Sets, Groups and Knots
Course Notes
Math 101, Harvard University, Fall 1998, Spring 2000

Contents

1 Introduction . . . 1
   1.1 Overview with examples . . . 1
   1.2 Logic, proofs, basic concepts . . . 3
   1.3 Equivalence relations . . . 4
   1.4 Induction . . . 4
2 Set Theory . . . 5
   2.1 Basic axioms . . . 5
   2.2 Relations, functions and induction . . . 6
   2.3 Cardinality and the axiom of choice . . . 8
3 Group Theory . . . 12
   3.1 Examples of groups; isomorphisms . . . 12
   3.2 Cyclic groups and greatest common divisor . . . 18
   3.3 Symmetric groups and group actions . . . 22
   3.4 Geometric examples of groups . . . 29
   3.5 Abelian groups . . . 32
   3.6 Homomorphisms and factor groups . . . 35
   3.7 Generators and relations . . . 39
4 Knot Theory . . . 42
   4.1 Knots and links . . . 42
   4.2 Linking number and tricoloring . . . 44
   4.3 The fundamental group . . . 45
   4.4 Knot polynomials . . . 51
   4.5 Immersed spheres . . . 54
5 Summary . . . 55

1 Introduction

1.1 Overview with examples

1. Introduction to conceptual and axiomatic mathematics, the writing of proofs, mathematical culture, with sets, groups and knots as topics.

2. Set theory: we will learn how to count, and show there are different sizes of infinity.

3. Group theory: Symmetry without object.

   Examples: square; 8 symmetries, nonabelian. A cube has 6 faces, 8 vertices, 12 edges, 24 symmetries. Note that 6, 8, 12 divide 24: why? Dodecahedron: 12,20,30: 60. Rhombic dodecahedron: 12 faces, 24 edges, 14 vertices! 14 doesn't divide 24 — what's going on? Parallel parking. Slide puzzle.

4. Knot theory: magic trick for tying a trefoil. We will prove that this trick is impossible! Knots exist. Are there infinitely many knots?

5. Overview: sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}^*$, $\mathbb{Z}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$.

6. What is 3? What is a number? The size of a set; bijections or matchings. {Bill, Hillary and Chelsea}.

7. Infinite sets. (a) Not bijective to a natural number. (b) Contain a copy of all the natural numbers. (c) Bijective to a proper subset. Hilbert's Hotel.

8. The set of all natural numbers, all integers, all even numbers, etc. are all the same size.

9. Theorem: $|\mathbb{R}| > |\mathbb{Z}|$. Is there anything in between? This question has no answer! (It is *independent*.)

10. Groups. Comes from algebra: a set G where we can form $a \cdot b$, $1 \cdot a = a$, and there exist inverses: $a^{-1} \cdot a = 1$.

11. Examples:

    (a) $\mathbb{R}^*$, $\mathbb{Z}$. The integers under multiplication are *not* a group.

    (b) The symmetries of a triangle.

    (c) The advancing of a clock by one hour. $H^{12} = 1$. If we allow flipping the clock over, then $FH = H^{11} = H^{-1}$.

    (d) The symmetries of a cube.

    (e) Permutations of 4 objects, drawn as wiring diagrams. The inverse is the mirror image. There are 24 elements to this group.

(f) The cube also has 24 symmetries. It has 6 faces, 12 edges, 8 vertices. Is it an accident that these all divide 24?

(g) The rhombic dodecahedron has 24 symmetries too. But it has 12 faces, 24 edges and 14 vertices. How is the 14 possible? Aside: sphere packing and the rhombic dodecahedron as a Voronoi cell; compare honeycombs. Aside: 3-coloring the rhombic dodecahedron; 3-coloring the cube. Is there a regular solid that cannot be 3-colored? Yes: the tetrahedron.

12. Knots: the knot trick (tying an unknot into a trefoil). Is this possible? Can the trefoil be converted to a figure eight? How can you tell knots apart?

13. A group can be associated to a knot.

1.2 Logic, proofs, basic concepts

1. Truth table for AB, $A+B$, $\overline{A+B}$, $\overline{AB}$, $A \iff B$, $A \implies B$, $\overline{B} \implies \overline{A}$.

2. False $\implies$ anything. If $1+1=3$, then 15 is a prime number. If Clinton isn't a liar, then I'm a monkey's uncle, and 21 is also prime.

3. Contrapositive: example: if $n \in \mathbb{Z}$ is a square, then $n \geq 0$. Equivalently, if $n < 0$, then n is not a square.

4. Quantifiers: $(\forall x \in A)P(x)$; $(\exists x \in A)P(x)$. Examples: $\forall x \in \mathbb{R}, x^2 \geq 0$; $\forall i,j \in \mathbb{Z}, i+j = j+i$. Note: $\exists x \in \mathbb{R} \ : \ x^2 = 2$. Uniqueness is not asserted! (Sometimes people use $\exists! x$ for uniqueness.)

5. Negation of quantifiers: $\sim (\forall x)P(x)$ is the same as $(\exists x) \sim P(x)$; similarly for $\exists$.

6. Example: $\forall x \in \mathbb{R} \exists y \in \mathbb{R} \ : \ xy = 1$. False (correct if we use $\mathbb{R}^*$). As it stands, negation is true: $(\exists x \ : \ \forall y) xy \neq 1$. In fact, just take $x = 0$.

7. General principle: to establish "If A then B", or "For all x satisfying A, we have B", you must give a proof. To *disprove* a statement of that type, you must give a *counterexample*. (E.g. $x = 0$ above.)

8. Common linguistic fallacies: All aspirin is not alike. Everyone can't be number one.

1.3 Equivalence relations

1. Ordered pairs and the product $A \times B$. Relations.

2. Equivalence relations: the same thing can have many names. Example on $\mathbb{Z}$: $a \sim b$ if $a - b$ is even.

3. The definition of $\mathbb{Q}$ by an equivalence relation.

4. The definition of $\mathbb{Z}/10$. This forms a group under addition. What about under multiplication?

5. Equivalence relation: what is the rule behind the sequence 8, 5, 4, 9, 1, 7, 6, 10, 3, 2, 0? (Alphabetical order). Consider equivalence relation on the numbers $0 - 10$ of having the same first letter. It can be represented as a directed graph: an arrow from a to b means $(a, b) \in R$.

6. Equivalence relations and sets that are not well-defined. Examples:

   $\{x \in \mathbb{Z}/10 \ : \ x$ is prime.$\}$ (Not well defined)
   $\{x \in \mathbb{Z}/10 \ : \ x$ can be represented by a prime.$\}$ (1,2,3,5,7,9)
   $\{x \in \mathbb{Z}/10 \ : \ x$ can be represented by infinitely many primes.$\}$ (1,3,7,9)

   The last is an important statement in number theory!

1.4 Induction

1. Principle of induction: if $S \subset \mathbb{Z}^+$ satisfies $1 \in S$ and $n \in S \implies (n+1) \in S$, then $S = \mathbb{Z}^+$.

2. Examples:

   $1 + 2 + \cdots + n = n(n+1)/2$.
   Every $n > 1$ is a product of primes.
   If $|X| = n$ then $|\mathcal{P}(X)| = 2^n$.

3. Prove by induction that people can live arbitrarily long: let $P(n)$ be the assertion: it is possible to live n microseconds.

4. The job interview: each candidates holds a playing card to his forehead, so the others can see it but he cannot. The candidates must call out as soon as they can deduce that the card they hold is the ace of spaces. But in fact all the cards are aces of spades! What happens?

2 Set Theory

2.1 Basic axioms

1. Axiom I. (Extension) A set is determined by its elements.

2. From extension we can *prove* $A = B \,\&\, B = C \implies A = C$. We can also define $A \subset B$. Is $A \sim B$ if $A \subset B$ an equivalence relation? It's symmetric and transitive... but not reflexive.

