Math 3230 - Abstract Algebra I
Summary of terms and theorems

1 Binary operations

Definitions and Theorems

1. *Associativity* of a binary operation $\circ$ on a set A means $(a \circ b) \circ c = a \circ (b \circ c)$ for **all** $a, b, c \in A$.
2. *Commutativity* of a binary operation $\circ$ on a set A means $a \circ b = b \circ a$ for **all** $a, b \in A$.
3. An *identity* element for a binary operation $\circ$ on a set A is an $e \in A$ such that $e \circ a = a$ and $a \circ e = a$ for **all** $a \in A$.
4. If the binary operation $\circ$ on A has identity e, an *inverse* of $a \in A$ is $a' \in A$ such that $a \circ a' = e$ and $a' \circ a = e$. **Note**: the inverse is in A and depends on the particular element. If there is no identity element, inverses make no sense.

Examples

1. In $\mathbb{R}$, addition and multiplication are both associative and commutative, with respective identities 0 and 1: for all a, b, and c in $\mathbb{R}$,

$$\begin{aligned} (a+b)+c = a+(b+c) \qquad & (ab)c = a(bc) \\ a+b = b+a \qquad & ab = ba \\ a+0 = 0+a = a \qquad & a \cdot 1 = 1 \cdot a = a. \end{aligned}$$

   In $\mathbb{R}$ the additive inverse of a is $-a$, and for non-zero a in $\mathbb{R}$ its multiplicative inverse is $1/a$ (0 has no multiplicative inverse).

2. In $\mathbb{C}$ addition and multiplication are both associative and commutative, with respective identities 0 and 1 (formulas in the previous example remain valid with real numbers replaced by complex numbers). In $\mathbb{C}$ the additive inverse of $z = x+yi$ is $-x-yi$, and for non-zero $z = x+yi$ in $\mathbb{C}$ its multiplicative inverse is $(x-yi)/(x^2+y^2)$.

3. Matrix multiplication on $\mathrm{M}_n(\mathbb{R})$ is associative with identity I_n. It is **not** commutative when $n \geq 2$. A matrix in $\mathrm{M}_n(\mathbb{R})$ has an inverse for multiplication precisely when its determinant is not 0. In the 2×2 case, the inverse of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $\frac{1}{ad-bc}\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$ when $ad - bc \neq 0$.

4. For any set X, composition of functions $X \to X$ is associative: if $f\colon X \to X$, $g\colon X \to X$, and $h\colon X \to X$ are all functions then $(f \circ g) \circ h = f \circ (g \circ h)$ as functions $X \to X$. Composition is usually not commutative: for most pairs of functions $X \to X$ the order of composition matters. The identity function $i\colon X \to X$ for composition is $i(x) = x$ for all $x \in X$. A function $f\colon X \to X$ has an inverse for composition precisely when it is a bijection (injective and surjective).

5. For any set X, the functions $X \to \mathbb{R}$ (not to be confused with the functions $X \to X$ in the previous example) can be added or multiplied pointwise: if $f\colon X \to \mathbb{R}$ and $g\colon X \to \mathbb{R}$ then we define $f+g\colon X \to \mathbb{R}$ and $fg\colon X \to \mathbb{R}$ by $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$ for $x \in X$. Both addition and multiplication of functions $X \to \mathbb{R}$ are commutative and associative. For functions $X \to \mathbb{R}$ the identity for addition is the constant function 0 and the identity for multiplication is the constant function 1. Every function $f\colon X \to \mathbb{R}$ has additive inverse $-f$, where $(-f)(x) = -(f(x))$ for all $x \in X$, and f has a multiplicative inverse precisely when it never takes the value 0, in which case its multiplicative inverse is the function $g(x) = 1/f(x)$ for all $x \in X$.

Non-examples

Because associativity and commutativity are properties on all pairs in a set, to prove a binary operation is not associative or not commutative it suffices to find a single counterexample: the property might hold some of the time but it has to fail at least once.

1. Subtraction on $\mathbb{Z}$ is not associative or commutative: $1-(2-3) = 2$ while $(1-2)-3 = -4$ and $1-2 = -1$ while $2-1 = 1$. There is no identity element for subtraction: if $e \in \mathbb{Z}$ satisfies $e-a = a$ for all a in $\mathbb{Z}$ then at $a = 0$ we see $e-0 = 0$, so $e = 0$ and then $0-a = a$ for all $a \in \mathbb{Z}$, which is false nearly all the time (indeed for every non-zero a).

2. Division on $\mathbb{R} - \{0\}$ is not associative or commutative: $1/(2/3) = 3/2$ while $(1/2)/3 = 1/6$ and $1/2 \neq 2/1$. There is no identity element either (why?).

3. On $\mathbb{R}_{>0}$, exponentiation ($a \circ b = a^b$) is not associative or commutative. For example, $(2^1)^2 = 4$ and $2^{(1^2)} = 2$, while $2^1 = 2$ and $1^2 = 1$.

4. Addition on $\mathbb{R}_{>0}$ is associative and commutative, but there is no identity.

5. Addition on $\mathbb{R}_{\geq 0}$ is associative and commutative with identity 0, but there are no inverses for non-zero elements: if $a \in \mathbb{R}_{\geq 0}$ and $a \neq 0$, there is no $a' \in \mathbb{R}_{\geq 0}$ such that $a + a' = 0$.

2 Groups

Definitions and Theorems

1. A *group* is a set G with a binary operation $\circ$ on it that is associative, has an identity (in G!), and each element of G has an inverse (in G!). For a general group G its operation is usually written multiplicatively: $g \circ h$ is written as gh, $\underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$ is written as g^n, and the inverse of g is written as g^{-1}.

2. When the operation on a group G is commutative, the group is called *commutative* or *abelian*. In an abstract abelian group additive notation is often used: the identity is 0, the operation is $g+h$, $\underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$ is written as ng, and the inverse of g is written as $-g$. (Do not use additive notation if a group is not abelian.)

3. Groups that are not commutative are called *non-commutative* or *non-abelian*. Non-commutativity means $gh \neq hg$ at least once, not always (*e.g.*, $ge = eg$ for all g in a group).

4. A group G is called *cyclic* if there is some element $g \in G$ such that (using multiplicative notation) every element of G has the form g^n for $n \in \mathbb{Z}$. We then write $G = \langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ and say g is a *generator* of G. Cyclic groups must be abelian, but the converse is false (see Non-examples below).

   Note. For groups where the operation is written additively, we write ng for n copies of g added together instead of g^n (n copies of g multiplied together), so $\langle g \rangle = \{ng : n \in \mathbb{Z}\} = \{\ldots, -2g, -g, 0, g, 2g, \ldots\}$.

Examples

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ with the operation of addition are abelian groups. Other abelian groups are the set of n-tuples $\mathbb{Z}^n$, $\mathbb{Q}^n$, $\mathbb{R}^n$, and $\mathbb{C}^n$ using componentwise addition and the set of $n \times n$ matrices $\mathrm{M}_n(\mathbb{Z})$, $\mathrm{M}_n(\mathbb{Q})$, $\mathrm{M}_n(\mathbb{R})$ and $\mathrm{M}_n(\mathbb{C})$ with matrix addition.

2. Three groups under multiplication are $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$, which are the non-zero rational numbers, non-zero real numbers, and non-zero complex numbers.

3. The set $\mathbb{Z}_m$ with the operation of addition modulo m is a finite abelian group.

4. The set μ_m of mth roots of unity in $\mathbb{C}$ with the operation of multiplication is a finite abelian group.

5. The set $U(m)$ of integers modulo m that are relatively prime to m, with the operation of multiplication modulo m, is a finite abelian group.

6. The set of $n \times n$ real matrices with non-zero determinant is a non-abelian group under multiplication. This group is denoted $\mathrm{GL}_n(\mathbb{R})$.

7. Some finite non-abelian groups include S_n (all permutations of $\{1, 2, \ldots, n\}$) for $n \geq 3$, which has $n!$, and D_n (all rigid motions of a regular n-gon) for $n \geq 3$, both under the operation of composition. In S_n every pair of disjoint permutations commute, but nondisjoint permutations may or may not commute: in S_3, (12) and (13) don't commute while (123) and (132) do commute (they are inverses).

8. The motions of the Rubik's cube under composition are a *huge* group, of order

$$\frac{8!12!3^8 2^{12}}{2 \cdot 3 \cdot 2} = \underbrace{43,252,003,274,489,856,000}_{\approx 4.3 \cdot 10^{19}} = 2^{27}3^{14}5^3 7^2 11.$$

9. The group $\mathbb{Z}$ is cyclic, with generator 1 or -1.

10. The group $\mathbb{Z}_m$ is cyclic, with generator 1 mod m or more generally a mod m when $(a, m) = 1$. For instance, additive generators of $\mathbb{Z}_8$ are 1, 3, 5, or 7 mod 8.

11. The group μ_m is cyclic, with a generator $\cos(2\pi/m) + i\sin(2\pi/m)$.

Non-examples

1. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_m$ under multiplication are not groups since 0 has no inverse.

2. The non-zero integers $\mathbb{Z} - \{0\}$ under multiplication are not a group since most integers (in fact all of them except ± 1) have no inverse for multiplication in $\mathbb{Z} - \{0\}$.

3. The set of 2×2 *integer* matrices with non-zero determinant is not a group under multiplication because some (in fact most) such matrices don't have a matrix inverse with integer entries.

4. The group $\mathbb{Q}$ under addition is not cyclic: no fraction has all its (additive) multiples equal to all of $\mathbb{Q}$.

5. Every cyclic group is abelian but many abelian groups are not cyclic. For instance, all $U(m)$ are abelian and many are not cyclic; the first three noncyclic $U(m)$ are $U(8)$, $U(12)$, and $U(15)$.

3 Subgroups

Definitions and Theorems

1. A *subgroup* of a group G is a subset H of G that is a group using the same operation that G has. (Associativity on a subset is automatic, and if G is an abelian group then commutativity of the operation on a subset is automatic. The identity element and inverses in a subgroup have to be the same as in G.)

2. A *cyclic subgroup* H is a subgroup that is a cyclic group in its own right: $H = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ for some $a \in H$.

