

## SOME NOTES ON (MOSTLY FINITE) GROUPS

Throughout,  $G$  is a group. If  $H$  is a subgroup of  $G$ , we write  $H \leq G$ .

### COSETS; LAGRANGE'S THEOREM

**Definition.** Let  $H \leq G$ . Then for any  $x, y \in G$ ,  $x \equiv y \pmod{H}$  if and only if  $x^{-1}y \in H$ .

One should really write  $x \equiv_{\text{left}} y$ . There is a similarly defined relation,  $x \equiv_{\text{right}} y \pmod{H}$  if and only if  $xy^{-1} \in H$ .

**Lemma.** Let  $H \leq G$ . Then  $\equiv \pmod{H}$  is reflexive, symmetric and transitive, i.e., it is an equivalence relation. (The same holds for  $\equiv_{\text{right}} \pmod{H}$ ).

Consequently, as for any equivalence relation, if we define  $[x] := \{y \in G \mid y \equiv x \pmod{H}\}$ , for each  $x \in G$ , then for any  $g, h \in G$ , either  $[g] = [h]$  or  $[g] \cap [h] = \emptyset$ .

For any  $x, y \in G$ ,  $x^{-1}y$  is the unique element such that  $y = x(x^{-1}y)$ . Therefore  $x \equiv y \pmod{H}$  if and only if  $y = xh$  for some  $h \in H$ . Therefore for any  $x \in G$ ,

$$[x] = xH, \text{ where we define } xH := \{xh \mid h \in H\}$$

The various sets  $xH$ , as  $x$  varies over  $G$ , are called the **left cosets of  $H$  in  $G$** . The set of all such left cosets is written  $G/H := \{xH \mid x \in G\}$ . The number of left cosets is written  $|G : H| := |G/H|$ , and is called the **index of  $G$  in  $H$** .

As observed above, for all  $x, y \in G$ , either  $xH = yH$  or  $xH \cap yH = \emptyset$ . Notice that  $x = xe \in xH$  for any  $x \in G$ . Thus we can also say that for all  $x, y \in G$ ,

$$x \in yH \iff xH = yH \iff xH \cap yH \neq \emptyset.$$

**WARNING:**  $G/H$  can not always be made into a group. Only if  $H$  is a “normal” subgroup (see below) can a “quotient group” structure be put on  $G/H$ .

**Lagrange's Theorem.** Let  $G$  be a finite group and  $H \leq G$ . Then  $|G| = |H| \cdot |G : H|$ .

**Corollary.** If  $G$  is a finite group and  $H \leq G$ , then both  $|H|$  and  $|G : H|$  divide  $|G|$ .

**Corollary (Groups of Prime Order).** If  $G$  is a group and  $|G| = p$  is a prime, then  $G$  has no subgroups other than itself and  $\{e\}$ , and  $G \cong (\mathbb{Z}_p, +)$ .

**Corollary (Orders of Elements).** If  $G$  is a finite group and  $g \in G$ , then the order  $|g|$  of  $g$  divides  $|G|$ .

### PARTIAL CONVERSES TO LAGRANGE'S THEOREM

There is no converse to Lagrange's Theorem. That is, it is not true in general that if  $|G| = n$  and  $m|n$ , then  $G$  must have a subgroup of order  $m$ . However, under some extra hypotheses, this may be true.

An important partial converse to Lagrange's Theorem, which we are not covering, is Sylow's Theorem, which asserts among other things that if  $m$  is a power of a prime, and  $m \mid |G|$ , then  $G$  must have a subgroup of order  $m$ .

Here is a baby case of Sylow's Theorem, sometimes called Cayley's Theorem (but beware the name; there are many “Cayley's Theorem”s).

**Theorem (Subgroups of Prime Order Exist).** Let  $G$  be a finite group and let  $p$  be a prime such that  $p$  divides  $|G|$ . Then  $G$  has an element  $x$  of order  $p$  (and  $\langle x \rangle$  is then a subgroup of  $G$  of order  $p$ ).