3. Axiom II. (Specification) If A is a set then $\{x \in A \ : \ P(x)\}$ is also a set.

4. Examples: $A \cap B = \{x \in A \ : \ x \in B\}$. $A - B = \{x \in A \ : \ x \notin B\}$. $\mathbb{R} - \mathbb{Q} =$ irrationals; $\mathbb{Q} - \mathbb{R} = \emptyset$.

$$\{x \in \mathbb{Z} \ : \ \exists y \in \mathbb{Z}, y + y = x\} = \text{even numbers.}$$
$$\{x \in \mathbb{Z} \ : \ x/n \in \mathbb{Z} \, \forall n > 0\} = \{0\}.$$
$$\{x \in \mathbb{Z} \ : \ x^2 < 0\} = \emptyset.$$

5. Discussion: The Barber of Seville; Russell's paradox. If $X = \{A \ : \ A \notin A\}$, is $X \in X$? There is no universe: given a set A, set $X = \{B \in A \ : \ B \notin B\}$. We claim $X \notin A$. Indeed, if $X \in A$, then $X \in X$ iff $X \notin X$.

6. Now assume at least one set A exists; then we can form

$$0 = \emptyset = \{x \in A \ : \ x \neq x\},$$

but nothing else for sure. (E.g. A might be $\emptyset$.)

7. Axiom III. (Pairs) If A and B are sets then so is $\{A, B\}$. From this axiom and $\emptyset = 0$, we can now form $\{0,0\} = \{0\}$, which we call 1; and we can form $\{0,1\}$, which we call 2; but we cannot yet form $\{0,1,2\}$.

8. Axiom IV. (Unions) If A is a set, then $\bigcup A = \{x \ : \ \exists B, B \in A \ \& \ x \in B\}$ is also a set. From this axiom and that of pairs we can form $\bigcup\{A, B\} = A \cup B$. Thus we can define $x^+ = x + 1 = x \cup \{x\}$, and form, for example, $7 = \{0,1,2,3,4,5,6\}$.

9. Intersections. If $A \neq \emptyset$, we can define $\bigcap A = \{x \ : \ \forall B \in A, x \in B\}$. Since A has at least one element B_0, we have $\bigcap A \subset B_0$ and thus the intersection is a set. Note: $\bigcap \emptyset$ is undefined!

   Examples: $\bigcap\{A\} = A$, $\bigcap\{A, B\} = A \cap B$.

10. Axiom V. (Powers) If A is a set, then $\{B \ : \ B \subset A\}$ is also a set.

11. Examples: $X = \{B \in \mathcal{P}(52) \quad : \quad B \text{ has example 5 elements}\}$ is the number of possible poker hands. $|X| = 2,598,960$.

    Pascal's triangle. The subsets with $k+1$ elements of $\{1, \ldots, n\}$ can be partitioned into those that include n and those that do not. Thus $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

12. Axiom VI. (Infinity) There exists a set A such that $0 \in A$ and $x + 1 \in A$ whenever $x \in A$. The smallest such set is unique, and we call it $\mathbb{N} = \{0,1,2,3,\ldots\}$.

13. A kindly mathematician uncle asks his niece, "What's the highest number you know?" The niece replies, "168,000,000". The uncle asks, "But what about 168,000,001"? And the niece replies, "I was close, wasn't I?" (Hubbard)

14. We can now define, for $i, j \in \mathbb{N}$, $i < j$ iff $i \in j$. What is $i \cap j$? $i \cup j$?

2.2 Relations, functions and induction

1. Ordered pairs: $(a, b) = \{\{a\}, \{a, b\}\}$. Then $(a, b) = (a', b')$ iff $a = a'$ and $b = b'$. By definition, $A \times B = \{(a, b) \ : \ a \in A, b \in B\}$. Note that $A \times B \subset \mathcal{P}(\mathcal{P}(A \cup B))$, so it is a set.

2. Set theory as a programming language. The point of the definitions of $\mathbb{N}$ and (a, b) is not so much that they are natural or canonical, but that they work. In other words set theory provides a very simple language in which the rest of mathematics can be *implemented.*

3. A *relation* R between A and B is a subset $R \subset A \times B$. It has a *domain* and *range.*

   A relation can be visualized as a directed graph with vertices $A \cup B$ and with an edge from a to b exactly when $(a, b) \in \mathbb{R}$.

4. Examples: an equivalence relation is a subset of $A \times A$ with certain properties. The relation $i < j$ on $\mathbb{Z}$. The relation $b|a$ on $\{1, 2, \ldots, 10\}$.

5. A *function* $f : A \to B$ is a relation between A and B such that for each $a \in A$, there is a unique b such that $(a, b) \in f$. We write this as $b = f(a)$. Functions are also called *maps.*

6. The set of all $f : A \to B$ is denoted B^A. Why? How many elements does 3^5 have? (Answer: 243.)

7. A function can be *injective* and/or *surjective.* It is *bijective* if both.

8. Composition of maps: $f \circ g$. If $f : A \to B$ is bijective, then there is a unique map $g : B \to A$ such that $g \circ f(x) = x \, \forall x \in A$.

9. Examples: $f(i) = i^2$ is injective on $\mathbb{N}$, but not on $\mathbb{Z}$. It is surjective in neither case. The function $\sin : \mathbb{R} \to [-1, 1]$ is surjective but not injective. Its restriction, $\sin : [-\pi/2, \pi/2] \to [0, 1]$, is bijective. Its restriction, $\sin : [0, 1] \to [-1, 1]$, is injective but not surjective.

10. There is a natural bijection between $A \times A$ and A^2.

11. There is a natural bijection between $\mathcal{P}(A)$ and 2^A.

12. Functions, unions and intersections. Let $f : X \to Y$ be a function. We set $f(A) = \{f(a) \ : \ a \in A\}$. In this way we obtain a map $f : \mathcal{P}(X) \to \mathcal{P}(Y)$.

    In general, $f(A \cap B) \neq f(A) \cap f(B)$. We only have $f(A \cap B) \subset f(A) \cap f(B)$. However, if f is *injective*, then equality holds. We always have, however, $f(A \cup B) = f(A) \cup f(B)$.

13. If $f : A \to B$ is a function, for any subset $X \subset B$ we define $f^{-1}(X) = \{a \in A : f(a) \in X\}$. Thus we have $f^{-1} : \mathcal{P}(B) \to \mathcal{P}(A)$. This map preserves intersection and unions: e.g. $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.

    Abusing notation, one also writes $f^{-1}(b)$ for $f^{-1}(\{b\})$.

2.3 Cardinality and the axiom of choice

1. *Cardinality.* We say sets A and B have the same *cardinality* if there is a bijection between A and B. We will write this relation as $|A| = |B|$. It is an equivalence relation.

2. Theorem. $|\mathbb{N}| \neq |\mathbb{R}|$. Proof. If we had a list of all real numbers, $(r_1, r_2, r_3, \ldots)$, we could make a new real numbers s whose ith digit satisfies $(s)_i \neq (r_i)_i$. Then s is not on the list!

3. Theorem (Cantor). A and $\mathcal{P}(A)$ do not have the same cardinality.

    Proof. Given $f : A \to \mathcal{P}(A)$, let $B = \{a : a \notin f(a)\}$. Suppose $B = f(a)$. Then $a \in B$ iff $a \notin B$. By the same method one proves there is no list of all real numbers.

4. Corollary. There are many different sizes of infinity.

5. Exercise: $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. Thus the real numbers are an example of the 'second kind' of infinity, the continuum. (The proof is best given using the Schröder-Bernstein theorem, to be presented below).

6. If we think of $\mathcal{P}(\mathbb{N}) \cong 2^{\mathbb{N}}$ as sequences (a_i) of binary digits, then the proof that $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$ is almost the same as digit diagonalization.