3. An *abelian subgroup* H is a subgroup that is an abelian group in its own right: $hk = kh$ for all $h, k \in H$.

4. The *center* $Z(G)$ of a group G is all elements of G that commute with everything in G: $Z(G) = \{z \in G : zg = gz \text{ for all } g \in G\}$.

5. **Theorem**. *Every subgroup of an abelian group is abelian and every subgroup of a cyclic group is cyclic.* The first result only relies on some very simple reasoning (and knowing what the words mean), but the second result requires a clever idea (using division algorithm in $\mathbb{Z}$).

Examples

1. In S_4, (12) and (34) commute and $H = \{(1), (12), (34), (12)(34)\}$ is an abelian subgroup of S_4 that is not cyclic (every element squares to (1)).

2. In S_4 let $g = (1234)$. Then $g^2 = (13)(24)$, $g^3 = (1432) = (4321)$, and $g^4 = (1)$, so $\langle g \rangle = \{(1), (1234), (13)(24), (4321)\}$.

3. Subgroups of $\mathbb{Z}$ include the even integers $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$, and more generally $a\mathbb{Z} = \{am : m \in \mathbb{Z}\}$ for $a \in \mathbb{Z}$. (In fact it is a theorem that every subgroup of $\mathbb{Z}$ is $a\mathbb{Z}$ for some integer a.)

4. In $\mathbb{R}^\times$, the subset $\mathbb{R}_{>0}$ of positive numbers is a subgroup.

5. In $\mathbb{R}^\times$, the subset $\langle 2 \rangle = \{2^n : n \in \mathbb{Z}\} = \{\ldots, 1/4, 1/2, 1, 2, 4, \ldots\}$ is a subgroup.

6. In $\mathbb{C}^\times$, the subset $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is a subgroup.

7. In $\mathrm{GL}_2(\mathbb{R})$, one cyclic subgroup is $\{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\} = \{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n : n \in \mathbb{Z}\} = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$.

8. Subgroups of $\mathrm{GL}_2(\mathbb{R})$ include $\mathrm{Aff}(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{R}^\times, b \in \mathbb{R}\}$ and $\mathrm{SL}_2(\mathbb{R}) =$ the 2×2 matrices with determinant 1. These are both non-abelian, but the subgroup of diagonal matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ where $a, b \in \mathbb{R}^\times$ is an abelian subgroup.

9. The alternating group A_n, which is all *even* permutations in S_n, is a subgroup of S_n.

10. Every group G has the subgroups G and $\{e\}$. If a subgroup contains a then it must at least contain $\langle a \rangle$, but could be larger.

11. The group S_n is not cyclic for $n \geq 3$ since it is non-abelian for $n \geq 3$. While S_n for $n \geq 3$ does not have a single generator, it is generated by all the transpositions (ij).

12. The center of a group is a subgroup of G. If G is abelian then $Z(G) = G$, and conversely. Having $Z(G)$ be a "small" subgroup of G is a measure of G being highly non-abelian.

13. The center of $\mathrm{GL}_2(\mathbb{R})$ consists of the scalar diagonal matrices $\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{R}^\times\}$. This is determined by testing commutativity with a couple of basic matrices like $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Note these have determinant 1, so they also show the center of $\mathrm{SL}_2(\mathbb{R})$ is the scalar diagonal matrices with determinant 1, which is $\pm I_2$.

14. The Rubik's cube group has a center of size 2: the identity and the "superflip" move.

Non-examples

1. In $\mathbb{Z}$, while the even integers $2\mathbb{Z}$ are a subgroup, the odd integers $1 + 2\mathbb{Z}$ are not a subgroup (no identity, not closed under addition).

2. In $\mathbb{R}^\times$, while the positive numbers $\mathbb{R}_{>0}$ are a subgroup, the negative numbers $\mathbb{R}_{<0}$ are not a subgroup (no identity, not closed under multiplication).

3. Even though $\mathbb{R}^\times$ is a subset of $\mathbb{R}$ and each is a group under a suitable operation (addition for $\mathbb{R}$, multiplication for $\mathbb{R}^\times$), we do not consider $\mathbb{R}^\times$ to be a subgroup of $\mathbb{R}$ since the operations are not the same.

4. In the group $\mathbb{R}$, the subset of positive real numbers is closed under addition but is not a subgroup of $\mathbb{R}$ since there is no additive identity. The subset $\mathbb{R}_{\geq 0}$ of nonnegative numbers is not a group (under addition) even though it has an identity since additive inverses generally fail to exist in $\mathbb{R}_{\geq 0}$.

4 Order

Definitions and Theorems

1. The *order* of a subgroup $H \subset G$ is the size of H and is denoted $|H|$. When H is infinite, often we write $|H| = \infty$.

2. The *order* of an element $g \in G$ is the size of $\langle g \rangle$ and is denoted $|g|$, so $|g| = |\langle g \rangle|$.

3. **Theorem**. *If $|g| < \infty$ then $|g|$ is the smallest $n \geq 1$ such that $g^n = e$. If $|g| = \infty$ there is no $n \geq 1$ such that $g^n = e$.*

4. **Theorem**. *If $|g| = n$ is finite then $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ and $g^i = g^j \iff i \equiv j \bmod n$. We have $|g^k| = n$ when $(k, n) = 1$ and $|g^d| = n/d$ if $d \mid n$.*

Examples

1. We have $|\mathbb{Z}_m| = m$, $|S_n| = n!$, $|A_n| = n!/2$, and $|D_n| = 2n$. The order of $U(m)$ is denoted $\varphi(m)$, so $\varphi(4) = |\{1, 3 \bmod 4\}| = 2$ and $\varphi(5) = |\{1, 2, 3, 4 \bmod 5\}| = 4$.

2. In $\mathbb{Z}$, every integer besides 0 has infinite order under addition, while 0 has order 1.

3. In the group $\mathbb{R}^\times$, 1 has order 1, -1 has order 2 (because $(-1)^2 = 1$ while $(-1)^1 \neq 1$), and every non-zero real number besides ± 1 has infinite order.

4. In $\mathbb{C}^\times$, -1 has order 2 and i has order 4. The complex number $\cos(2\pi/n) + i\sin(2\pi/n)$ has order n. Most non-zero complex numbers, like most non-zero real numbers, have infinite multiplicative order.

5. In S_4, $|(1234)| = 4$: $(1234)^2 = (13)(24)$, $(1234)^3 = (1432) = (4321)$, and $(1234)^4 = (1)$. More generally, in S_n a k-cycle $(i_1 i_2 \ldots i_k)$ has order k.

6. In a finite group every element has finite order. In $\mathbb{Z}_m$ the order of $a \bmod m$ is $m/(a, m)$. In $U(m)$ there is no simple formula for the order of an element (other than $\pm 1 \bmod m$).

Non-examples

1. If $g^n = e$ in a group, this does **not** imply $|g| = n$. Consider $(-1)^4 = 1$ in $\mathbb{R}^\times$ and -1 has order 2, not 4. What $g^n = e$ implies is that $|g| \leq n$. In fact, $g^n = e \iff |g| \mid n$.

2. In S_3, $|(12)| = |(23)| = 2$ and $|(12)(23)| = |(123)| = 3$, so $|(12)(23)| \neq |(12)||(23)|$.

3. In $\mathrm{GL}_2(\mathbb{R})$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ both have order 2, but their product $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order (for $n \in \mathbb{Z}$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$), so in some groups two non-commuting (!) elements with finite order can have a product with infinite order.

5 Cosets

Definitions and Theorems

1. For a subgroup H in a group G, a *left coset* of H is a subset of the form $gH = \{gh : h \in H\}$ and a *right coset* of H is a subset of the form $Hg = \{hg : h \in H\}$. A coset is usually not a subgroup but can be viewed as a "translated subgroup" from either the left side or right side. When G is non-abelian, gH need not equal Hg as subsets of G.

   Additive notation: a left coset is $g+H = \{g+h : h \in H\}$ and a right coset is $H+g = \{h+g : h \in H\}$. Since $+$ is commutative we have $g+h = h+g$ for all $h \in H$, so $g+H = H+g$ as subsets of G.

2. A *representative* of a coset (gH or Hg) is any element in the coset.

Examples

1. In $\mathbb{Z}$, $3+2\mathbb{Z} = 1+2\mathbb{Z}$ and this is not a subgroup of $\mathbb{Z}$.

2. In $\mathbb{Z}$, $1+2\mathbb{Z} = 3+2\mathbb{Z} = 5+2\mathbb{Z} = -1+2\mathbb{Z} = a+2\mathbb{Z}$ for each odd integer a (that is, each a in the coset $1+2\mathbb{Z}$).

3. In S_4, let $H = \langle(1234)\rangle = \{(1234), (13)(24), (1432), (1)\}$. Then

$$\begin{aligned} (12)H &= \{(234), (1324), (143), (12)\} \\ H(12) &= \{(134), (1423), (243), (12)\} \end{aligned}$$

   and

$$\begin{aligned} (13)H &= \{(12)(34), (24), (14)(23), (13)\} \\ H(13) &= \{(14)(23), (24), (12)(34), (13)\}. \end{aligned}$$

   Thus $(12)H \neq H(12)$ while $(13)H = H(13)$.

4. In D_4 let $H = \langle s\rangle = \{1, s\}$. Then $rH = \{r, rs\}$ and $Hr = \{r, sr\}$. Since $rs \neq sr$ in D_4, the left and right cosets rH and Hr are different (their intersection is $\{r\}$).

5. In D_4, let $H = \langle s\rangle = \{1, s\}$. Then $rsH = \{rs, rs^2\} = \{rs, r\} = rH$ (see previous example). Both r and rs are in this coset and they represent the same left H-coset.

Non-examples

1. In S_4 let H be the subgroup $\{(1), (12), (34), (12)(34)\}$. For $g = (1234)$ we have

$$\begin{aligned} gH &= \{(1234), (134), (123), (13)\}, \\ Hg &= \{(1234), (234), (124), (24)\} \end{aligned}$$

   so $gH \neq Hg$.