Proof (class, 11/30): Consider the following set of ordered  $p$ -tuples of elements of  $G$ :

$$S := \{(x_1, x_2, \dots, x_p) \mid x_i \in G \text{ for } i = 1, 2, \dots, p, \text{ and } x_1 x_2 \cdots x_p = e\}.$$

Notice that

$$x_1 x_2 \cdots x_p = e \iff x_p = (x_1 x_2 \cdots x_{p-1})^{-1} \iff x_p x_1 x_2 \cdots x_{p-1}.$$

The first equivalence implies that  $|S| = |G|^{p-1}$ , since for any  $x_1, \dots, x_{p-1} \in G$  there is a unique  $x_p$  completing  $x_1, \dots, x_{p-1}$  to a  $p$ -tuple in  $S$ . Since  $p$  divides  $|G|$ ,

$$|S| \equiv 0 \pmod{p}.$$

The second equivalence above, applied repeatedly, implies that

For any  $(x_1, x_2, \dots, x_p) \in S$ , the cyclic permutation  $(x_p, x_1, x_2, \dots, x_{p-1})$  is also in  $S$ .

To see this use the fact that  $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$ . Or just as good, multiply the equation  $x_1 x_2 \cdots x_p = e$  on the left by  $x_p$  and on the right by  $x_p^{-1}$ ; the new right side is  $x_p x_p^{-1} = e$ .

Any  $(x_1, x_2, \dots, x_p) \in S$  has  $p$  cyclic permutations in  $S$  (some of them may coincide), namely

$$(x_1, x_2, \dots, x_p), (x_2, x_3, \dots, x_p, x_{p+1}), (x_3, x_4, \dots, x_p, x_{p+1}, x_{p+2}), \dots, (x_p, x_{p+1}, \dots, x_{2p-1}). \quad (1)$$

Here subscripts are to be read “modulo  $p$ ”, so that  $x_{p+1}$  means  $x_1$ ,  $x_{2p-1}$  means  $x_{p-1}$ , etc.

Let  $E = \{(x_1, x_2, \dots, x_p) \in S \mid x_1 = x_2 = \cdots = x_p\}$  and let  $T = S - E$ . Take any  $(x_1, x_2, \dots, x_p) \in T$ ; we claim that all  $p$  of the cyclic permutations (see (1)) are different. For otherwise

$$(x_1, x_2, \dots, x_p) = (x_{d+1}, x_{d+2}, \dots, x_{d+p}) \text{ for some } d, 1 \leq d < p.$$

Therefore  $x_i = x_{d+i}$  for all  $i = 1, \dots, p$  (and therefore for all integers  $i$ , since we are reading subscripts mod  $p$ ). Therefore  $x_1 = x_{d+1} = x_{2d+1} = \cdots = x_{jd+1}$  for all integers  $j$ . SINCE  $p$  IS PRIME, and  $d \not\equiv 0 \pmod{p}$ , every congruence class modulo  $p$  contains one of the integers  $jd + 1$  (as  $j$  varies). Therefore  $x_1 = x_2 = \cdots = x_p$  so  $(x_1, x_2, \dots, x_p) \in E$ , contradiction.

Consequently  $|T| \equiv 0 \pmod{p}$ . But  $|S| = |T| + |E|$  and  $|S| \equiv 0 \pmod{p}$ . Therefore  $|E| \equiv 0 \pmod{p}$ . In particular  $|E| \neq 1$ . Also  $(e, e, \dots, e) \in E$  so there exists  $(x, x, \dots, x) \in E$  such that  $x \neq e$ . Then  $x^p = 1$  so  $x$  has order  $p$ .

## GROUPS OF SMALL ORDER

For a given integer  $m \geq 1$  let  $N(m)$  be the number of groups of order  $m$ , up to isomorphism. We check the following table:

$m$	2	3	4	5	6
$N(m)$	1	1	2	1	2
Groups	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_5$	$\mathbb{Z}_6, D_3$

By the Groups of Prime Order corollary to Lagrange's Theorem,  $\mathbb{Z}_m$  is the only group of order  $m = 2, 3, 5$ .