7. *Finite and infinite sets.* A set A is *finite* iff there is a bijection $f : A \to n$ for some $n \in \mathbb{N}$. That is, A is finite iff $|A| = |n|$ for some $n \in \mathbb{N}$.

8. A set is *infinite* iff it is not finite.

    Theorem. $\mathbb{N}$ is infinite. Proof. Otherwise, there would for some n be an injective map $\mathbb{N} \hookrightarrow n$, and hence an injective map $n + 1 \hookrightarrow n$. But we can prove by induction on n that no such map exists.

9. Theorem (Pigeon-hole principle). If A is finite, then any injective map $f : A \to A$ is surjective.

    Proof. By induction on $|A| = n$.

10. Application: for any prime p and $a \neq 0$, there is an integer b such that $ab = 1 \bmod p$. (I.e. $b = 1/a$).

    Proof: the map $b \mapsto ab$ is $1 - 1$ on $\mathbb{Z}/p$, so it is onto.

    Example: $1/10 = 12 \bmod 17$; in fact $10 * 12 = 120 = 7 * 17 + 1$.

11. (Cantor's definition of infinity) A set A is infinite iff there exists a map $f : A \to A$ which is injective but not surjective.

    (Every infinite set is a Hilbert's hotel). The proof uses a new axiom.

12. Axiom VII (The Axiom of Choice): For any set A there is a function $c : \mathcal{P}(A) - \{\emptyset\} \to A$, such that $c(B) \in B$ for all $B \subset A$.

13. Theorem: A is infinite iff there is an injective map $f : \mathbb{N} \to A$.

    Proof: If A is finite then any subset of A is finite, so there is no injection of $\mathbb{N}$ into A.

    Now assume A is infinite; we will construct f. Pick some $a \in A$. Then define, by induction, $f(0) = a$ and $f(n+1) = c(A - \{f(0), \dots, f(n)\})$. The resulting map is injective by construction.

14. Proof of Cantor's definition. Suppose A is infinite. Find a sequence a_i in A and define $f(a_i) = a_{i+1}$, $f(x) = x$ otherwise. Then f is 1-1 but its image omits a_0.

15. *Inverses:* Another application of AC. For any surjective map $f : X \to Y$, there is a map $g : Y \to X$ such that $g(f(x)) = x$. Proof. Let $g(y) = c(f^{-1}(y))$, where c is a choice function for $\mathcal{P}(X)$.

16. The Banach-Tarski paradox. As a consequence of AC, you can cut a grapefruit into 5 pieces and reassemble them by rigid motions to form 2 grapefruits. (Now you've gone too far.)

17. *Relative size.* Let us say $|A| \leq |B|$ if

    (1) there is an injection $f : A \hookrightarrow B$; or
    (2) there is a surjection $g : B \twoheadrightarrow A$, or $A = \emptyset$.

    Theorem: (1) and (2) are equivalent.

    Proof: given the inclusion f we obtain from f^{-1} a surjection from $f(A)$ back to A, which we can extend to the rest of B as a constant map so long as $A \neq \emptyset$. Conversely, using the Axiom of Choice, we take f to be a section of g, i.e. set $f(a) = c(g^{-1}(\{a\}))$.

18. *The Schröder-Bernstein theorem.* If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

    Proof. We will assume A and B are disjoint — this can always be achieved, if necessary, by replacing A, B with $A \times \{0\}, B \times \{1\}$.

    Suppose we have injections $f : A \to B$ and $g : B \to A$. Then we obtain an injection
    $$F = f \cup g : A \to B.$$

    To clarify the proof, say $F(x)$ is the *child* of x, and x is the *parent* of $F(x)$. Since F is injective, a child can have only one parent, and every element of $A \cup B$ is a parent. However some parents are no-one's child; let us call them *godfathers.*

    For any $x \in A \cup B$, either x is descended from a unique godfather (possibly x itself), or x has no godfather; it has an infinite line of ancestors (or x is descended from itself.)

    Now partition A into 3 pieces, A_0, A_A and A_B. A_0 is the elements $x \in A$ with no godfather; A_A consists of those x whose godfather is in A; and A_B is those whose godfather is in B. Similarly define B_0, B_A, B_B.

    There is a bijection $A_0 \leftrightarrow B_0$ defined by sending a to its child $F(a)$. It is injective because F is, and it is surjective because every $x \in B_0$ has a parent, which must lie in A_0.

    There is a bijection $A_A \leftrightarrow B_A$ defined by sending each $a \in A_A$ to its child $F(a)$. The inverse map sends children to their parents. There are no godfathers in B_A, so the inverse is well-defined.

    Similarly there is a bijection $A_B \leftrightarrow B_B$, sending $a \in A$ to its parent in B_B. Putting these three bijections together shows $|A| = |B|$.

19. Countable sets. We say A is countable if $|A| \leq \mathbb{N}$. Finite sets are countable.

20. If A is countable and infinite, then $|A| = |\mathbb{N}|$. Proof. Infinite implies $|\mathbb{N}| \leq |A|$, and countable implies $|A| \leq |\mathbb{N}|$; apply SB.

21. The set of things that can be described in words is countable. Thus most real numbers have no names.

22. The integers $\mathbb{Z}$ can be constructed from $2 \times \mathbb{N}$; they satisfy $|\mathbb{Z}| = |\mathbb{N}|$.

23. The rationals $\mathbb{Q}$ are $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^*/\sim$, where $(a,b) \sim (c,d)$ if $ad - bc = 0$.

24. The real numbers $\mathbb{R}$ as Dedekind cuts: $\mathbb{R}$ is the set of ordered partitions (A, B) of $\mathbb{Q}$ such that $a < b$ for every $a \in A$ and $b \in B$, with the convention that B has no least element.

    Example: $\sqrt{2} = (A, B)$ where A is the union of the negative rationals and all those with $q^2 < 2$, and B is the subset of positive rationals with $q^2 > 2$.

25. Theorem. If $x_1 < x_2 < \ldots < M$ is an increasing sequence of real numbers, then there is a real number y such that $x_n \to y$.

    Proof. Using Dedekind cuts, write $x_i = (A_i, B_i)$, and set $y = (A, B)$ where $A = \bigcup A_i$ and $B = \bigcap B_i$. The upper bound insures that $B \neq \emptyset$. ■

    Example: when we write $\pi = 3.141592\ldots$, we are describing a real number as a limit of rational numbers.

26. Theorem. $\mathbb{N}^2$ is countable. Proof. Define a bijection $f : \mathbb{N} \to \mathbb{N}^2$ by $f(n) = (a, b)$ where $n + 1 = 2^a(2b + 1)$.

    Cor. $\mathbb{Z} \times \mathbb{Z}$ is countable.

27. Theorem. $\mathbb{Q}$ is countable. Proof. We have

$$|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}^*| \leq |\mathbb{Z}^2| = |\mathbb{N}^2| = |\mathbb{N}|.$$

28. Corollary. Most real numbers are irrational.

29. Example: $\sqrt{2}$ is irrational. If it had a rational square root, we could write it in lowest terms as p/q. But then $p^2 = 2q^2$ implies both p and q are even.

30. Corollary. In fact, most real numbers are transcendental. (This means x satisfies no polynomial equation with integral coefficients.)

31. Theorem: $|\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$. Thus the functions on $\mathbb{R}$ represent the third kind of infinity.