6 Dihedral Groups (review)

Definitions and Theorems

1. For $n \geq 3$, the group D_n is $\{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$ where r has order n, s has order 2, and $sr = r^{-1}s$. The order of this group is $2n$.
2. **Theorem**. *For all $k \in \mathbb{Z}$, $sr^k = r^{-k}s$.*
3. **Theorem**. The center of D_n is $\{1\}$ is n is odd and $\{1, r^{n/2}\}$ is n is even.

Examples

1. In D_4, $rsr^2s^3r^3s = rsr^2sr^3s = rr^{-2}ssr^3s = r^{-1}r^3s = r^2s$.
2. In D_n, the reflections are $s, rs, \ldots, r^{n-1}s$ and all have order 2. In particular, rs has order 2, so $|rs| = 2$ while $|r||s| = n \cdot 2 = 2n$. Thus $|rs| \neq |r||s|$.
3. The only rotation of order 2 is $r^{n/2}$ (180-degree rotation) for even n.

7 Index and Lagrange's Theorem

Definitions and Theorems

1. **Theorem**. *If H is a subgroup of a group G then different left cosets of H are disjoint. Equivalently, if $gH \cap g'H \neq \emptyset$ then $gH = g'H$. In particular, if $g' \in gH$ then $g'H = gH$.*

   Each left coset gH has the same cardinality as H: $H \to gH$ by $h \mapsto gh$ is a bijection between H and gH.

   Similar results hold for right cosets: if $Hg \cap Hg' \neq \emptyset$ then $Hg = Hg'$, and $H \to Hg$ by $h \mapsto hg$ is a bijection between H and Hg.

2. The *index* of a subgroup H in G is the number of different left cosets of H in G. This is also the number of different right cosets of H in G. It is denoted $[G : H]$.

3. **Theorem**. (Lagrange) *If H is a subgroup of a finite group G then $[G : H]|H| = |G|$. In particular, in a finite group each subgroup has order dividing the order of the group.*

4. **Theorem**. *The order of each element of a finite group G divides the order of G. In particular, $g^{|G|} = e$ for all $g \in G$.* (For abelian G this can be proved without using Lagrange's theorem.)

5. **Theorem**. (Fermat) *For prime p, if $a \not\equiv 0 \bmod p$ then $a^{p-1} \equiv 1 \bmod p$.* This is the special case of Theorem 4 for $G = U(p)$.

6. **Theorem**. (Euler) *For $m \geq 2$, if $(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \bmod m$.* This is the special case Theorem 4 for $G = U(m)$.

Examples

1. For a subgroup H of a finite group G, $[G : H] = |G|/|H|$.

2. $[\mathbb{Z} : m\mathbb{Z}] = |\{m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, m - 1 + m\mathbb{Z}\}| = m$ for each positive integer m.

3. $[\mathbb{R}^\times : \mathbb{R}_{>0}] = 2$ since $\mathbb{R}^\times = \mathbb{R}_{>0} \cup -\mathbb{R}_{>0}$ (cosets are positive and negative real numbers).

4. $[\mathbb{R}^\times : \{\pm 1\}] = \infty$ since each coset is of the form $x\{\pm 1\} = \{x, -x\}$, a pair of numbers equal up to sign, and there are infinitely many such cosets in $\mathbb{R}^\times$.

5. $[\mathbb{R} : \mathbb{Z}] = \infty$: the different cosets $a + \mathbb{Z}$ are represented by the real numbers a in the interval $[0, 1)$.

8 Conjugation

Definitions and Theorems

1. In a group G, we call elements x and y *conjugate* if $y = gxg^{-1}$ for some $g \in G$.
2. The *conjugacy class* of $x \in G$ is $\{gxg^{-1} : g \in G\}$.
3. In a group G, we call subgroups H and K *conjugate* if $K = gHg^{-1} = \{ghg^{-1} : h \in H\}$ for some $g \in G$.
4. **Theorem**. *Different conjugacy classes in a group are disjoint. Equivalently, if two conjugacy classes in a group overlap then they are equal.*
5. **Theorem**. *If H is a subgroup of G then gHg^{-1} is also a subgroup of G for each $g \in G$.* (This is a contrast with cosets gH of H, which are **never** subgroups except for the coset H itself.)
6. **Theorem**. *For $g \in G$ and a subgroup H of G, the conditions $gH = Hg$ and $gHg^{-1} = H$ are equivalent.*
7. **Theorem**. *For a subgroup H of G, $gHg^{-1} = H$* **for all** *$g \in G$ if and only if $gHg^{-1} \subset H$* **for all** *$g \in G$.*

Examples

1. In D_4, the conjugacy classes are $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, r^2s\}$, $\{rs, r^3s\}$.
2. In D_n, all reflections are conjugate when n is odd (each reflection is across a line through a vertex and the center of the opposite edge) and there are two conjugacy classes of reflections when n is even (reflection across a vertex-vertex line vs. across a vertex-opposite edge line).
3. In S_n, all transpositions are conjugate to (12): if $i \neq 1, 2$ and $j \neq 1, 2$ then
$$(ij) = (1i)(2j)(12)(2j)(1i) = (1i)(2j)(12)((1i)(2j))^{-1}.$$
If $i = 1$ and $j \neq 1, 2$ then $(ij) = (1j) = (2j)(12)(2j) = (2j)(12)(2j)^{-1}$. If $i = 2$ and $j \neq 1, 2$ then $(ij) = (2j) = (1j)(12)(1j) = (1j)(12)(1j)^{-1}$.
4. For a k-cycle $(i_1 i_2 \dots i_k)$ and $\sigma \in S_n$, $\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \dots\, \sigma(i_k))$ is also a k-cycle. This explains the previous example: if $i \neq 1, 2$ and $j \neq 1, 2$ then $(ij) = \sigma(12)\sigma^{-1}$ where $\sigma = \binom{12ij}{ij12}$, if $i = 1$ and $j \neq 1, 2$ then $(ij) = (1j) = \sigma(12)\sigma^{-1}$ where $\sigma = \binom{2j}{j2} = (2j)$, and if $i = 2$ and $j \neq 1, 2$ then $(ij) = (2j) = \sigma(12)\sigma^{-1} = \sigma(21)\sigma^{-1}$, where $\sigma = \binom{1j}{j1} = (1j)$.
5. In S_4 let H be the subgroup $\{(1), (12), (34), (12)(34)\}$. For $g = (1234)$ we have $g^{-1} = (4321)$ and
$$(1234)(1)(4321) = (1) \qquad (1234)(12)(4321) = (23)$$
$$(1234)(34)(4321) = (14) \qquad (1234)(12)34)(4321) = (14)(23),$$

so

$$gHg^{-1} = \{(1), (14), (23), (14)(23)\} \neq H.$$

Non-examples

1. The rotations r and r^3 in D_4 are conjugate in D_4: $srs^{-1} = r^3$. But r and r^3 are **not** conjugate in the subgroup $\langle r \rangle$ since this subgroup is abelian and different elements of an abelian group are not conjugate in that group.

2. Since $|gHg^{-1}| = |H|$ when H is finite, to prove $gHg^{-1} = H$ for a specific $g \in G$ it suffices to show $gHg^{-1} \subset H$ (that is, $ghg^{-1} \in H$ for all $h \in H$). But there are infinite subgroups $H \subset G$ where, for specific $g \in G$, $gHg^{-1} \subset H$ and $gHg^{-1} \neq H$. For example, let $G = \mathrm{Aff}(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{R}^\times, b \in \mathbb{R}\}$ and $H = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$. If $g = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ then $g^{-1} = \left(\begin{smallmatrix} 1/2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $g\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)g^{-1} = \left(\begin{smallmatrix} 1 & 2n \\ 0 & 1 \end{smallmatrix}\right)$, so $gHg^{-1} = \{\left(\begin{smallmatrix} 1 & 2n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\}$ is a proper subset of H (it does not contain $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$). Moreover, $g^{-1}\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)g^{-1} = \left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right) \notin H$, so in this example we have $gHg^{-1} \subset H$ and $g^{-1}Hg \not\subset H$!

9 Normal subgroups, quotient groups

Definitions and Theorems

1. A subgroup N in a group G is called *normal* if its left and right coset by each $g \in G$ is the same: $gN = Ng$ for all $g \in G$. (**Warning**: saying $gN = Ng$ means the two *sets* gN and Ng are equal, **not** necessarily that $gn = ng$ for all $n \in N$.) The notation for N being a normal subgroup of G is $N \lhd G$ and we often write gN as $\overline{g}$.

2. **Theorem**. *Every subgroup of a group with index* 2 *is a normal subgroup.*

3. $[S_n : A_n] = 2$ and therefore A_n is a normal subgroup of S_n since it has index 2.

4. If N is a normal subgroup of G then its cosets can be multiplied by the rule $gN \cdot g'N = gg'N$ (or $\overline{g} \cdot \overline{g'} = \overline{gg'}$). This is well-defined (that is, independent of the representatives used for the two cosets of N) and makes the cosets of N in G into a group called the *quotient group* or *factor group* of G modulo N, and denoted G/N. Its order is $[G : N]$, the identity is $\overline{1} = N$, and $(gN)^{-1} = g^{-1}N$ (that is, $\overline{g}^{-1} = \overline{g^{-1}}$).

5. **Theorem**. *Let $N \lhd G$. If G is abelian then G/N is abelian. If G is cyclic then G/N is cyclic.*

Examples

1. In a group G, the center $Z(G)$ is a normal subgroup.

2. In an abelian group every subgroup is normal. The converse is false: every subgroup of Q_8 is normal but Q_8 is not abelian.

3. In $\mathbb{R}$, $2\pi\mathbb{Z}$ is a subgroup that is automatically normal since $\mathbb{R}$ is abelian, and the quotient group $\mathbb{R}/2\pi\mathbb{Z}$ has coset representatives $a \in [0, 2\pi)$. Cosets in $\mathbb{R}/2\pi\mathbb{Z}$ look like angles on a circle using radian measure, *e.g.*, $-\pi = \pi$ in $\mathbb{R}/2\pi\mathbb{Z}$ just as $-\pi$ and π are the same angle in radians. The real numbers equal to $\overline{0}$ in $\mathbb{R}/2\pi\mathbb{Z}$ are the integral multiples of 2π. Addition in the quotient group $\mathbb{R}/2\pi\mathbb{Z}$ is the same as adding angles up to an integral multiple of 2π.