Suppose that  $|G| = 4$  but  $G \not\cong \mathbb{Z}_4$ . Then  $G$  has no element of order 4. Write  $G = \{e, a, b, c\}$ . For any  $g \in G$ ,  $|g|$  divides 4 by the Orders of Elements corollary. So  $a, b, c$  have order 2:  $a^2 = b^2 = c^2 = e$ . The product  $ab$  cannot be  $e$  since  $a^2 = e$  and  $a \neq b$ . Also  $ab \neq a$  since  $b \neq e$ , and  $ab \neq b$  since  $a \neq e$ . The only alternative is

$ab = c$ . Similarly the product of any two (different) elements of  $\{a, b, c\}$ , in either order, is the third element. Therefore if  $G$  and  $G'$  are any two noncyclic groups of order 4, any bijection from  $G \rightarrow G'$  taking  $e$  to  $e$  is an isomorphism. So there is one noncyclic group of order 4 up to isomorphism. One such group is  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , so the table is correct for  $m = 4$ .

Suppose that  $|G| = 6$  but  $G \not\cong \mathbb{Z}_6$ . Then by Orders of Elements corollary, the elements of  $G$  have order 1, 2 or 3. Moreover by the Subgroups of Prime Order Exist theorem,  $G$  has an element  $g$  of order 3 and an element  $t$  of order 2. Then  $g \neq g^{-1}$ , both of order 3. The subgroup  $H = \langle g \rangle \cong \mathbb{Z}_3$  consists of  $e, g, g^{-1}$ , and  $|G : H| = 2$  by Lagrange. Now  $t \notin H$ , so

$$G = H \cup tH = \{e, g, g^{-1}, t, tg, tg^{-1}\}, \quad g^3 = t^2 = e. \quad (2)$$

If  $tg$  has order 3, then  $(tg)^{-1}$  can't equal  $tg, g^{\pm 1}$ , or  $t$ , so  $(tg)^{-1} = tg^{-1}$ . Therefore  $g^{-1}t = (tg)^{-1} = tg^{-1}$ , so  $g^{-1}$  and  $t$  commute. But then  $(g^{-1}t)^3 = g^3t^3 = t \neq e$ , contradicting the fact that  $g^{-1}t$  has order 3.

Therefore  $tg$  has order 2. Then,  $tgtg = e$ , so

$$gt = tg^{-1} \text{ and then } g^2t = ggt = gtg^{-1} = tg^{-1}g^{-1} = tg^{-2} \quad (3)$$

Claim: (2) and (3) determine the multiplication table for  $G$ . Every element of  $G$  has the form  $g^i$  or  $tg^i$  for some  $0 \leq i \leq 2$ . The possible products are as follows (exponents of  $g$  are to be read modulo 3):

$$g^i g^j = g^{i+j}, \quad (tg^i)g^j = tg^{i+j}, \quad g^i tg^j = tg^{-i}g^j = tg^{j-i}, \quad tg^i tg^j = t^2 g^{j-i} = g^{j-i}. \quad (4)$$

Any other noncyclic group  $G'$  of order 6 similarly has elements which can be labelled  $g', t'$ , and which satisfy the analogues of (2), (3), (4). The bijection  $G \rightarrow G'$  taking  $e$  to  $e, g$  to  $g', t$  to  $t', tg$  to  $t'g'$ , etc., is then an isomorphism.

Therefore there is at most one noncyclic group of order 6, up to isomorphism. One such group is  $D_3$ , the symmetry group of an equilateral triangle.

The table is therefore correct for  $m = 6$ .

