset of itself.

By hypothesis, f restricted to $S' = \{1,2,\dots,n-1\}$ does *not* map S' to a proper subset of itself. The restriction of an injective function is still injective. Thus, either $f(i) = n$ for some $1 \leq i < n$, or $f(S')$ is the *whole* set S'. In the former case, let j be the least element not in the image $f(S)$. (Since $f(i) = n$, $j \neq n$, but this doesn't matter.) Replace f by $\pi \circ f$ where π is the permutation of $\{1,\dots,n\}$ that interchanges j and n and leaves everything else fixed. Since permutations are bijections, this $\pi \circ f$ is still an injection of S to a proper subset. Thus, we have reduced to the second case, that $f(S') = S'$. By injectivity, $f(n)$ can't be in S', but then $f(n) = n$, and the image $f(S)$ is not a proper subset of S after all, contradiction. ///

In a similar vein, one can *prove* the Pigeon-Hole Principle, namely, that for $m < n$ a function

$$f : \{1,\dots,n\} \longrightarrow \{1,\dots,m\}$$

cannot be injective. Suppose this is false. Let n be the smallest such that there is $m < n$ with an injective map as above. The restriction of an injective map is still injective, so f on $\{1,\dots,n-1\}$ is still injective. By the minimality of n, it must be that $n - 1 = m$, and that f restricted to $\{1,\dots,m\}$ is a bijection of that set to itself. But then there is no possibility for $f(n)$ in $\{1,\dots,m\}$ without violating the injectivity. Contradiction. Thus, there is no such injection to a smaller set.

Exercises

1.1 Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ be a polynomial with integer coefficients a_i. Show that if $f(x) = 0$ has a root in $\mathbb{Q}$, then this root is an integer dividing a_0.

1.2 Show that $x^2 - y^2 = 102$ has no solutions in integers

1.3 Show that $x^3 - y^3 = 3$ has no solutions in integers.

1.4 Show that $x^3 + y^3 - z^3 = 4$ has no solutions in integers.

1.5 Show that $x^2 + 3y^2 + 6z^3 - 9w^5 = 2$ has no solutions in integers.

1.6 The defining property of *ordered pair* (a, b) is that $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$. Show that the set-theoretic construction $(a, b) = \{\{a\}, \{a, b\}\}$ succeeds in making an object that behaves as an ordered pair is intended. (*Hint:* Beware: if $x = y$, then $\{x, y\} = \{x\}$.)

1.7 Let p be a prime, and q a positive integer power of p. Show that p divides the binomial coefficients $\binom{q}{i} = q!/i!(q-i)!$ for $0 < i < q$.

1.8 Show that the greatest common divisor of non-zero integers x, y, z is the smallest positive integer expressible as $ax + by + cz$ for integers a, b, c.

1.9 Let m, n be relatively prime integers. Without using factorizations, prove that $m|N$ and $n|N$ implies $mn|N$.

1.10 (*A warm-up to Hensel's lemma*) Let $p > 2$ be a prime. Suppose that b is an integer not divisible by p such that there is a solution y to the equation $y^2 = b \bmod p$. Show (by induction on n) that for $n \geq 1$ there is a unique $x \bmod p^n$ such that $x = b \bmod p$ and

$$x^p = b \bmod p^n$$

1.11 (*Another warm-up to Hensel's lemma*) Let $p > 2$ be a prime. Let y be an integer such that $y \equiv 1 \bmod p$. Show (by induction on n) that for $n \geq 1$ there is a unique $x \bmod p^n$ so that

$$x^p = y \bmod p^n$$

1.12 Let φ be Euler's phi-function, equal to the number of integers ℓ such that $1 \leq \ell < n$ with ℓ relatively prime to n. Show that for a positive integer n

$$n \;=\; \sum_{d|n,\ d>0} \varphi(d)$$

2. Groups I

2.1 *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

[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

as *addition*. And when the operation is written as addition, the identity is often written as 0 instead of e.

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,

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

---

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. ///

2.1.1 Remark: These uniqueness properties justify speaking of *the* inverse and *the* identity.

2.2 *Subgroups*

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**.

2.2.1 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.

2.2.2 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]

2.2.3 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, $n|j - i$. ///

2.2.4 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:

2.2.5 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:

2.2.6 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. ///

2.3 *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:

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

2.3.1 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.

2.3.2 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*.

2.3.3 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.

2.4 *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

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

2.4.1 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. ///

2.4.2 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.

2.4.3 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 $x^r = y$.

2.4.4 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 $r \bmod n$. 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 $r/d \bmod n/d$, 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. ///

2.5 *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

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

2.5.1 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.

2.5.2 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

2.5.3 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

2.5.4 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. ///

2.6 *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**.

2.6.1 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

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

2.6.2 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).

2.6.3 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*.

2.6.4 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]

2.6.5 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,

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

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 $h \in gG_s$. ///

2.6.6 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

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

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.

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

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

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*:

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

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

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

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

2.6.8 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).

2.7 *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.

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

2.7.2 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

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

- 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:

2.7.3 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

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

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

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,

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

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

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

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

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

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

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

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. ///

2.7.4 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.

2.7.5 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.

2.8 *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]

$$G \oplus H$$

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

2.8.1 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 inB 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. ///

2.8.2 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. ///

2.8.3 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. ///

2.8.4 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.

2.8.5 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]

---

[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.

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

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

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:

2.8.6 Proposition:

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

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

$$f_z(x) = zx$$

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,

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

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

[24] This should be expected.

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.

2.8.7 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. ///

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

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

[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.

[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.

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 $k \bmod p$. 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 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:

2.8.8 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

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

[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

[33] Lagrange

[34] Lagrange

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

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]

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

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

[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.

[38] Using Euler's totient function φ.

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,

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

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.

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

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

[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.

[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 $ab = ba$.