4. The center of D_4 is $N = \{1, r^2\}$. What "is" the group D_4/N? It has order 4. Is it abelian? Is it cyclic? Writing out the cosets (left vs. right doesn't matter since $N \lhd D_4$), we get

$$\overline{1} = N = \{1, r^2\}, \quad \overline{r} = rN = \{r, r^3\},$$

$$\overline{s} = sN = \{s, sr^2\} = \{s, r^2s\}, \quad \overline{rs} = rsN = \{rs, rsr^2\} = \{rs, r^3s\}.$$

   These are disjoint and fill up all of D_4, so we are done with the listing of cosets. The identity in D_4/N is $\overline{1} = N$.

   In the group D_4/N, $\overline{r}^2 = \overline{r^2} = \overline{1}$ since $r^2 \in N$. (More explicitly in terms of cosets, $(rN)^2 = rNrN = r^2N = N$ since $r^2 \in N$.) Thus $\overline{r}$ has order 2 in D_4/N even though r has order 4 in D_4 (a certain amount of collapsing has happened). Also $\overline{s}^2 = \overline{s^2} = \overline{1}$ and $\overline{rs}^2 = \overline{(rs)^2} = \overline{1}$.

since $(rs)^2 = 1$ (check that algebraically, or see that rs is a reflection). Thus each non-identity element of D_4/N has order 2, so D_4/N (having order 4) is not cyclic. Writing $D_4/N = \{\overline{1}, \overline{r}, \overline{s}, \overline{rs}\}$, we have $\overline{r} \cdot \overline{s} = \overline{s} \cdot \overline{r}$ since the left side is $\overline{rs} = rsN$ and the right side is $\overline{sr} = srN = r^3sN = rsN$ (the N-coset containing r^3s is rsN), so D_4/N is abelian even though D_4 is not.

5. In S_4 let N be the subgroup $\{(1), (12)(34), (13)(24), (14)(23)\}$ (identity and all products of disjoint 2-cycles). For $g = (1234)$ we have

$$gN = \{(1234), (13), (1432), (24)\}$$
$$Ng = \{(1234), (24), (1432), (13)\},$$

so $gN = Ng$ for this one g. To prove $gN = Ng$ for **all** $g \in S_4$ it suffices to check that equation for a set of permutations that generates S_4, such as $(12), (23)$, and (34). Check that $(12)N = N(12)$, $(23)N = N(23)$, and $(34)N = N(34)$.

6. In the group S_4 the subgroup $N = \{(1), (12)(34), (13)(24), (14)(23)\}$ is normal (see the previous result). The number of cosets of N in S_4 is $[S_4 : N] = |S_4|/|N| = 24/4 = 6$. The 6 cosets

$$(1)N, \quad (12)N, \quad (13)N, \quad (23)N, \quad (123)N, \quad (321)N$$

are distinct, either by tedious direct calculation or by the following conceptual reasoning: if $aN = bN$ for a, b taken from $\{(1), (12), (13), (23), (123), (132)\}$ then $ab^{-1} \in N$, and the chosen representatives belong to S_3, so $ab^{-1} \in S_3 \cap N = \{(1)\}$, and thus $a = b$. Hence for different a and b in S_3 we have $aN \neq bN$. Therefore the above listing of 6 cosets, each of order $|N| = 4$, exhausts the group S_4 (of order $24 = 6 \cdot 4$).

Since $N \lhd S_4$, the group law in S_4/N is $(gN)(hN) = ghN$. From the choice of coset representatives above, the group law on S_4/N resembles the group law in S_3.

In S_4 let H be the subgroup $\{(1), (12), (34), (12)(34)\}$. For $g = (1234)$ we have $gH \neq Hg$ since

$$gH = \{(1234), (134), (123), (13)\},$$
$$Hg = \{(1234), (234), (124), (24)\}$$

7. Let $G = S_4$ and let $H = \{(1), (12), (34), (12)(34)\}$. The operation $(aH)(bH) = abH$ is not well-defined on left H-cosets. That is, if $aH = a'H$ and $bH = b'H$, it not always true that $abH = a'b'H$. Consider the left cosets

$$(13)H = \{(13), (123), (134), (1234)\}, \quad (14)H = \{(14), (124), (143), (1243)\}.$$

Then $(13)H = (134)H$ and $(14)H = (143)H$, but $(13)(14)H = (143)H = (14)H$ while $(134)(143)H = (1)H = H$. Since $H \neq (14)H$ (for example, $(14) \in (14)H$ but $(14) \notin H$), we get $(13)(14)H \neq (134)(143)H$.

Non-examples

1. In D_4, $\langle s \rangle = \{1, s\}$ is a subgroup of order 2 that is not normal since $r\langle s \rangle r^{-1} = \langle rsr^{-1} \rangle = \langle r^2 s \rangle = \{1, r^2 s\} \neq \langle s \rangle$. Also $\langle r^2 \rangle = \{1, r^2\}$ is a subgroup of order 2 that is normal (this is the center of D_4), so cyclic subgroups of a group with the same size need not both be normal or both be non-normal.

10 Homomorphisms

Definitions and Theorems

1. A *homomorphism* from the group $(G, \cdot)$ to the group $(H, \circ)$ is a function $f\colon G \to H$ that transforms the operation in G to the operation in H:

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

   for all $g_1, g_2 \in G$. The set $f(G) = \{f(g) : g \in G\}$ of all values f has in H is called the *image* of f.

2. The *kernel* of a homomorphism $f\colon G \to H$ is the elements in G mapped to the identity in H:

   $$\ker f = \{g \in G : f(g) = e_H\}.$$

3. **Theorem**. *If $f\colon G \to H$ is a homomorphism then $f(e_G) = e_H$, $f(g)^n = f(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$, $\ker f$ is a subgroup of G, and image $f(G)$ is a subgroup of H.*

   (If either group is written additively then the identities change: $f(0) = 0$ and $f(ng) = nf(g)$ if both groups are additive, $f(0) = 1$ and $f(ng) = f(g)^n$ if only the first group is additive, and $f(1) = 0$ and $f(g^n) = nf(g)$ if only the second group is additive.)

4. **Theorem**. *For every homomorphism $f\colon G \to H$ the kernel $\ker f$ is a normal subgroup of G.*

5. **Theorem**. *A homomorphism is injective if and only if its kernel is trivial.*

6. **Theorem**. *For a homomorphism $f\colon G \to H$ and $g \in G$ of order n, $f(g)$ has order dividing n.*

7. Let G be a group and N be a normal subgroup. Then there is a "canonical" reduction homomorphism $r\colon G \to G/N$ called *reduction* mod N, defined by $r(g) = gN = \overline{g}$ for all $g \in G$.

Examples

1. Doubling is a homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}$ where $f(a) = 2a$ for all $a \in \mathbb{Z}$. Being a homomorphism means $2(a+b) = 2a+2b$, which is a special case of the distributive property for multiplication over addition. This homomorphism is injective but it is not surjective: its kernel is $\{0\}$ and its image is $2\mathbb{Z}$.

2. In an abelian group G, $(g_1g_2)^k = g_1^k g_2^k$ for all $g_1, g_2 \in G$ and $k \in \mathbb{Z}$, so for each integer k the kth power function $f(g) = g^k$ is a homomorphism $G \to G$. (If G is written additively the identity becomes $k(g_1 + g_2) = kg_1 + kg_2$. The previous example is the special case $G = \mathbb{Z}$ and $k = 2$, using additive notation.) If $k = -1$ the kth power homomorphism is inversion on G and this function is its own inverse since $(g^{-1})^{-1}$. For a non-abelian group, inversion $g \mapsto g^{-1}$ is *not* a homomorphism since $(gg')^{-1} = (g')^{-1}g^{-1}$, which usually is not $g^{-1}(g')^{-1}$.

3. For fixed $g \in G$, conjugation by g is the function $f\colon G \to G$ by $f(x) = gxg^{-1}$. This is an homomorphism from G to itself.

4. Reduction modulo 2 is a homomorphism $f\colon \mathbb{Z} \to \mathbb{Z}_2$, since $f(a+b) = a+b \bmod 2 = a \bmod 2 + b \bmod 2 = f(a) + f(b)$. This homomorphism is surjective but not injective. More generally, for each integer $m \geq 2$ the reduction $r\colon \mathbb{Z} \to \mathbb{Z}_m$ where $r(a) = a \bmod m$ is a homomorphism that is surjective but not injective.

5. For an $m \times n$ real matrix A, the function $L_A\colon \mathbb{R}^n \to \mathbb{R}^m$ where $L_A(\mathbf{v}) = A\mathbf{v}$ is additive, so it is a homomorphism ($\mathbb{R}^n$ and $\mathbb{R}^m$ are additive groups) and $\ker L_A = \{\mathbf{v} \in \mathbb{R}^n : A\mathbf{v} = \mathbf{0}\}$ is the null space of A.

6. If $N \lhd G$ then the reduction mapping $r\colon G \to G/N$ where $r(g) = gN$ is a homomorphism by the definition of the group operation in G/N and it is surjective with kernel N.

7. If $f\colon G \to \widetilde{G}$ is a homomorphism and $N \lhd G$, the image $f(N)$ need not be a normal subgroup of $\widetilde{G}$. For example, in D_3 if $G = \langle s \rangle = \{1, s\}$ and $\widetilde{G} = D_3$, and $f\colon \langle s \rangle \to D_3$ is the inclusion function, then $\langle s \rangle \lhd \langle s \rangle$ but $f(\langle s \rangle) = \langle s \rangle \not\lhd D_3$.

8. The exponential function $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ is a group homomorphism since $e^{x+y} = e^x e^y$, and the natural logarithm $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ is a group homomorphism since $\ln(ab) = \ln a + \ln b$. That a homomorphism $f\colon G \to H$ satisfies $f(g^n) = f(g)^n$ is related to the equations $e^{nx} = (e^x)^n$ (homomorphism from an additive to multiplicative group) and $\ln(x^n) = n \ln x$ (homomorphism from a multiplicative to additive group).