To prove this, first notice that we have the easy inequality:

$$|\mathcal{P}(\mathcal{P}(\mathbb{N}))| = |\mathcal{P}(\mathbb{R})| = |2^{\mathbb{R}}| \leq |\mathbb{R}^{\mathbb{R}}|.$$

On the other hand, we can construct an injection $i : \mathbb{R}^2 \to \mathbb{R}$ by interleaving decimal digits. Since a function $f : \mathbb{R} \to \mathbb{R}$ is a special kind of relation $f \subset \mathbb{R} \times \mathbb{R}$, we then have:

$$|\mathbb{R}^{\mathbb{R}}| \leq |\mathcal{P}(\mathbb{R}^2)| = |\mathcal{P}(\mathbb{R})|,$$

and so $|\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$ by the Schröder-Bernstein theorem.

32. Another way to think of the fact that $|\mathbb{R}^2| = |\mathbb{R}|$ is that $|\mathbb{N} \times 2| = |\mathbb{N}|$, and thus

$$|\mathbb{R}^2| = |\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N} \times 2)| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|.$$

33. Using the Axiom of Choice, one can prove that for any two sets A and B, $|A| \leq |B|$ or $|B| \leq |A|$.

34. *The continuum hypothesis.* Is there a set A such that $|\mathbb{N}| < |A| < |2^{\mathbb{N}}|$? It is now known that this question *cannot be answered* using the axioms of set theory (assuming these axioms are themselves consistent).

3 Group Theory

3.1 Examples of groups; isomorphisms

1. A *group* $\langle G, * \rangle$ is a set G together with a map $* : G \times G \to G$, sending each *ordered* pair of elements (a, b) from G to its *product* $a * b \in G$. The following axioms must be satisfied:

   (a) There exists an *identity element* $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.

   (b) For every $a \in G$ there exists an *inverse* $a' \in G$ such that $a * a' = a' * a = e$.

(c) The product is associative: for all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.

2. Theorem. The identity and inverse are unique.

   Proof. If e and e' are both identities, then $e = e * e' = e'$, since they are both right and left identities. Similarly, if a' and a'' are inverses of a, then by associativity we have

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

3. Theorem. The equation $a * x = b$ has a unique solution x in a group G.

   Proof. We have $a'(a * x) = a' * b = x$.

4. First examples. Consider $G = \mathbb{Z}$ with the following operations.

   (a) $a * b = a + b$. This is a group.

   (b) $a * b = ab$. Not a group (most elements have no inverse).

   (c) $a * b = ab/2$. Not a group ($ab/2 \notin \mathbb{Z}$). One says G is not *closed* under the group operation.

   (d) $a * b = a + b - 2$. This is a group! We have $e = 2$, $a' = 4 - a$.

   (e) $a*b = ab+1$. This is not associative. We have $(a*b)*c = abc+c+1$, while $a * (b * c) = abc + a + 1$.

5. The group $\mathbb{Z}/n = \{0, 1, 2, \ldots, n - 1\}$. We define $a * b = a + b \bmod n$. That is, we form the sum and take the remainder after division by n.

   In this group, $a' = n - a$.

6. *Casting out nines.* You can take any whole number and reduce it $\bmod n$. This gives a map $\mathbb{Z} \to \mathbb{Z}/n$ compatible with addition.

   Now notice that $1 = 10 = 100 = \ldots = 1 \bmod 9$. Thus reduction $\bmod 9$ is the same as adding up the digits. This is the famous trick of 'casting out nines' to check arithmetic.

   Example: We are all familiar with the fact that the 2-digit multiples of 9 add up 9: 18, 27, ...81. Similarly, 522 is divisible by 9; 741 is divisible by 3, as is 174 and 147.

7. Finite examples. Consider $G = \{0, 1, 2, 3, 4\}$.

   (a) $a * b = a + b \bmod 5$. This is a group.

   (b) $a * b = ab$. This is not a group; the identity is 1, but $0 * a = 0$ for all a.

   (c) $\langle (\mathbb{Z}/5) - \{0\}, a * b = ab \rangle$. This is a group; $2 * 3 = 1$, $4 * 4 = 1$, $1 * 1 = 1$.

   (d) $\langle (\mathbb{Z}/10) - \{0\}, a * b = ab \rangle$. This is not a group; $2 * 5 = 10 = 0$ is not in G.

   (e) Theorem. If we let $G = (\mathbb{Z}/n)^*$ consists of those residue classes a such that $(a, n) = 1$, then G forms a group under multiplication. In particular $(\mathbb{Z}/p) - \{0\}$ is a multiplicative group for any prime p.

8. *Continuous examples.* The groups $\mathbb{R}$, $\mathbb{R}^n$, $\mathbb{R}^*$, $\mathbb{C}$, $\mathbb{C}^*$. Groups of matrices.

9. *Commutative groups.* A group is *commutative* if $a * b = b * a$ for all $a, b \in G$. All the groups we have seen so far are commutative. But not all groups are commutative.

   One also says such groups are *abelian.* (What's purple and commutes?)

10. *Symmetric groups.* For any set A, let $S(A)$ be the set of all bijections $f : A \to A$, with the group law $f * g = f \circ g$. Then $S(A)$ is a group.

11. Now consider $S(\mathbb{R})$. Let $f(x) = x+1$, $g(x) = 2x$. Then $f \circ g(x) = 2x+1$, while $g \circ f(x) = 2x + 2$. Thus $f * g \neq g * f$. (On the other hand, $g * h = h * g$ if $h(x) = x + t$, and $f * h = h * f$ if $h(x) = ax$, $a \neq 0$.)

12. Example: $S_n = S(n)$, $n \in \mathbb{N}$. For $n = 3$ this group is not commutative. It can be thought of as the symmetries of a triangle with vertices $\{0, 1, 2\}$. Then the element 'flip', $f = (12)$, and the element 'rotate', $r = (012)$, do not commute. Indeed, $r(f(0)) = r(0) = 1$, but $f(r(0)) = f(1) = 2$, and thus $f * r \neq r * f$.

    Cor: S_n is non-commutative for $n \geq 3$.

13. Theorem. In any group G, $(a * b)' = b' * a'$.

    Proof. $(a * b) * (b' * a') = a * (b * b') * a' = a * e * e' = a * a' = e$.

The order is important in a non-commutative group!

14. What about S_2? This group just has two elements, $\langle e, a\rangle$, and $a*a = e$. What about S_1? This is the *trivial group*, with just the identity map. What about $S_0 = S(\emptyset)$?! This is also trivial — and nonempty!

15. *Table of a group.* List the elements of $S(3)$ as e, r, r^2, f, rf, r^2. Then make a table where the (a, b)-entry is $a * b$. This can be done using the basic observations $fr = r^2 f$ and $f^2 = r^3 = e$ coming from symmetries of a triangle.

    A couple of useful principles. (i) The first row and column are copies of the edges of the table. (ii) Every row and every column lists a permutation of the group.

    Note that commutativity corresponds to symmetry of the table. Note that e's on the diagonal tell you the elements that satisfy $a = a'$.

16. *Order of an element.* For any element $a \in G$, we let $a^i = a * a * \cdots a$, the product with i terms, if $i > 0$; $a^0 = e$; $a^{-i} = (a^i)'$.

    Then $a^i a^j = a^{i+j}$. The *order* of a is the least $n > 0$ such that $a^n = e$, or infinity if no such n exists.

17. Theorem. If a has finite order n, the $a' = a^{n-1}$.

18. Examples.

    (a) In $\mathbb{Z}/10$, $\text{ord}(0) = 1$, $\text{ord}(1) = 10$, $\text{ord}(2) = 5$, $\text{ord}(3) = 10$, $\text{ord}(4) = 5$, $\text{ord}(5) = 2$.

    (b) In S_3, the element $r = (012)$ has order 3; the element $f = (12)$ has order 2; the identity has order 1.

    (c) In $\mathbb{R}$, every element other than 0 has infinite order. In $\mathbb{R}^*$, 1 has order 1, -1 has order 2, and every other element has infinite order.

19. *Isomorphism.* Two groups $\langle G, *\rangle$ and $\langle H, \#\rangle$ are *isomorphic* if there is a bijection $f : G \to H$ such that $f(a * b) = f(a)\#f(b)$.