(Remarks: The argument of case 6 can be generalized to show that  $N(2p) = 2$  for any odd prime  $p$ , the two groups of order  $2p$  being  $Z_{2p}$  and  $D_p$ . There are 5 groups of order 8:  $Z_2 \times Z_2 \times Z_2, Z_2 \times Z_4, Z_8, D_8$ , and  $Q_8 = \{\pm e, \pm i, \pm j, \pm k\}$ . In  $Q_8$  the multiplication is given by  $(-e)^2 = e, i^2 = j^2 = k^2 = -e, ij = -ji = k, jk = -kj = i, ki = -ik = j$ .)  $Q_8$  is a subgroup of  $U(\mathbf{H})$ .)

## HOMOMORPHISMS, QUOTIENT GROUPS, NORMAL SUBGROUPS

Element-by-element analysis of groups is quite inefficient as soon as the group order gets significantly into double figures, and certainly for group orders in the thousands, say. An "architectural" approach to group structure is usually better; by Lagrange's theorem, the orders of subgroups are highly restricted. Homomorphisms provide a way to decompose groups into a normal subgroup and a quotient group.

**Definition.** If  $G$  and  $H$  are groups, a (group) homomorphism from  $G$  to  $H$  is a function  $\phi : G \rightarrow H$  such that  $\phi(xy) = \phi(x)\phi(y)$  for all  $x, y \in G$ . Moreover the kernel of  $\phi$  is defined by

$$\ker \phi = \{g \in G \mid \phi(g) = e\}.$$

**Proposition.** The following assertions hold.

- If  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow K$  are group homomorphisms, then so is the composite  $\psi \circ \phi : G \rightarrow K$ .
- If  $\phi : G \rightarrow H$  is a group homomorphism, then  $\phi(e) = e$  and  $\phi(g^n) = (\phi(g))^n$  for all  $g \in G$  and  $n \in \mathbb{Z}$ .
- If  $\phi : G \rightarrow H$  is a group homomorphism and  $g \in G$ , then  $|\phi(g)|$  divides  $|g|$  in the sense that if  $|g| < \infty$ , then  $|\phi(g)| < \infty$  and  $|\phi(g)| \mid |g|$ .

(d)  $\text{im } \phi \leq H$ . Indeed for all  $M \leq G$ ,  $\phi(M) = \{\phi(x) \mid x \in M\} \leq H$ .

(e)  $\ker \phi \leq G$ .

(f) Let  $K = \ker \phi$ . Then for any  $x, y \in G$ ,

$$x \equiv_{\text{left}} y \pmod{K} \iff \phi(x) = \phi(y) \iff x \equiv_{\text{right}} y \pmod{K}.$$

Furthermore,  $Kx = xK$  for all  $x \in G$ .

**Definition.** A subgroup  $K$  of a group  $G$  is called a **normal** subgroup of  $G$  (notation:  $K \triangleleft G$ ) if and only if  $Kx = xK$  for all  $x \in G$ . (Synonyms:  $K$  is a self-conjugate subgroup of  $G$ , a normal divisor of  $G$  (German: Normalteiler), an invariant subgroup of  $G$ .)

**Theorem.** Let  $\phi : G \rightarrow H$  be a group homomorphism. Let  $K = \ker \phi$ . Then  $K \triangleleft G$ . Moreover,  $\phi$  is injective if and only if  $K = \{e\}$ .

**Proposition-Definition.** Suppose that  $H \triangleleft G$ . As defined earlier,  $G/H$ , is the set of all left cosets of  $H$  in  $G$ . The equation

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

defines a binary operation on  $G/H$ , with respect to which  $G/H$  is a group (called the quotient group of  $G$  by  $H$ , or the factor group of  $G$  by  $H$ ). The notation for this group is just  $G/H$ , the same as for the set of left cosets. But it is always understood to have the group meaning only if  $H \triangleleft G$ .

The importance of the assumption that  $H \triangleleft G$  is to establish that the operation is well-defined:

**Lemma.** Suppose that  $H \triangleleft G$ , and  $x, x', y, y' \in G$ . If  $xH = x'H$  and  $yH = y'H$ , then  $(xy)H = (x'y')H$ .