9. The sign function $\operatorname{sign}\colon \mathbb{R}^\times \to \{\pm 1\}$, sending each non-zero real number x to its sign, is a homomorphism that is surjective with kernel $\{x \in \mathbb{R}^\times : x > 0\} = \mathbb{R}_{>0}$,

10. Since $\det(AB) = \det A \det B$ for all A and B in $\mathrm{M}_2(\mathbb{R})$, the determinant is a homomorphism $\det\colon \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ with kernel $\mathrm{SL}_2(\mathbb{R})$ and image $\mathbb{R}^\times$ since $a = \det\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Non-examples

1. The determinant is a multiplicative function $\det\colon \mathrm{M}_2(\mathbb{R}) \to \mathbb{R}$, but this is not a homomorphism since $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{R}$ are not groups under multiplication.

2. On a non-abelian group G, inversion $i\colon G \to G$ is **never** a homomorphism. We have $i(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = i(g_2) i(g_1)$, so inversion actually reverses the order of multiplication. That is not a full proof of inversion not being a homomorphism. If inversion were a homomorphism then $i(g_1 g_2) = i(g_1) i(g_2) = g_1^{-1} g_2^{-1} = (g_2 g_1)^{-1}$ for all $g_1, g_2 \in G$, so we'd have $(g_1 g_2)^{-1} = (g_2 g_1)^{-1}$. Inverting both sides, $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$, which means G is abelian, a contradiction.

11 Isomorphisms

Definitions and Theorems

1. An *isomorphism* from the group G to the group H is a bijective homomorphism $f\colon G \to H$. When there is an isomorphism from G to H we say G and H are *isomorphic* and write $G \cong H$.

2. **Theorem**. *Every infinite cyclic group is isomorphic to* $\mathbb{Z}$.

3. **Theorem**. *Every finite cyclic group of order* n *is isomorphic to* $\mathbb{Z}_n$.

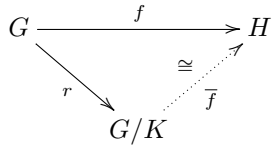
4. **Theorem**. *If* $f\colon G \to H$ *is an isomorphism then it satisfies the following properties:*

   - g *has order* n *if and only if* $f(g)$ *has order* n,
   - g *and* g' *commute in* G *if and only if* $f(g)$ *and* $f(g')$ *commute in* H,
   - g *and* g' *are conjugate in* G *if and only if* $f(g)$ *and* $f(g')$ *are conjugate in* H,
   - $f(Z(G)) = Z(H)$ *(so* $Z(G) \cong Z(H)$ *using the isomorphism* f *from* G *to* H*)*,
   - G *is abelian if and only if* H *is abelian, and* G *is cyclic if and only if* H *is cyclic.*

   All of these equivalences are in general *false* if $|G| > 1$ and $f\colon G \to \widetilde{G}$ is the trivial homomorphism,which is not an isomorphism.

5. **First Isomorphism Theorem**. *If* $f\colon G \to H$ *is a homomorphism and* $K = \ker f$*, then* G/K *is isomorphic to the image* $f(G)$ *by the mapping* $gK \mapsto f(g)$ *for all* $gK \in G/K$.

   In terms of the reduction homomorphism $r\colon G \to G/K$*, there is a unique isomorphism* $\overline{f}\colon G/K \to f(G)$ *such that the diagram below commutes:* $f = \overline{f} \circ r$.



Examples

1. For fixed $g \in G$, conjugation by g is the function $f\colon G \to G$ by $f(x) = gxg^{-1}$. This is an isomorphism of G with itself.

2. When G is an *abelian* group, inversion $g \mapsto g^{-1}$ is an isomorphism of G with itself.

3. The exponential function $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ and the logarithm $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ are isomorphisms between $\mathbb{R}$ and $\mathbb{R}_{>0}$, and are inverses of each others.

4. Since $\det\colon \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism with kernel $\mathrm{SL}_2(\mathbb{R})$ and image $\mathbb{R}^\times$, because $a = \det\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times$ by the first isomorphism theorem.

5. The sign function $\mathrm{sign}\colon \mathbb{R}^\times \to \{\pm 1\}$ sending each non-zero real number x to its sign is a homomorphism that is surjective with kernel $\{x \in \mathbb{R}^\times : x > 0\} = \mathbb{R}_{>0}$, so $\mathbb{R}^\times/\mathbb{R}_{>0} \cong \{\pm 1\}$.

Non-examples

1. From Example 6 in Section 9, the subgroups H and N of S_4 are both isomorphic to $\mathbb{Z}_2^2$ but H is not normal in S_4 while N is normal in S_4.

2. For odd primes p, the Heisenberg group

$$\mathrm{Heis}(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

   is a non-abelian group of order p^3 in which all non-identity elements have order p. The group $\mathbb{Z}_p^3$ is an abelian group of order p^3 in which all non-identity elements have order p. Thus $\mathrm{Heis}(\mathbb{Z}_p)$ and $\mathbb{Z}_p^3$ have the same number of element of each order, but they are not isomorphic (one group is abelian and the other is not.)

3. The simplest reason two finite groups would not be isomorphic is that they don't have the same size. For prime p we will describe two finite groups of the same order built from $\mathrm{GL}_2(\mathbb{Z}_p)$, one a subgroup and the other a quotient group. Then we will determine whether or not the two groups are isomorphic.

   Subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. The first group is $\mathrm{SL}_2(\mathbb{Z}_p)$. The determinant $\det\colon \mathrm{GL}_2(\mathbb{Z}_p) \to U(p)$ is a homomorphism that is surjective (same proof as for real matrices) with kernel $\mathrm{SL}_2(\mathbb{Z}_p)$, so $\mathrm{GL}_2(\mathbb{Z}_p)/\mathrm{SL}_2(\mathbb{Z}_p) \cong U(p)$ by the first isomorphism theorem. Thus $|\mathrm{GL}_2(\mathbb{Z}_p)|/|\mathrm{SL}_2(\mathbb{Z}_p)| = |U(p)| = p-1$, so $|\mathrm{SL}_2(\mathbb{Z}_p)| = |\mathrm{GL}_2(\mathbb{Z}_p)|/(p-1)$.

   Quotient group of $\mathrm{GL}_2(\mathbb{Z}_p)$. The second group is $\mathrm{GL}_2(\mathbb{Z}_p)/Z$, where Z is the center of $\mathrm{GL}_2(\mathbb{Z}_p)$. The center is the scalar diagonal matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) = aI_2$ for non-zero a in $\mathbb{Z}_p$: such matrices are in the center, and conversely a matrix that commutes with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ is already scalar diagonal. Thus $|Z| = |\{aI_2 : a \in U(p)\}| = p-1$. The center is a normal subgroup and the quotient group $\mathrm{GL}_2(\mathbb{Z}_p)/Z$ has order $|\mathrm{GL}_2(\mathbb{Z}_p)|/(p-1)$, which matches the order of $\mathrm{SL}_2(\mathbb{Z}_p)$: even though we have not listed here exactly what the order *is*, we found the same formula for the order of $\mathrm{SL}_2(\mathbb{Z}_p)$ and $\mathrm{GL}_2(\mathbb{Z}_p)/Z$.

   Are these two groups isomorphic? To prove they are, we'd like to write down an isomorphism between them. To prove they are not isomorphic, we need to find some group-theoretic property that they do not share. Which way does it go?

   For odd primes p we will show $\mathrm{SL}_2(\mathbb{Z}_p)$ has a nontrivial center while $\mathrm{GL}_2(\mathbb{Z}_p)/Z$ has a trivial center, so they are *not* isomorphic.

   That $\mathrm{SL}_2(\mathbb{Z}_p)$ has a nontrivial center can be shown with an explicit example: $-I_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is in $\mathrm{SL}_2(\mathbb{Z}_p)$ and it's not the identity since $-1 \neq 1$ in $\mathbb{Z}_p$ (here is where we use $p \neq 2$). Since it is a scalar diagonal matrix, it commutes with all matrices in $\mathrm{SL}_2(\mathbb{Z}_p)$.

   To show $\mathrm{GL}_2(\mathbb{Z}_p)/Z$ is trivial, suppose in this group that $\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}$ lies in its center. That means $\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}\,\overline{A} = \overline{A}\,\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}$ for all $\overline{A} \in \mathrm{GL}_2(\mathbb{Z}_p)/Z$. We want to deduce that $\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}$ is trivial in $\mathrm{GL}_2(\mathbb{Z}_p)/Z$.

The condition $\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}\,\overline{A} = \overline{A}\,\overline{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)}$ means $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and A commute "modulo Z", which for $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ says

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}$$

for some non-zero x and y in $\mathbb{Z}_p$. These equations simplify to

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} x(a+c) & x(b+d) \\ xc & xd \end{pmatrix}, \quad \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix} = \begin{pmatrix} ay & by \\ (a+c)y & (b+d)y \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{Z}_p)$.

From the second row of the first equation we get $c = xc$ and $c+d = xd$. If $x \neq 1$ then $c = 0$ by the first equation, so the second equation becomes $d = xd$, so $d = 0$. But an invertible matrix can't have 2nd row (0 0), so $x \neq 1$. Arguing similarly with the second column of the second equation we get $b = by$ and $d = (b+d)y$; if $y \neq 1$ then $b = 0$, so $d = dy$, so $d = 0$, making the second column $\binom{0}{0}$, which is impossible. Thus $x = 1$ and $y = 1$, which makes the above equations

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}, \quad \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix} = \begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}.$$

From the first equation, $c = 0$ and $a = d$ in $\mathbb{Z}_p$. From the second equation, $b = 0$ and $a = d$ again. So $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, which is in Z, so our original matrix is trivial in $\mathrm{GL}_2(\mathbb{Z}_p)/Z$. That completes the proof that $\mathrm{GL}_2(\mathbb{Z}_p)/Z$ has a trivial center.

12 Direct products

Definitions and Theorems

1. **Theorem.** *Let G_1, G_2 be groups and let*

$$G = G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \text{ and } g_2 \in G_2\}.$$

Define a binary operation on G by

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Then G is a group with respect to this operation. The identity is (e_1, e_2) and the inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}).