    One of the *main problems* in group theory is to classify groups up to isomorphism.

20. *Order of a group.* The order of G is its number of elements, $|G|$. Clearly if $G \cong H$ then $|G| = |H|$.

21. Example: $\mathbb{Z}/2$ and S_2 are isomorphic.

    Example: $\mathbb{Z}/6$ and S_3 both have order 6, but they are *not* isomorphic. Because $\mathbb{Z}/6$ is commutative, but S_3 is not! Or, because $\mathbb{Z}/6$ has an element of order 6, but S_3 does not.

22. Theorem. Any two groups of order one are isomorphic.

    Proof. Define $f : G_1 \to G_2$ by $f(e) = e$.

23. Theorem. Any group G of order two is isomorphic to $\mathbb{Z}/2$.

    Proof. We can write $G = \langle e, a\rangle$ and the only question is, what is $a * a$? But it must be e, since a needs an inverse.

24. Theorem. Any group G of order three is isomorphic to $\mathbb{Z}/3$.

    Proof. We can write $G = \langle e, a, b\rangle$, and start filling in the group table. What goes in position (a, b)? It can't be a, because there's already an a in that row, and it can't be b, because there's a b in that column! So it must be e. Similarly $b * a = e$ and we quickly see $a^3 = e$ and $G \cong \mathbb{Z}/3$.

25. *Complex numbers.* Recall that $i^2 = -1$, $(a + ib)(c + id) = (ac - bd) + i(bc + ad)$. Thus $G = \{1, i, -1, -i\}$ forms a subgroup of $\mathbb{C}^*$ isomorphic to $\mathbb{Z}/4$.

    We also have $e^{i\theta} = \cos\theta + i\sin\theta$, the unit vector at angle θ. Since $e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}$, we see (a) all nth roots of unity are of the form $e^{2\pi ik/n}$; and (b) altogether these form a cyclic group U_n.

26. An abelian group that is not cyclic: the Klein 4-group, $V_4 \cong \mathbb{Z}/2\times\mathbb{Z}/2$.

27. Theorem. The only groups of order 4 are (up to isomorphism) the Klein 4-group, V_4, and $\mathbb{Z}/4$.

    Proof. Every element has order 2, 3 or 4. Suppose there is an element of order 4; then we have $\mathbb{Z}/4$. Suppose 3 is the maximal order. Then the group is $\langle e, a, a^2, a^3, b\rangle$, but what is ab? It must be a power of a, contradiction. So finally we can assume every element has order two. Then the group table is easy to complete, and we find the group is V_4.

28. *Subgroups.* Let $H \subset G$ be a subset of a group $\langle G, *\rangle$. Then H is a *subgroup* of G if (a) $*(H \times H) \subset H$ and (b) $\langle H, *|H \times H\rangle$ is a group.

Part (a) say H is *closed* under the product $*$.

29. *Trivial subgroups.* We always have $H = \{e\}$ and $H = G$ as subgroups of G. The first is called the *trivial* group.

30. Theorem. Let H be a subset of G. Then H is a subgroup iff

    (a) $e \in H$;

    (b) $a, b \in H \implies a * b \in H$; and

    (c) $a \in H \implies a' \in H$.

    Proof. Just check: (0) we have $*(H \times H) \subset H$; and (1) identity exists, (2) inverses exist; and (3) associativity is inherited.

31. Examples: $\mathbb{Q} \subset \mathbb{R}$; $\mathbb{N} \subset \mathbb{Z}$; $\mathbb{R}^2 \subset \mathbb{R}^3$; $\{1, i, -1, -i\} \subset \mathbb{C}^*$.

    Examples: $\mathbb{Q}^+ \subset \mathbb{R}^*$ and $\subset \mathbb{R}$. $\{a + b\sqrt{2} \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{R}$. $\{3^n \ : \ n \in \mathbb{Z}\} \subset \mathbb{R}^*$. $\{f \ : \ f|[0,1] = 0\} \subset \mathbb{R}^{\mathbb{R}}$.

32. *Lattice of subgroups.* The intersection of any collection of subgroups is a subgroup. So the subgroups form a lattice, closed under intersection.

    Examples: in V_4, there are 3 proper subgroups; in $\mathbb{Z}/4$, there is just one.

    Intersections of subgroup. Theorem. For any nonempty set of subgroups $H_i \subset G$, the intersection $H = \bigcap H_i$ is also a subgroup.

33. *Sets of generators.* For any set $S \subset G$, we can consider the collection $\mathcal{H}$ of all subgroups H with $S \subset H \subset G$. Note that $\mathcal{H}$ has at least one element, namely G itself.

    We define *subgroup generated by* S to be $\langle S \rangle = \bigcap \mathcal{H}$. It is a general principle that the intersection of any collection of subgroups is again a subgroup; let's check it.

    Since $e \in H$ for all H, we have $e \in \bigcap cH$. If $a, b \in \bigcap \mathcal{H}$, then $a, b \in H$ for every H, and hence $a * b \in H$ and $a' \in H$, so $a * b$ and a' also belong to $\bigcap \mathcal{H}$. ∎

34. *Cayley graph.* Given generators a_i for G, we draw a directed graph with a vertex for each $g \in G$ and an edge from g to $a_i g$, colored by a_i. If a_i has order two, the arrow is dropped.

    Examples: $\langle \mathbb{Z}, 1\rangle$; $\langle \mathbb{Z}/n, 1\rangle$; $\langle V_4, a, b\rangle$; generators i, j; the star, i.e. $\mathbb{Z}/5$ with generator 2.

    Examples: (S_3, f, r) vs. $(\mathbb{Z}/6, 2, 3)$. Two triangles running opposite directions in one case, the same direction in the other. Visualizing commutativity.

3.2 Cyclic groups and greatest common divisor

1. *Cyclic group generated by an element.* Theorem. For any $a \in G$, the set $H = \{a^n \ : \ n \in \mathbb{Z}\}$ is a subgroup.

   Proof. We have $a^{n+m} = a^n a^m$, and $(a^n)' = a^{-n}$, and by convention $a^0 = e$. ∎

   This group $H = \langle a\rangle$ is the *cyclic subgroup of G generated by a.* We have $|\langle a\rangle| = \mathrm{ord}(a)$.

2. *Cyclic groups.* A group G is *cyclic* if $G = \langle a\rangle$ for some $a \in G$. an element $a \in G$ such that every $g \in G$ can

3. Theorem. Any finite cyclic group with is isomorphic to $\mathbb{Z}/n$ where $n = |G|$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$.

   Proof. Let $a \in G$ be a generator of G. Define $f : \mathbb{Z} \to G$ by $f(n) = a^n$. This map is clearly a surjection, and it satisfies $f(ij) = (a^i)(a^j) = a^{i+j}$.

   If f is injective, then it is an isomorphism and we are done.

   Otherwise, $a^i = a^j$ for some $i < j$, so $a^n = e$. Consider the least $n > 0$ such that $a^n = e$. Define $f : \mathbb{Z}/n \to G$ by $f(i) = a^i$; note that $a^{i+kn} = a^i a^{kn} = a^i e^k = a^i$, so f is well-defined. As before $f(i + j) = f(i)f(j)$.

   If this final map is not injective, then there are $0 \le i, j < n$ such that $f(i) = f(j)$. But then $a^{j-i} = e$, and $j - i < n$, contrary to our choice of n. So f is injective and we have shown G is isomorphic to $\mathbb{Z}/n$. ∎

4. *Matrices.* If you have matrices $A = (a_{ij})$ and $B = (b_{ij})$, of dimension $I \times J$ and $I' \times J'$ respectively; then if $J = I'$ you can form the product

$$(AB)_{ik} = \sum_{j=1}^{J} a_{ij} b_{jk}.$$

The result is an $I \times K$ matrix.