PROOF. Since  $xH = x'H$ ,  $x^{-1}x' \in H$ . Similarly  $y^{-1}y' \in H$ . We must prove that  $(xy)^{-1}(x'y') \in H$ . Set  $h = x^{-1}x' \in H$ . Then

$$(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}hy' = h'y^{-1}y' \quad (5)$$

for some  $h' \in H$ . This is because  $y^{-1}h \in y^{-1}H = Hy^{-1}$ ,  $H$  being normal in  $G$ . Therefore  $y^{-1}h = h'y^{-1}$  for some  $h' \in H$ .

Finally since  $y^{-1}y' \in H$ , (5) implies that  $(xy)^{-1}(x'y') \in H$ .

The verification of the group axioms in  $G/H$  is straightforward and left to the reader. (The identity element is  $eH = H$ , and  $(xH)^{-1} = x^{-1}H$ .)

By definition of  $|G : H|$ ,  $|G/H| = |G : H|$ . By Lagrange's Theorem, if  $G$  is finite, then

$$|G/H| = |G|/|H|.$$

**Fundamental Theorem of Group Theory (or First Isomorphism Theorem).** Let  $\phi : G \rightarrow H$  be a group homomorphism. Then

(a)  $\text{im } \phi \leq H$ ;

(b)  $\ker \phi \triangleleft G$ ;

(c)  $G/\ker \phi \cong_{\phi} \text{im } \phi$ , by the isomorphism defined by  $\hat{\phi}(xH) = \phi(x)$  for all  $x \in G$ .

**Examples.**

(a) Every subgroup of an abelian group is normal.

(b) If  $G = (\mathbb{Z}, +)$  and  $H = n\mathbb{Z}$ , then  $G/H \cong \mathbb{Z}_n$ .

(c) If  $G = \langle g \rangle \cong \mathbb{Z}_n$ , and  $H = \langle g^m \rangle$  for some positive divisor  $m$  of  $n$ , then  $G/H = \langle gH \rangle \cong \mathbb{Z}_m$ .

- (d) If  $G = D_n$ , with reflection subgroup  $\langle \rho \rangle \cong \mathbb{Z}_n$ , then  $\langle \rho \rangle \triangleleft G$  and  $G/\langle \rho \rangle \cong \mathbb{Z}_2$ . (See (e).)
- (e) If  $H \leq G$  and  $|G : H| = 2$ , then  $H \triangleleft G$ . (Proof: Let  $x \in G$ . If  $x \in H$ , then  $xH = H = Hx$ . If  $x \notin H$ , then  $\bar{G} = H \cup xH$  so  $xH = G - H$ . Similarly,  $Hx = G - H$ . Therefore  $xH = Hx$ .)
- (f) Let  $F$  be a field, and  $n \in \mathbb{N}$ . Then  $\det : GL_n(F) \rightarrow U(F)$  is a surjective homomorphism. So  $SL_n(F) := \{g \in GL_n(F) \mid \det(g) = 1\}$  is a normal subgroup of  $GL_n(F)$ , and

$$GL_n(F)/SL_n(F) \cong U(F).$$

## CONJUGATES

Let  $G$  be a group. For any  $g, x \in G$ , the element

$$gxg^{-1}$$

is called a  $G$ -conjugate of  $x$  (or the conjugate of  $x$  by  $g$ ). Since  $x = exe^{-1}$ , every  $x \in G$  is a  $G$ -conjugate of itself. If  $G$  is abelian, then the only  $G$  conjugate of  $x$  is  $x$  itself. More generally if  $x$  is an element such that for all  $g \in G$ ,  $xg = gx$ , then the only  $G$ -conjugate of  $x$  is  $x$  itself.

If  $X \subseteq G$ , then  $gXg^{-1} := \{gxg^{-1} \mid x \in X\}$ .