2. The group $G = G_1 \times G_2$ in the previous theorem is called the (*external*) *direct product* of G_1 and G_2. This is a kind of "multiplication" of two groups. We start with G_1 and G_2, and build $G_1 \times G_2$. Inside $G_1 \times G_2$ are subgroups $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$, which are isomorphic to G_1 and G_2, respectively. Even if G_1 or G_2 is non-abelian, in $G_1 \times G_2$ the elements of G_1 commute with the elements of G_2: $(g_1, g_2) = (g_1, e_2)(e_1, g_2) = (e_1, g_2)(g_1, e_2)$.

3. The definition of direct products can be extended to more than two groups by induction, and $\prod_{i=1}^{n} G_i$ is used as a shorthand for $G_1 \times G_2 \times \cdots \times G_n$. If $G_1 = G_2 = \cdots = G_n = G$, then it is common to write G^n for $\underbrace{G \times \cdots \times G}_{n \text{ times}}$.

4. **Theorem** *Let $(g, h) \in G \times H$. If g and h have finite orders m and n respectively, then the order of (g, h) in $G \times H$ is the least common multiple of m and n.*

5. **Theorem** *The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if and only if* $\gcd(m, n) = 1$.

6. **Theorem**. *For groups G_1 and G_2, $G_1 \times G_2$ is abelian if and only if G_1 and G_2 are both abelian.*

7. **Theorem**. *If G_1 and G_2 are finite cyclic groups with relatively prime order then $G_1 \times G_2$ is cyclic.* (The converse is false, *e.g.*, $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 4 and no element has order 4.)

8. Reversing the construction of direct products (passing from "multiplication" to "factoring"), when is a group isomorphic to a direct product of two subgroups? Let G be a group with subgroups H and K satisfying the following conditions.

   - $G = HK = \{hk \colon h \in H, k \in K\}$
   - $H \cap K = \{e\}$
   - $hk = kh$ for all $k \in K$ and $h \in H$.

   Then $G \cong H \times K$, where an isomorphism $f \colon H \times K \to G$ is given by $f(h, k) = hk$. We say G is the (*internal*) *direct product* of its subgroups H and K.

Examples

- $\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n\text{m,times}}$ is a direct product of n copies of $\mathbb{R}$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_4$ are direct products of abelian groups that are not cyclic: the first has order 4 but each element has order 1 or 2, while the second has order 8 and each element has order dividing 4.
- $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic: $(1, 1)$ is a generator.
- $\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$ since each non-zero real number has a unique expression in the form $\pm x$ for some sign and some $x > 0$. This is an example of an internal direct product with $H = \{\pm 1\}$ and $K = \mathbb{R}_{>0}$.

Non-examples

- In the group D_n we have subgroups $H = \langle r \rangle = \{1, r, r^2, \ldots, r^{n-1}\}$ and $K = \langle s \rangle = \{1, s\}$ with $D_n = HK$ (each element of D_n is of the form r^i or $r^i s$ for some exponent i) and $H \cap K = \{1\}$, but that does *not* mean $D_n \cong H \times K$. Indeed, $H \times K = \langle r \rangle \times \langle s \rangle$ is abelian since H and K are both abelian, but D_n is non-abelian. What goes "wrong" here is that elements of D_n written in the form r^i or $r^i s$ do not multiply componentwise, *e.g.*, $(1s)(rs) \neq rs^2 = r$. In fact, $(1s)(rs) = r^{-1}ss = r^{n-1}$, which is not r. (More generally, $(r^i s)(r^j s) = r^{i-j}$, which is not usually $r^i r^j s^2 = r^{i+j}$.)

13 Finite Abelian Groups

Definitions and Theorems

1. **Theorem**. *If g and h commute and have finite order then $|gh| = |g||h|$ if $(|g|, |h|) = 1$.* There is no simple rule like this in general if $(|g|, |h|) \neq 1$.

2. **Fundamental Theorem of Finite Abelian Groups** *Every finite abelian group G is isomorphic to a direct product of cyclic groups of prime-power order: if $|G| > 1$ then*

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

   where the p_i's are prime numbers that are not necessarily distinct and each $\alpha_i \geq 1$.

3. **Theorem**. *If G is a finite abelian group and H is a cyclic subgroup of maximal order, then $G \cong H \times K$ for some subgroup K of G.*

Examples

1. Every finite abelian group of order 4 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_4$. Every cyclic group of order 4 is isomorphic to $\mathbb{Z}_4$ and the noncyclic abelian groups of order 4 are all isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. For example, $U(8) = \{1, 3, 5, 7 \bmod 8\}$ and $U(12) = \{1, 5, 7, 11 \bmod 12\}$ are both noncyclic of order 4 (each non-identity element has order 2), so $U(8)$ and $U(12)$ are both isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   An example of an isomorphism $f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to U(8)$ is $f(a, b) = 3^a 5^b \bmod 8$. This can be discovered from writing

$$U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{3} \cdot \overline{5}\} = \{\overline{1}, \overline{3}\} \cdot \{\overline{1}, \overline{5}\} = \langle \overline{3} \rangle \cdot \langle \overline{5} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

   An example of an isomorphism $f\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to U(12)$ is $f(a, b) = 5^a 7^b \bmod 12$.

2. Every finite abelian group of order 6 is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$, which is cyclic ($(1, 1)$ has order 6), so all finite abelian groups of order 6 are cyclic. For instance, $U(7)$ and $U(9)$ are both of order 6 and thus are cyclic. Explicitly, $U(7) = \langle 3 \bmod 7 \rangle$ and $U(9) = \langle 2 \bmod 9 \rangle$.

Non-examples

1. In the non-abelian group Q_8, $H = \langle i \rangle = \{1, i, -1, -i\}$ is a cyclic subgroup of maximal order and we can't write $Q_8 \cong H \times K$ for a subgroup K of Q_8: if we could then $|K| = 8/4 = 2$ so K must be $\{\pm 1\}$ since the only element of order 2 in Q_8 is -1, but H and $\{\pm 1\}$ don't intersect trivially (in fact $\{\pm 1\} \subset H$). Another problem is that H is abelian and K would have to be abelian (all groups of order 2 are cyclic and thus abelian), so $H \times K$ would be abelian but Q_8 is *not* abelian.

14 Group actions (and orbits)

Definitions and Theorems

1. Let X be a set and G be a group. A (*left*) *action* of G on X is a map $G \times X \to X$ given by $(g, x) \mapsto g \cdot x$ where

   - $e \cdot x = x$ for all $x \in X$,
   - $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $x \in X$ and g_1, g_2 in G.

2. Let X be a set on which G acts. For each $x \in X$, the *orbit* of x is defined to be

   $$\mathcal{O}_x = \{g \cdot x \colon g \in G\}.$$

   This is a subset of X. A *fixed point* for the group action is an $x \in X$ such that $g \cdot x = x$ for all $g \in G$. The fixed points are the $x \in X$ where $\mathcal{O}_x = \{x\}$ has size 1.

3. Let G be a group acting on the set X. For $x \in X$, its *stabilizer subgroup* in G is

   $$G_x = \{g \in G : g \cdot x = x\}.$$

   (More suggestive notation is Stab_x for G_x.) This is a subgroup of G.

4. **Theorem**. *Different orbits in a group action are disjoint.*

   If the orbit of x and the orbit of y in X overlap, say at z, then $z = g \cdot x$ and $z = g' \cdot y$ for some g and g' in G. Then $x = g^{-1} \cdot z = g^{-1} \cdot (g' \cdot y) = (g^{-1}g') \cdot y$, so everything in the orbit of x is in the orbit of y: for all $h \in G$, $h \cdot x = h \cdot ((g^{-1}g') \cdot y) = hg^{-1}g' \cdot y$ is in the orbit of y. A similar argument shows everything in the orbit of y is in the orbit of x, so the two orbits agree. Thus two orbits in a group action that are not equal have to be disjoint.

   This theorem generalizes the disjointness of different left cosets (and, separately, of right cosets) and the disjointness of different conjugacy classes, since those are both examples of orbits for a group action (Examples 6, 7 and 9 below).

5. **Theorem**. *If $y = g \cdot x$ for some $g \in G$ then $\{h \in G : y = h \cdot x\}$ is the left coset gG_x.*

6. **Theorem**. *If $y = g \cdot x$ for some $g \in G$ then $G_y = gG_xg^{-1}$, so stabilizer subgroups of different points in the same orbit are conjugate subgroups.*

7. **Theorem** (Orbit-stabilizer formula) *If G acts on X and $x \in X$, the elements in the orbit of x correspond to left cosets of the stabilizer G_x: $g \cdot x \longleftrightarrow gG_x$ for all $g \in G$. In particular, when G is finite*

   $$|\mathcal{O}_x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

8. **Theorem**. (Fixed-point congruence) *If G is a finite group with order equal to a power of a prime p then*

$$|X| \equiv |\mathrm{Fix}(X)| \bmod p,$$

where $\mathrm{Fix}(X)$ *is the set of fixed points for the group action.*

This theorem is useful in at least two ways: if $|X|$ is not divisible by p, the congruence shows $\mathrm{Fix}(X)$ is not empty, since its size is non-zero mod p and thus can't be 0, and also if $|X|$ is divisible by p and we know $\mathrm{Fix}(X)$ is not empty (so its size is greater than 0), we know $\mathrm{Fix}(X)$ has size at least p.

Examples

1. The group $G = S_n$ has a natural action on the set $X = \{1, 2, \ldots, n\}$ by permutations. The second group action axiom in this case says $\sigma(\tau(i)) = (\sigma\tau)(i)$ for $\sigma, \tau \in S_n$ and $1 \leq i \leq n$, which is how the product (composite function) $\sigma\tau = \sigma \circ \tau$ is defined. This action has a single orbit, because for any distinct $x, y \in X$, the transposition (xy) is an element in S_n sending x to y.

2. The group $\mathbb{R}$ acts on the set $\mathbb{R}$ by translations: $a \cdot x = x + a$. We have $0 \cdot x = x + 0 = x$ and $(a \cdot (b \cdot x)) = (x + b) + a = x + (a + b) = (a + b) \cdot x$.