We always have $(AB)C = A(BC)$ when the products are all defined, because $(ABC)_{il} = \sum_{j,k} a_{ij} b_{jk} c_{kl}$.

5. *Examples.* Square matrices of rank n. The identity matrix. The powers of a diagonal matrix. Not every square matrix is invertible; those that are form the group $GL_n(\mathbb{R})$. They are characterized by $\det(A) \neq 0$.

The 2×2 matrices are *closed* under multiplication. The set of all matrices $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ and $\det(A) = ad - bc$ form a group. This group is called $SL_2(\mathbb{Z})$. The hard part is the inverse: it's given by $A' = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

6. *Examples.* The diagonal matrices $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The matrix $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ has order 2. The matrix $A = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has order 6. These give finite subgroups $H \subset SL_2(\mathbb{Z})$. The matrix $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order. The matrix $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ also has infinite order, and is related to the Fibonacci numbers.

7. If $G = \langle a \rangle$ then G is a cyclic group and a is a *generator* for G.

A cyclic group can have more than one generator. In $\mathbb{Z}$, the only generators are ± 1.

What are the generators of $\mathbb{Z}/10$? They are $\{1, 3, 7, 9\}$.

8. Theorem. Any subgroup of a cyclic group is cyclic.

Proof. Let $H \subset G = \langle a \rangle$. If H is the trivial subgroup then $H = \langle e \rangle$. Otherwise, we can consider the least $n > 0$ such that $a^n \in H$. We claim $b = a^n$ generates H. Indeed, consider the cyclic group $\langle b \rangle = \{a^{ni} : i \in \mathbb{Z}\}$. Since $b \in H$, we have $\langle b \rangle \subset H$, and if $\langle b \rangle = H$ then we're done.

If not, there is an element $x \in H - \langle b \rangle$. Since G is cyclic, $x = a^j$ for some j which is not a multiple of n. Choose i such that $ni < j < n(i+1)$. Then $xb^{-i} = a^j a^{-ni} = a^{j-ni} \in H$, and we have $0 < j - ni < n$, contrary to our choice of n. This contradiction shows $\langle b \rangle = H$. ∎

9. Theorem. Every subgroup of $\mathbb{Z}$ is of the form $H = n\mathbb{Z}$ for some $n \geq 0$. Thus the subgroups of $\mathbb{Z}$ are in 1-1 correspondence with $\mathbb{N}$.

10. When is $a\mathbb{Z} \subset b\mathbb{Z}$? Exactly when $b|a$. Thus the subgroup of the *additive* group $\mathbb{Z}$ already reveal the multiplicative structure of $\mathbb{Z}$.

    The lattice of subgroups of $\mathbb{Z}$ has $\mathbb{Z}$ as the largest subgroup, then $p\mathbb{Z}$ for p prime as the next largest subgroups, and so on.

11. Example: in $\mathbb{Z}$, we have

$$\langle a, b\rangle = \{na + mb \ : \ n, m \in \mathbb{Z}\}.$$

12. *Greatest Common Divisor.* For any $a \in \mathbb{Z}$, we say $c|a$ if there is an $n \in \mathbb{Z}$ such that $cn = a$.

    Examples: $a|0$ and $1|a$ for every a. $-1|7$; $2|-6$. We have $\gcd(a, b) = \gcd(b, a) = \gcd(-a, b)$.

    Given any $a, b \in \mathbb{Z}$, we define $\gcd(a, b) = c$ where $c \geq 1$ is the largest number such that $c|a$ and $c|b$.

13. Examples: $\gcd(3, 5) = 1$; $\gcd(10, 7) = 1$; $\gcd(21, 15) = 3$; $\gcd(84, 120) = 12$.

14. Theorem. For any $a, b \in \mathbb{Z}$, we have

$$\langle a, b\rangle = \gcd(a, b)\mathbb{Z}.$$

    Proof. Write $\langle a, b\rangle = c\mathbb{Z}$. Since $\langle a, b\rangle$ contains $a\mathbb{Z}$ and $b\mathbb{Z}$, and is in turn generated by c, we can write a and b as multiples of c, so $c|a$ and $c|b$.

    Now if $d|a$ and $d|b$, then $a, b \in d\mathbb{Z}$ and so $c\mathbb{Z} = \langle a, b\rangle \subset d\mathbb{Z}$. But then $d|c$, and in particular $d \leq c$. This shows c is the *greatest* of call common divisors of a and b, and so $c = \gcd(a, b)$.

15. *The Euclidean algorithm.* To compute $\gcd(a, b)$ for $a > b$: define $\gcd(a, 0) = a$, and otherwise $\gcd(a, b) = \gcd(b, a - nb)$ for the least n such that $0 \geq a - nb < b$.

    Examples:

$$\gcd(84, 120) = \gcd(36, 84) = \gcd(12, 36) = 12.$$
$$\gcd(84, 35) = \gcd(35, 14) = \gcd(14, 7) = \gcd(7, 0) = 7.$$
$$\gcd(112, 45) = \gcd(45, 22) = \gcd(22, 1) = \gcd(1, 0) = 1.$$

The Euclidean algorithm is much faster than factoring!

16. *The golden ratio: the first irrational number.* The golden rectangle has aspect ratio $x > 1$ satisfying $1 : (x-1) = x : 1$, i.e. $x^2 - x - 1 = 0$. By geometry, the Euclidean algorithm for x never terminates, so x is irrational.

    Given this infinite divisibility, it is interesting that Democratis should have advocated the atomic theory.

17. We can also express $\gcd(a, b)$ as the product, over all primes dividing both a and b, of the maximal prime power p^e that divides both.

    We say $a, b > 0$ are *relatively prime* if $\gcd(a, b) = 1$. This is the same as saying no prime divides both a and b.

18. Theorem. For any $a, b \in \mathbb{Z}$ there exist $r, s \in \mathbb{Z}$ such that $ar + bs = \gcd(a, b)$.

    Proof. The set $H = \{ar + bs \ : \ r, s \in \mathbb{Z}\}$ clearly coincides with $\langle a, b\rangle$. ■

19. Cor. We have $\gcd(a, b) = 1$ iff there are r, s with $ar + bs = 1$.

20. Cor. A pair (a, b) occurs as a row (or column) of a matrix in $SL_2(\mathbb{Z})$ iff $\gcd(a, b) = 1$.

21. Theorem. An element $a \in \mathbb{Z}/b$ generates $\mathbb{Z}/b$ iff $\gcd(a, b) = 1$.

    Proof. The element a generates iff $a^n = na = 1 \bmod b$ for some $n \in \mathbb{Z}$, iff $an + bm = 1$ for some $n, m \in \mathbb{Z}$, iff $\gcd(a, b) = 1$.

    Example: the generators of $\mathbb{Z}/9$ are $\{1, 2, 4, 5, 7, 8\}$.

22. Theorem. More generally, for any $a \in \mathbb{Z}/b$ we have $\langle a\rangle = \langle \gcd(a, b)\rangle$ and the order of a is $b/\gcd(b, a)$.

    Proof. Let $c = \gcd(a, b)$. Notice that, since $c|b$, the group $\langle c\rangle$ just consists of the multiples of c up to b, so it has order b/c.

Now we will show $\langle a \rangle = \langle c \rangle$. We have $ar + bs = c$ for some $r, s \in \mathbb{Z}$. Since $ar = c \bmod b$, we have $\langle c \rangle \subset \langle a \rangle$. On the other hand, c divides a, so $a = nc$ and thus $\langle a \rangle \subset \langle c \rangle$. Thus $\langle a \rangle = \langle c \rangle$. ∎

23. Corollary. The subgroups of $\mathbb{Z}/b$ correspond bijectively to the divisors c of b, together with zero.

24. Example. In the group $G = \mathbb{Z}/18$ the possible subgroups are $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 6 \rangle$ and $\langle 9 \rangle$, ordered by divisibility.