The connection between conjugates and normal subgroups is this:

**Theorem.** Let  $H \leq G$ . Then the following conditions are equivalent:

- (a)  $H \triangleleft G$ .
- (b) For every  $g \in G$ ,  $gHg^{-1} = H$ .
- (c) For every  $g \in G$  and  $h \in H$ ,  $ghg^{-1} \in H$ .

Conjugates of  $x$  are very similar to  $x$  itself in the following sense.

**Theorem.** Let  $g \in G$ . Then the mapping  $G \rightarrow G$  sending

$$x \mapsto gxg^{-1} \text{ for all } x \in G$$

is an isomorphism from  $G$  to  $G$ . (An isomorphism from  $G$  to  $G$  is also called an automorphism of  $G$ .)

So if  $x$  and  $y$  are conjugate (by  $g$ ), the similarity between them has this precise meaning: conjugation by  $g$  is a “symmetry” of  $G$  carrying  $x$  to  $y$ .

In  $D_n$ , for example,  $\rho$  and  $\rho^{-1}$  are conjugate by any reflection. A reflection whose axis passes through a vertex  $a$ , and a reflection whose axis passes through a vertex  $b$ , are conjugate by a rotation carrying  $a$  to  $b$ . Similarly any two reflections whose axes pass through **no** vertex are conjugate. No reflection of the first type (axis passes through some vertex) is conjugate to a reflection of the second type (axis passes through no vertex).

**Proposition.** Conjugacy in  $G$  is an equivalence relation on  $G$ .

## SYMMETRIC GROUPS

**Definition.** Let  $S$  be any set (finite or infinite). Then  $Sym(S)$  is the group of all bijections from  $S$  to  $S$ . (Such bijections are called **permutations** of  $S$ .) The group operation is composition of functions. If  $n \in \mathbb{N}$ , then  $Sym(n)$  is defined to be  $Sym(\{1, 2, \dots, n\})$ .

The order of  $Sym(n)$  is  $|Sym(n)| = n!$ .

**Theorem.** Any element  $g \in \text{Sym}(n)$  is a product of disjoint cycles, in a unique way (except for the order in which the cycles appear). The order of  $g$  is the lcm of the lengths of the cycles.

**Proposition.** Let  $x \in \text{Sym}(n)$ , written as the product of disjoint cycles:

$$x = (a b c \cdots d)(e f \cdots) \cdots$$

Let  $g \in \text{Sym}(n)$ . Then

$$gxg^{-1} = (g(a) g(b) g(c) \cdots g(d))(g(e) g(f) \cdots) \cdots.$$

**Corollary.** Two elements of  $\text{Sym}(n)$  are conjugate if and only if they have the same “cycle shape” – i.e. their decompositions as products of disjoint cycles have the same number of cycles of any given length.

**Examples.** In  $\text{Sym}(2)$ ,  $e$  is conjugate only to itself, as is  $(12)$ .

In  $\text{Sym}(3)$ , all 2-cycles  $(ab)$  are conjugate (to one another); all 3-cycles  $(abc)$  are conjugate.

In  $\text{Sym}(4)$ , all 2-cycles are conjugate; all 3-cycles are conjugate; all 4-cycles are conjugate, and the three elements of the form  $(ab)(cd)$  are all conjugate.

In  $\text{Sym}(5)$  there are 7 conjugacy types:  $e$ ,  $(ab)$ ,  $(abc)$ ,  $(abcd)$ ,  $(abcde)$ ,  $(ab)(cd)$ , and  $(abc)(de)$ .

**Definition.** A transposition is a 2-cycle.

An important identity:

$$(1\ 2\ 3 \cdots n) = (1\ n)(1\ (n-1)) \cdots (1\ 3)(1\ 2). \quad (7)$$

**Theorem.** Every element of  $\text{Sym}(n)$  is a product of (not necessarily disjoint or distinct) transpositions.

**Theorem.** In  $\text{Sym}(n)$ , if  $t_1, t_2, \dots, t_n$  are transpositions such that  $t_1 t_2 \cdots t_n = e$ , then  $n$  is even.