3. The group $\mathbb{R}^\times$ acts on the set $\mathbb{R}$ by multiplications: $a \cdot x = ax$. We have $1 \cdot x = (1)(x) = x$ and $(a \cdot (b \cdot x)) = a(bx) = (ab)x = (ab) \cdot x$.

4. The group $\mathbb{R}^\times$ acts on the set $\mathbb{R}_{>0}$ by exponents: $a \cdot x = x^a$. We have $1 \cdot x = x^1 = x$ and $(a \cdot (b \cdot x)) = (x^b)^a = x^{ab} = ab \cdot x$.

5. The group $G = \mathrm{GL}_2(\mathbb{R})$ has a natural action on $X = \mathbb{R}^2$ by

$$A \cdot \mathbf{v} = A\mathbf{v}$$

for all $A \in \mathrm{GL}_2(\mathbb{R})$ and $\mathbf{v} \in \mathbb{R}^2$. The second group action axiom in this case says $A(B(\mathbf{v})) = (AB)(\mathbf{v})$ for $A, B \in \mathrm{GL}_2(\mathbb{R})$ and $\mathbf{v} \in \mathbb{R}^2$, which is one of the rules for how matrix multiplication works.

For each non-zero $\mathbf{v}$ in $\mathbb{R}^2$, its stabilizer subgroup in $\mathrm{GL}_2(\mathbb{R})$ is all $A \in \mathrm{GL}_2(\mathbb{R})$ such that $A\mathbf{v} = \mathbf{v}$: A has $\mathbf{v}$ as an eigenvector with eigenvalue 1. For example, if $\mathbf{v}$ is on the x-axis and not equal to $\mathbf{0}$ then for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$$A\mathbf{v} = \mathbf{v} \Longleftrightarrow A = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : d \neq 0 \right\}.$$

For $A \in \mathrm{GL}_2(\mathbb{R})$, its fixed point set $\{\mathbf{v} \in \mathbb{R}^2 : A\mathbf{v} = \mathbf{v}\}$ is the set of vectors in $\mathbb{R}^2$ that are eigenvectors of A with eigenvalue 1. If A does not have 1 as an eigenvalue then the only vector in $\mathbb{R}^n$ fixed by A is $\mathbf{0}$.

6. Let G be a group and H be a subgroup of G. Then the group H acts on the set $X = G$ by left multiplication:

$$h \cdot g = hg$$

for all $h \in H$ and $g \in G$. The H-orbit of g is $\{h \cdot g : h \in H\} = \{hg : h \in H\}$, which is the right coset Hg.

7. Let G be a group and H be a subgroup. We can describe left H-cosets in G as orbits of the group H acting on the set G by "right-inverse" multiplication: $g \cdot h = hg^{-1}$. (We need to multiply on the right by the inverse of g in order to have an action satisfying $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ in general.) The H-orbit of g is $\{h \cdot g : h \in H\} = \{gh^{-1} : h \in H\} = \{gh : h \in H\} = gH$.

8. Let $X = \mathbb{R}$ and $G = \mathbb{Z}$ and consider the group action $n \cdot x = n + x$ for all $n \in \mathbb{Z}$ and $x \in \mathbb{R}$. Since $\mathbb{Z}$ is a subgroup of $\mathbb{R}$ this group action can be seen as a special case of the action considered in Examples 6 and 7. The orbits for this action of $\mathbb{Z}$ on $\mathbb{R}$ are the cosets $x + \mathbb{Z}$ for $x \in \mathbb{R}$. All orbits are infinite, so this group action has no fixed points (no orbit has size 1).

9. Let G be a group. Then G acts on itself ($X = G$) by *conjugation*: for $g \in G$ and $x \in G$,

$$g \cdot x = gxg^{-1}$$

for all $g \in G$ and $x \in G$. The orbit of $x \in G$ is $\{gxg^{-1} : g \in G\}$, which is the conjugacy class of x. The stabilizer subgroup $G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$ is the *centralizer* of x in G, denoted as $Z(x)$. The set of fixed points for the conjugation action of G on itself is $\{x \in G : gx = xg \text{ for all } g \in G\}$, which is the center $Z(G)$.

By the orbit-stabilizer formula the conjugacy class of x, which is an orbit $\{gxg^{-1} : g \in G\}$ for the conjugation action of G on itself, has size $|G|/|Z(x)|$ where $Z(x) = \{g \in G : gx = xg\}$. If $\{x_1, \ldots, x_r\}$ represents the different conjugacy classes in G then

$$|G| = \sum_{i=1}^{k} |\mathcal{O}_{x_i}| = \sum_{i=1}^{r} \frac{|G|}{|Z(x_i)|},$$

which expresses $|G|$ as a sum of integers that are each factors of G.

The conjugacy classes of size 1 are the elements in the center $Z(G)$, and if we collect those counts of 1 together then the above equation becomes

$$|G| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|Z(x_i)|},$$

where $x_1, \ldots, x_k$ represent conjugacy classes of size greater than 1 and $Z(G) = \{x_{k+1}, \ldots, x_r\}$. This is called the *class equation* for G. For example, when $G = S_3$ its center is trivial and its other conjugacy classes are the three 2-cycles and the two 3-cycles. The class equation in this case says $6 = 1 + 3 + 2$. When $G = \mathbb{Z}_6$, the class equation says $6 = 6$.

10. Let G be a group. Then G acts on the set of its subgroups by *conjugation*: for $g \in G$ and a subgroup $H \subset G$,
$$g \cdot H = gHg^{-1}$$
for all $g \in G$ and $H \subset G$. The orbit of a subgroup H is $\{gHg^{-1} : g \in G\}$. The stabilizer subgroup of H is $\{g \in G : gHg^{-1} = H\}$, which is called the *normalizer* of H in G and written as $\mathrm{N}(H)$. The subgroup $\mathrm{N}(H)$ contains H and is the largest subgroup of G containing H and in which H looks normal.

11. Let $G = D_n = \langle r, s\rangle$ where s is reflection across the x-axis in $\mathbb{C}$ and r is rotation by $2\pi/n$ radians about the origin. If we let $X = \mathbb{C}$ then the n-th roots of unity can be considered as the vertices of a regular n-gon inscribed in the unit circle with center 0 and one vertex at 1. This inspires us to define the group action of D_n on $\mathbb{C}$ by
$$rz = (\cos(2\pi/n) + i\sin(2\pi/n))z \quad \text{and} \quad sz = \bar{z}.$$
Here multiplication by $\cos(2\pi/n) + i\sin(2\pi/n)$ is a counterclockwise rotation by $2\pi/n$ radians (this may be easiest to see if z is written in polar coordinates) and $\bar{z}$ is complex conjugation (reflection across the real axis).

    The transformations r and s can be described as 2×2 matrices:
$$r = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \text{ and } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$
This lets us view D_n as a subgroup of $\mathrm{GL}_2(\mathbb{R})$.

    The numbers fixed by s are those in $\mathbb{R}$ because real numbers are the only numbers fixed by complex conjugation and and the only fixed point of r is 0 because the only fixed point of a rotation in a plane is the center of the rotation. If x is a vertex of the regular n-gon then its stabilizer subgroup in D_n is a subgroup of order 2 generated by the line of reflection through x. If x is any other point on the regular n-gon then its stabilizer subgroup is trivial.

Non-examples

1. For a group G and subgroup H, right multiplication $h \cdot g = gh$ is usually not a group action of H on G since $(h_1 \cdot (h_2 \cdot g)) = gh_2h_1 = (h_2h_1) \cdot g$, which is usually not $(h_1h_2) \cdot g = gh_1h_2$.

2. Multiplication of $\mathbb{R}$ on $\mathbb{R}$, where $a \cdot x = ax$, is not a group action even though $(a \cdot (b \cdot x)) = ab \cdot x$, since the group $\mathbb{R}$ that is acting is a group under addition, not multiplication. The formula $a \cdot x = ax$ *is* a group action of $\mathbb{R}^\times$ on $\mathbb{R}$.

15 Cauchy's theorem and the Sylow theorems

Definitions and Theorems

1. **Cauchy's Theorem.** *Let G be a finite group and let p be a prime number such that p divides $|G|$. Then G contains a subgroup of order p.*

   Since subgroups of prime order are automatically cyclic, an equivalent formulation of Cauchy's theorem is that if p divides $|G|$ then G contains an element of order p. This theorem can be proved in two ways: (i) induct on $|G|$ and treat abelian and non-abelian groups separately, applying the class equation for the non-abelian case, (ii) look at solutions in G to the multivariable group equation $g_1 g_2 \cdots g_p = e$ and let $\mathbb{Z}_p$ act on these solutions by cyclic shifts.

2. A *p-subgroup* of G is a subgroup of G that has p-power size. Writing $|G| = p^k m$ where p does not divide m, a *Sylow p-subgroup* (also called a p-Sylow subgroup) of G is a subgroup of G with order p^k. (When p is not a factor of $|G|$ the Sylow p-subgroups of G are trivial.)

3. **First Sylow Theorem.** *Let G be a finite group and p be a prime. There is a Sylow p-subgroup of G: writing $|G| = p^k m$ where p does not divide m, G contains a subgroup of order p^k.*

   In fact if p^r is any power of p dividing $|G|$, not just the largest such power of p, then G has a subgroup of order p^r. Such nonmaximal p-subgroups in G do not fit the second and third Sylow theorems below.

4. **Second Sylow Theorem.** *Let G be a finite group and let p be a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P and Q are two Sylow p-subgroups of G, then there exists $g \in G$ such that $gPg^{-1} = Q$.*

   A consequence of the conjugacy of all Sylow p-subgroups of G, for a specific prime p, is that a Sylow p-subgroup P of G is a normal subgroup of G if and only if P is the only Sylow p-subgroup of G. This also shows all Sylow p-subgroups of a finite group are isomorphic to each other: if $Q = gPg^{-1}$, then conjugation by g is an isomorphism from P to Q.

5. **Third Sylow Theorem.** *Let G be a finite group and let p be a prime dividing $|G|$. Write $|G| = p^k m$, where $k \geq 0$ and m is not divisible by p. Then the number n_p of Sylow p-subgroups of G satisfies $n_p \equiv 1 \bmod p$ and $n_p \mid m$.* (While often not stated explicitly as part of the third Sylow theorem, in the course of proving it one can show $n_p = [G : \mathrm{N}(P)]$, where P is a Sylow p-subgroup and $\mathrm{N}(P)$ is its normalizer.)