25. Example. What is the order of $a = 1024$ in $\mathbb{Z}/9999$? Every divisor of $a = 2^{10}$ is a power of 2, and 9999 is even, so $\gcd(1024, 9999) = 1$ — and thus a generates, $\mathrm{ord}(a) = 9999$.

26. *Least Common Multiple.* Similarly, one can define $\mathrm{lcm}(a, b) > 0$ by $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{lcm}(a, b)\mathbb{Z}$.

    Indeed, once one sees that the lattice of subgroups under inclusion corresponds bijectively to the lattice of non-negative integers under division, it is clear that 'meet' and 'join' in the lattice of groups correspond to 'gcd' and 'lcm' in the lattice of integers.

3.3 Symmetric groups and group actions

1. Theorem. For any set A, $S(A)$ is a group.

2. *Notation for permutations.* Let S_n be the permutations of an n-element set, which for compatibility with Fraleigh we consider as $\{1, 2, \ldots, n\}$. Then we can express any element $\sigma \in S_n$ as a $2 \times n$ matrix with the first row listing $1, 2, \ldots, n$ and the second row listing $f(1), f(2), \ldots, f(n)$. This is just like ordered pairs only you have to read vertically!

3. Examples.

   Let $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{smallmatrix}\right)$, $\beta = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{smallmatrix}\right)$. Then α^{-1} is obtained by writing α upside-down and reordering: $\alpha^{-1} = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{smallmatrix}\right)$. Similarly, $\beta^{-1} = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{smallmatrix}\right)$. And the product is given by $\alpha\beta = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{smallmatrix}\right)$.

   The standard generators for S_3 are $r = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ and $f = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$.

4. Theorem (Cayley): Every finite group G is isomorphic to a subgroup of S_n for some n.

   Proof. To each element $g \in G$ we associate the permutation $\sigma_g \in S(G)$ with $\sigma_g(a) = ga$. To see σ_g is a permutation, note that it is invertible, in fact $\sigma_g^{-1} = \sigma_{g^{-1}}$. Also $\sigma_g(e) = g$ so the map $g \mapsto \sigma_g$ is $1-1$.

   Let $H = \{\sigma_g \ : \ g \in G\} \subset S(G)$. Then it is easy to verify that H is a subgroup of $S(G)$. Clearly $\sigma_{gh} = \sigma_g \circ \sigma_h$, so the map $g \mapsto \sigma_g$ is an isomorphism to its image. ∎

   Example: $G = \mathbb{Z}/3$ is isomorphic to the subgroup of rotations inside $S_3 \cong S(G)$.

5. Remark. This theorem shows if $|G| = n$ then we can find G inside $S_{n!}$. If we allow permutation groups of infinite sets, then the same theorem works for infinite groups.

6. *Orbits.* Suppose $\sigma \in S(A)$. We define an equivalence relation by $a \sim b$ if $\sigma^i(a) = b$ for some $i \in \mathbb{Z}$. The equivalence classes are the *orbits* of σ.

   Example: for $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 5 & 1 & 3 & 9 & 6 & 7 & 2 \end{smallmatrix}\right)$, the orbits are $\{1,4\}$, $\{2,6,7,8,9\}$, $\{3,5\}$.

7. *Cycles.* A *cycle* is a permutation with at most one interesting orbit. We use the shorthand $(a_1 \ldots a_n)$ for the permutation that sends a_i to a_{i+1} and fixes everything else. The *length* of the cycle is n.

8. *Properties of cycles.* If $a = (a_1 \ldots a_n)$ then $a' = (a_n \ldots a_1)$. If $b = (b_1 \ldots b_m)$ and $\{a_i\}$ and $\{b_j\}$ are disjoint, then $ab = ba$.

9. *Cycle notation.* Theorem. If A is finite, then every permutation $\sigma \in S(A)$ is a product of disjoint cycles, $\sigma = \mu_1 \cdots \mu_\ell$. This expression for σ is unique up to permuting the cycles.

   Proof. On each orbit A_i of σ, define $\mu_i(x) = \sigma(x)$ for $x \in A_i$ and $\mu_i(x) = x$ elsewhere. Then μ_i is a cycle, and clearly σ is their product. ∎

Example: σ above is $(14)(28769)(35)$. We can write this is any order and cyclically permute the elements of any cycle. So we also have $\sigma = (53)(76928)(14)$.

Note: We *leave out* the trivial cycles in this product.

10. *Products of cycles.* How to take the product of cycles that might not be disjoint. Examples: $(12)(23) = (123)$, $(23)(12) = (213)$. More examples: $(12345)(35)(13) = (1)(23)(45)$.

11. *Dihedral group D_n.* The symmetries D_n of an n-gon are generated by a *rotation* r and a *flip* f, satisfying $frf = r^{-1}$ and $r^n = f^2 = e$. Any element of D_n can be written in the form r^i or $r^i f$, for $0 \leq i < n$. The elements with f in them all have order two! In fact $r^i f r^i f = f r^{-i} r^i f = f^2 = e$.

    Similarly we can multiply any two elements and write the result in the standard form: e.g.

    $$r^a f r^b f = r^a r^{-b} f^2 = r^{a-b}.$$

12. *Example: D_4 as a subgroup of S_4.* What are the symmetries of the square? Numbering the vertices counter-clockwise, we have $r = (1234)$, the counter-clockwise rotation. We also have flip on the ascending and descending diagonals, $a = (24)$ and $d = (13)$; and the vertical and horizontal flips, $v = (14)(23)$ and $h = (12)(34)$.

    It is then not hard to work out the group table.

13. *The lattice of subgroups of D_4.* To practice some cycle computations, lets look at the subgroup $\langle v, h\rangle$ generated by two orthogonal flips in D_4. Their product vh should be a rotation! Indeed, $vh = (14)(23)(12)(34) = (13)(24) = r^2$. Now r^2 commutes with any flip, so $\langle v, h\rangle$ is a Klein 4-group. Similarly $\langle a, d\rangle$ is a Klein 4-group. On the other hand, $\langle r\rangle$ is isomorphic to $\mathbb{Z}/4$.

    What about the group $\langle v, a\rangle$ — generated by two flips that are *not* orthogonal? This contains $av = (24)(14)(23) = (1234) = r$, and r and any flip generate D_4. In fact we have found all the subgroups of order 4.

The lattice of groups is:

$$
\begin{array}{ccccc}
 & & D_4 & & \\
 & \langle a,d\rangle & \langle r\rangle & \langle v,h\rangle & \\
\langle a\rangle & \langle d\rangle & \langle r^2\rangle & \langle v\rangle & \langle h\rangle \\
 & & \langle e\rangle & &
\end{array}
$$

Here r^2 forms the intersection of any pair of subgroups of order 4.

14. Theorem. The transpositions generate S_n.

    Proof 1. Any cycle is a product of transpositions and any permutation is a product of cycles. Example: $(12345) = (12)(23)(34)(45)$.

    Proof 2. Draw the picture of the map as a braid! ∎

15. Theorem. In fact S_n is generated by $\sigma = (123\ldots n)$ and $\tau = (12)$.

    Idea of proof. By conjugating τ by σ we get all adjacent transpositions, and these suffice. ∎

16. *The alternating group.* We define A_n as the subset of S_n consisting of permutations that can be expressed as products of an *even* number of cycles.

    Theorem (easy). A_n is a subgroup.

17. Theorem. Every element of S_n is either even or odd but not both.

    Lemma. Let $N(\sigma)$ be the number of orbits of σ. Then for any transposition τ, $N(\tau\sigma) = 1 + N(\sigma) \bmod 2$.