**Definition.** Let  $g \in \text{Sym}(n)$ . Then  $g$  is **even** (resp. **odd**) if and only if  $g$  can be expressed as the product of an even (resp. odd) number of transpositions.

**Corollary.** Let  $g \in \text{Sym}(n)$ . Then  $g$  is either even or odd, but not both. Moreover the product and inverse of even elements of  $\text{Sym}(n)$  are again even. If  $g, h \in \text{Sym}(n)$  are both even or both odd, then  $gh$  is even. Otherwise  $gh$  is odd.

By (7),  $n$ -cycles are even if  $n$  is odd, and odd if  $n$  is even. Unfortunate but universally adopted terminology!!

**Definition.**  $\text{Alt}(n)$  is the subgroup of  $\text{Sym}(n)$  consisting of all even elements.

**Example.**  $\text{Alt}(2) = \{e\}$ .

$\text{Alt}(3)$  consists of  $e$  and the two 3-cycles.

$\text{Alt}(4)$  consists of  $e$ , the 3-cycles, and the elements of the form  $(ab)(cd)$ .

$\text{Alt}(5)$  consists of  $e$ , the 3-cycles, the elements of the form  $(ab)(cd)$ , and the 5-cycles.

**Theorem.**  $\text{Alt}(n) \triangleleft \text{Sym}(n)$  and  $\text{Sym}(n)/\text{Alt}(n) \cong \mathbb{Z}_2$ .

## SIMPLE GROUPS

(Not required)

**Definition.** A group  $G$  is simple if and only if  $|G| > 1$ , and the only normal subgroups of  $G$  are  $G$  and  $\{e\}$ .

Example:  $\mathbb{Z}_p$  is simple if and only if  $p$  is prime.

**Theorem.** Let  $G$  be a finite group,  $|G| > 1$ . Then there are subgroups

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_{n-1} \triangleleft G_n \quad (8)$$

for some  $n \in \mathbf{N}$ , such that  $G_1/G_0, G_2/G_1, \dots, G_n/G_{n-1}$  are all simple.

As a result, to understand all finite groups, one might adopt the strategy of trying to answer the following two questions:

1. (Classification problem for simple groups) What are all the finite simple groups up to isomorphism?
2. (Extension problem) What are all possible ways to “assemble” finite simple groups to obtain arbitrary finite groups, as in (8)?

Although both these problems seemed totally beyond reach for a long time, and (2) is still intractable, important progress was made on them in the second half of the twentieth century. First, the classification problem was actually solved. Second, the extension problem was finessed by the discovery (by Helmut Bender) of an easier way to decompose groups than (8). In this decomposition there are only two pieces (good). The first is very close to a direct product of simple groups (pretty good). The second can be quite complicated (bad) but it can be studied by means of its action on the first piece by conjugation (good).

Let’s consider the classification problem in a little more detail.

**Theorem.** An abelian group  $G$  is simple if and only if  $G \cong \mathbb{Z}_p$  for some  $p$ .

**Theorem.**  $Alt(n)$  is simple and nonabelian for  $n \geq 5$ .

**Theorem.** Let  $F$  be a finite field and  $n$  an integer,  $n \geq 2$ . Then with two exceptions, the group

$$PSL_n(F) := SL_n(F)/Z$$

is simple, where  $Z$  is the subgroup of  $SL_n(F)$  consisting of all matrices of the form  $cI$ ,  $c \in F$ ,  $c^n = 1$ . The two exceptions are  $PSL_2(\mathbb{Z}_2)$  and  $PSL_2(\mathbb{Z}_3)$ , of orders 6 and 12 respectively.