The different parts of the Sylow theorems are proved by different group actions.

Examples

1. Let $G = S_n$ and let p be a prime dividing $n!$. Then p is a prime less than or equal to n, and an example of a permutation in S_n with order$p$ is the p-cycle $(12 \dots p)$. This illustrates Cauchy's theorem.

2. Let $G = D_n$, so $|G| = 2n$. If $p = 2$ then s has order 2. If p is an odd prime factor of $2n$ then $p \mid n$ and $r^{n/p}$ is an element of D_n with order p. This illustrates Cauchy's theorem.

3. Let G be a finite abelian group. Then by the Fundamental Theorem of Finite Abelian Groups, there is an isomorphism

$$G \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}),$$

   so $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. If p is a prime dividing $|G|$, then $p = p_i$ for some i. Under the isomorphism above, there is a subgroup H of G isomorphic to $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, so H is cyclic. If g is a generator of H, then $g^{p_i^{\alpha_i - 1}}$ is an element of G with order $p_i = p$. This illustrates Cauchy's theorem.

4. Let $G = S_3$. The order of $|G|$ is $6 = 2 \cdot 3$. Its Sylow 2-subgroups have order 2 and its Sylow 3-subgroups have order 3. By the third Sylow theorem, $n_2 \equiv 1 \bmod 2$ and $n_2 \mid 3$, while $n_3 \equiv 1 \bmod 3$ and $n_3 \bmod 2$. Therefore n_2 is 1 or 3 while $n_3 = 1$.

   There are three Sylow 2-subgroups of S_3: $\langle(12)\rangle$, $\langle(13)\rangle$ and $\langle(23)\rangle$, which are all conjugate to each other; that illustrates the 2nd Sylow theorem. The only Sylow 3-subgroup is $A_3 = \{(1), (123), (132)\}$, which is a normal subgroup of S_3.

5. We will use the Sylow theorems to show every group of order 15 is cyclic. Let $|G| = 15 = 3 \cdot 5$. A Sylow 3-subgroup of G has order 3 and a Sylow 5-subgroup of G has order 5. In G there is an element x with order 3 and element y with order 5 (Cauchy's theorem). Then $\langle x\rangle$ is a Sylow 3-subgroup and $\langle y\rangle$ is a Sylow 5-subgroup. By Sylow's third theorem, $n_3 \equiv 1 \bmod 3$ and $n_3 \mid 5$, so $n_3 = 1$. Also $n_5 \equiv 1 \bmod 5$ and $n_5 \mid 3$, so $n_5 = 1$. Hence $\langle x\rangle$ and $\langle y\rangle$ are both normal subgroups of G. Their intersection $\langle x\rangle \cap \langle y\rangle$ is trivial since this intersection is a subgroup with order dividing 3 and 5, hence of order 1.

   We show x and y commute. Consider $xyx^{-1}y^{-1}$. Writing this as $(xyx^{-1})y^{-1}$, it lies in $\langle y\rangle$ since $xyx^{-1} \in x\langle y\rangle x^{-1} = \langle y\rangle$ (the subgroup $\langle y\rangle$ is normal in G). Writing this as $x(yx^{-1}y^{-1})$, it lies in $\langle x\rangle$ since $yx^{-1}y^{-1} \in y\langle x^{-1}\rangle y^{-1} = \langle x\rangle$. Thus $xyx^{-1}y^{-1} \in \langle x\rangle \cap \langle y\rangle = \{e\}$, so $xyx^{-1}y^{-1} = e$, which means $xy = yx$. Hence $(xy)^i = x^i y^i$ for all integers i.

   The order of each element of G is 1, 3, 5, or 15. We don't have $(xy)^1 = e$, as otherwise $y = x^{-1}$ but the two sides have different orders. If $(xy)^3 = e$ then $x^3y^3 = e$, so $y^3 = e$, which is false (the order of y is 5). If $(xy)^5 = e$ then $x^5y^5 = e$, so $x^5 = e$, which is false (the order of x is 3, which doesn't divide 5). Hence the only option left is that xy has order 15, which implies $G = \langle xy\rangle$, which proves G is cyclic.

6. If $|G| = 100$ then a Sylow 2-subgroup has order 4 and a Sylow 5-subgroup has order 25 (and the Sylow p-subgroup of G for $p \neq 2, 5$ is trivial). By Sylow's third theorem, $n_5 \equiv 1 \bmod 5$ and $n_5 \mid 4$, so $n_5 = 1$: the Sylow 5-subgroup of G is normal. Also $n_2 \equiv 1 \bmod 2$ and $n_2 \mid 25$, so n_2 might be 1, 5, or 25. There is at least one group realizing each of the options for n_2:

   - if $G = \mathbb{Z}_{100}$ then $n_2 = 1$ (in an abelian group all subgroups are normal),

- if $G = D_5 \times \mathbb{Z}_{10}$ then $\langle s \rangle \times \langle 5 \bmod 10 \rangle = \{(1,0),(s,0),(1,5),(s,5)\}$ is a subgroup of order 4, hence is a Sylow 2-subgroup. Conjugating this subgroup (which leads to all other Sylow 2-subgroups of G), we get 4 additional subgroups by replacing s with the 4 other reflections in D_5. Thus $n_2 = 5$.
- if $G = D_5 \times D_5$ then each D_5 has 5 reflections, hence 5 subgroups of order 2, so in $D_5 \times D_5$ we can get Sylow 2-subgroups as $H \times K$ where H and K are subgroups of order 2 in D_5. Since H and K each have 5 options, the number of different subgroups $H \times K$ in G is $5^2 = 25$, so $n_2 \geq 25$. From $n_2 \in \{1, 5, 25\}$, we get $n_2 = 25$.

7. If $|G| = 24$ then a Sylow 2-subgroup has order 8 while a Sylow 3-subgroup has order 3 (and a Sylow p-subgroup for primes $p > 3$ is trivial). From the third Sylow theorem, $n_2 \equiv 1 \bmod 2$ and $n_2 \mid 3$, while $n_3 \equiv 1 \bmod 3$ and $n_3 \mid 8$. Thus $n_2 = 1$ or 3 while $n_3 = 1$ or 4. Below is a table of non-abelian groups of order 24 that we want to show are nonisomorphic. In the second column is a calculation of their centers, which for direct products uses the formula $Z(G \times H) = Z(G) \times Z(H)$.

G	$Z(G)$
S_4	$\{(1)\}$
D_{12}	$\{1, r^6\}$
$A_4 \times \mathbb{Z}_2$	$\{(1)\} \times \mathbb{Z}_2$
$Q_8 \times \mathbb{Z}_3$	$\{\pm 1\} \times \mathbb{Z}_3$
$D_4 \times \mathbb{Z}_3$	$\{1, r^2\} \times \mathbb{Z}_3$
$D_3 \times \mathbb{Z}_4$	$\{1\} \times \mathbb{Z}_4$
$D_3 \times \mathbb{Z}_2^2$	$\{1\} \times \mathbb{Z}_2^2$
$\mathrm{SL}_2(\mathbb{Z}_3)$	$\{\pm I_2\}$

Isomorphic groups must have isomorphic centers, so let's collect the groups based on the size of their center.

- Center of order 1: S_4.
- Center has order 2: D_{12}, $A_4 \times \mathbb{Z}_2$, and $\mathrm{SL}_2(\mathbb{Z}_3)$.
- Center of order 4: $D_3 \times \mathbb{Z}_4$ and $D_3 \times \mathbb{Z}_2^2$.
- Center of order 6: $Q_8 \times \mathbb{Z}_3$ and $D_4 \times \mathbb{Z}_3$.

Thus counting the size of the center distinguishes S_4 from the remaining groups. The groups $D_3 \times \mathbb{Z}_4$ and $D_3 \times \mathbb{Z}_2^2$ are not isomorphic because, even though their centers both have order 4, the centers are not isomorphic: the first group has a cyclic center and the second group has a noncyclic center.

To prove the remaining groups with center of equal size are not isomorphic, we look at their Sylow 2-subgroups: the Sylow p-subgroups of a group are conjugate to each other and thus are isomorphic to each other, so if two groups have nonisomorphic Sylow p-subgroups for some prime p, the groups can't be isomorphic to each other.

- It can be shown that D_{12} has $n_2 = 3$ while $A_4 \times \mathbb{Z}_2$ and $\mathrm{SL}_2(\mathbb{Z}_3)$ have $n_2 = 1$, so D_{12} is not isomorphic to $A_4 \times \mathbb{Z}_2$ or $\mathrm{SL}_2(\mathbb{Z}_3)$. The Sylow 2-subgroup of $A_4 \times \mathbb{Z}_2$ is $\{(1), (12)(34), (13)(24), (14)(23)\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^3$ and the Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$ is isomorphic to Q_8. Therefore $A_4 \times \mathbb{Z}_2$ and $\mathrm{SL}_2(\mathbb{Z}_3)$ are not isomorphic, since their Sylow 2-subgroups are not isomorphic.
- The groups $Q_8 \times \mathbb{Z}_3$ and $D_4 \times \mathbb{Z}_3$ both have $n_2 = 1$: a unique Sylow 2-subgroup. The Sylow 2-subgroup of $Q_8 \times \mathbb{Z}_3$ is $Q_8 \times \{0\} \cong Q_8$, and the Sylow 2-subgroup of $D_4 \times \mathbb{Z}_3$ is $D_4 \times \{0\} \cong D_4$. Since Q_8 and D_4 are not isomorphic (different number of elements of order 2), $Q_8 \times \mathbb{Z}_3$ and $D_4 \times \mathbb{Z}_3$ are not isomorphic.

Non-examples

1. In a group of order $75 = 3 \cdot 25$, subgroups of order 5 are not Sylow 5- subgroups: the Sylow 5-subgroups are those subgroups having maximal 5-power order, which is 25 rather than 5.
2. Not every element of a finite group is in some Sylow subgroup: only elements of prime-power order can be in one (and they are).