**Theorem (Classification of finite simple groups).** Every finite simple group is isomorphic to one of the following groups:

- (a)  $\mathbb{Z}_p$  for some prime  $p$ .
- (b)  $Alt(n)$  for some  $n \geq 5$ .
- (c) A “group of Lie type”, one of 19 infinite families of groups of matrices over finite fields. (One of these families consists of the groups  $PSL_n(F)$  above.)
- (d) One of exactly 26 other “sporadic” finite simple groups  $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$  (these 5 discovered by Émile Mathieu in the 1860’s),  $J_1$  (the next one to be discovered: 1965, by Zvonimir Janko),  $J_2, J_3, J_4$  (the last one to be discovered: 1974, again by Janko),  $Co_1, Co_2, Co_3, Fi_{22}, Fi_{23}, Fi_{24}, HS, Suz, Mc, O’N, Ly, Ru, HS, He, HN, Th, BM$  (the “Baby Monster”), and  $M$  =the “MONSTER”, first suspected to exist in the early 70’s (B. Fischer, R. Griess), and proved to exist (by hand!) in the early 80’s (R. Griess). The orders of these range from  $|M_{11}| = 11 \cdot 10 \cdot 9 \cdot 8 = 7,920$  to

$$\begin{aligned} |M| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &= 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 \approx 8 \times 10^{53}. \end{aligned}$$

$M_{11}$  was constructed, and is best understood, as a subgroup of  $Sym(11)$ . For a while the five Mathieu groups were rather controversial; the American group theorist G.A. Miller claimed to have proved that  $M_{24}$  couldn't exist, and a solid published proof of its existence seems not to have appeared until around 1930.

The Monster  $M$  was constructed, and to date is best understood, as a certain group of  $n \times n$  complex matrices with  $n = 196884$ . Thus,

$$M \leq GL_{196884}(\mathbf{C}).$$

The stories of the discoveries of the sporadic groups and the 19 families of groups of Lie type, of the proofs that they exist, of various efforts to “explain” their existence, and of the massive effort in the 60's and 70's which finally succeeded in proving the classification of finite simple groups, can be found in various articles and books. Joseph Gallian and Ronald Solomon (Notices of the American Mathematical Society), have separately written interesting accounts. Several of the best ones were written by Prof. Daniel Gorenstein, who was one of the architects of the classification plan, and its chief organizer, known sometimes as “Coach”. He was at Rutgers from 1969 until his death in 1992. The classification was announced in 1980, the combined result of tens of thousands of pages of journal articles and monographs, by somewhere between 50 and 100 group theorists. That “proof” is now known as the “first generation” proof; it had a glaring gap, which has been closed in the meantime. A “second generation” proof – better organized, although still massive – has been being written for many years by Gorenstein, Lyons and Solomon. Six volumes are published, with four or five more to come. Three of the discoverers of sporadic groups (O’Nan, Sims, Lyons) and one of the principal “explainers” of the Monster (Lepowsky) are still at Rutgers; Lepowsky did his work with a student, Arne Meurman, and Igor Frenkel of Yale. Sims, in particular, was the first to prove that several of the sporadic groups really exist, by constructing them as subgroups of  $Sym(n)$  for some  $n$ , and  $n$  was usually large. Using computers that were close to the largest available, but that still seemed much too small to support the necessary calculations in a reasonable time frame, Sims nevertheless succeeded in proving existence by devising original ways to calculate in groups acting on sets  $S$  with  $|S|$  in the range from  $10^7$  to  $10^{12}$ .

At the break of the 21st century, this theorem is not the only major recent theorem with a very, very long proof. (Another one is the four-color theorem, off-topic for group theory but on-topic for the complexity of the proof.) Serious discussion has now begun, sometimes with controversy, about the meaning of a “proof” whose length is measured in hundreds or thousands of pages, or which depends on machine calculations. Remarkably, in the last year a “formal proof” of the four-color theorem has been announced. This is a machine-generated proof using only axioms of mathematics and standard rules of inference. As I understand it, a person is needed to give the machine a sequence of (thousands of) intermediate goals, but the machine finds the proofs of these intermediate steps by itself, and at the end, the machine proof stands on its own.