    Proof. Multiplication by τ either joins two orbits together, or breaks one orbit into two. So in either case, the number of orbits changes by one.

    Proof of the Theorem. If σ can be expressed as both an even and odd product of permutations, then $N(\sigma) = N(e) = N(e) + 1 \bmod 2$, which is obviously impossible. (Thus N is even iff $N(\sigma) = N(e) \bmod 2$.)

18. Cor. The alternating group is a proper subgroup of S_n for $n \geq 2$. In fact it contains exactly half the elements of S_n.

    Proof. Every transposition is odd, and every odd element in S_n belongs to τA_n.

19. *Examples: Orientation.* Yet another way to look at the alternating group A_n involves the *orientation* of an $n-1$ simplex. Examples: The group S_2 acts on a directed segment; the subgroup A_2 preserves the arrow. The group S_3 acts on a triangle; the subgroup A_3 keeps the front face forward. The group S_4 acts on a tetrahedron; the subgroup A_4 doesn't turn the tetrahedron inside-out.

20. *Parity and braids.* Draw $g \in S_n$ as a braid. Then g can be written as a product of transpositions with one transposition for each crossing in the picture! As one moves the strands around, the parity never changes. Thus A_n is a proper subgroup of S_n.

21. *Parity and determinants.* Essentially the same distinction can be drawn by associating to $g \in S_n$ a linear transformation $A(g) : \mathbb{R}^n \to \mathbb{R}^n$ that sends (x_i) to $(x_{\sigma(i)})$. Then $\det A(g) = \pm 1$, and A_n is the subgroup where the determinant is $+1$.

22. *Why symmetric?* A function $f(x_1, \ldots, x_n)$ is said to be *symmetric* if $f(x_i) = f(x_{\sigma(i)})$ for any $\sigma \in S_n$. Thus the symmetric functions are those invariant under the symmetric group. That seems to be where the terminology comes from.

23. *Fermions.* The Pauli exclusion principle states that two electrons (or more generally, fermions) cannot occupy the same state. More technically, electrons are symmetric under A_n but anti-symmetric under odd permutations.

    This principle is what forces electrons to occupy higher and higher shells around an atom, and thus gives rise to chemistry.

24. *Sliding puzzles.* The famous Sam Lloyd puzzle with small sliding squares, sometimes cannot be done!

    The reason has to do with the alternating group. Each move of the puzzle is a transposition. But each move also moves the blank square from an even to an odd position or vice-versa. So if we start and end with the blank on the same square, we have made an even number of moves, hence an even number of transpositions. But half the elements of S_n cannot be expressed in this way! So if the puzzle is assembled randomly, there is a 50% chance that it cannot be solved.

A particularly clear example is the 2×2 puzzle, where the pieces can only be moved cyclically.

25. *Multiplicative notation.* For $A \subset G$ we let $xA = \{xa : a \in A\}$. Note that $x'xA = A$ and thus $|xA| = |A|$.

    We also write $AB = \{ab : a \in A, b \in B\}$. For example, if H is a subgroup, then $HH = H$, $HG = G$. If $xH = H$ then $xh = e$ for some h and hence $x = h' \in H$.

    Cosets. Let us say $x \sim y$ iff $xh = y$ for some $h \in H$. Check that this is an equivalence relation. ($xe = x$; $xh = y \implies yh^{-1} = x$; $xh_1 = y$ and $yh_2 = z \implies z = xh_1h_2$.)

    Now clearly $xH = [x]$. These equivalence classes are called the *left cosets* of H. You can play the same game with the right cosets.

26. Example. In $G = \mathbb{Z}/6$, there are 3 cosets of $\langle 3 \rangle$. The right and left cosets agree, as they would in any abelian group.

    Example. In $G = S_3$, let $H = \langle r \rangle$. Then the cosets are H and fH. (In fact you can tell which coset x is in by whether or not it reverses the orientation of a triangle.) Note that the right and left cosets agree.

    Let $H = \langle f \rangle$. Then the left cosets are H, rH, r^2H. (The coset is determined by where the element maps the vertex fixed by f.)

    Now consider the right cosets. These are different! $rH = \{r, rf\}$ while $Hr = \{r, fr\} = \{r, r^2 f\}$.

    These cosets are nicely pictured on the Cayley graph.

27. Theorem (Lagrange). If $H \subset G$ is a subgroup of a finite group, then $|H|$ divides $|G|$.

    Proof. Any coset xH has cardinality $|H|$. Since the cosets form a partition of G, their common cardinality must divide $|G|$. ∎

28. *Coset space.* The set of left cosets of G is denoted by G/H; it is also the set of equivalence classes of the relation $x \sim y$ if $xH = yH$.

29. Example: in studying the subgroups of D_4, we only needed to find subgroups of orders 8, 4, 2 and 1.

30. Cor: The order of any element in G divides $|G|$.

    Cor: If $|G| = p$ is a prime, then G is cyclic, i.e. $G \cong \mathbb{Z}/p$.

    In particular this completes the classification of groups of order up to 5.

31. *Group actions.* An *action* of G on a set A is a map $G \times A \to A$, usually written as left multiplication, such that

    $$(gh)a = g(ha), \text{ and}$$
    $$ea = a.$$

    Examples. $S(A)$ actions on A by $\sigma a = \sigma(a)$. Any subgroup $G \subset S(A)$ acts on A. The dihedral group acts on the vertices of a square, and on its edges, and on its diagonals.

32. *Transitivity.* A group action is *transitive* if for any $x, y \in A$, there is a $g \in G$ such that $g(x) = y$. This g need not be unique.

    Example. S_n acts transitively on $\{1, \dots, n\}$. But so does the cyclic group $\mathbb{Z}/n$ generated by $\sigma = (123 \dots n)$.

33. Example. Let A be the set of all 6 edges obtained from a square by adding in the diagonals. Then D_4 acts on A, but *not* transitively; it has two orbits.

34. *Stabilizer.* The *stabilizer* or *isotropy subgroup* of a given point $x \in A$ is just defined by

    $$H_x = \{h \in G \ : \ h \cdot x = x\}.$$

35. Theorem. Let G act transitively on a set A, and let $x \in A$ have stabilizer H_x. Then $|A| = |G|/|H_x|$.

    Proof. Define a map $f : G/H_x \to A$ by $f(g) = gx$. We claim this map is a bijection.

First, f is well-defined. If g is replaced by gh, $h \in H_x$, then $f(gh) = ghx = gx = f(g)$. So f is constant on each coset gH_x, so it is well-defined as a function on G/H_x.

Second, f is surjective by transitivity.

Finally, f is one-to-one. For if $f(g) = f(k)$, then $gx = kx$, so $k'gx = x$ and thus $k'g \in H_x$. But then $g \in kH_x$, so $[g] = [k]$ in G/H_x.

Thus A and G/H_x are in bijection, and since $|G/H| = |G|/|H|$, we have the theorem. ■

Examples in the plane: D_3 acts on a triangle with the stabilizer of a vertex given by $H_v = \{e, f\}$. The number of vertices is $|D_3|/|H_v| = 6/2 = 3$. Similarly for D_4.

The group D_4 also acts on the *diagonals* of a square. The stabilizer of the ascending diagonal is $\langle a, d \rangle$; it has order 4.

3.4 Geometric examples of groups

36. *Platonic solids.* A *Platonic solid* S is a polyhedron in space such that all faces, edges and vertices are equivalent. In other words, the symmetry group of S must act transitively on the vertices, edges and faces.

As a consequence, the number of vertices, faces and edges must divide the order of the symmetry group.

There are exactly 5 Platonic solids: the tetrahedron, the cube, the octahedron, the dodecahedron and the icosahedron.

The tetrahedron. The symmetry group of a tetrahedron is A_4; it can be described as the orientation-preserving permutations of the vertices.

The cube. The symmetry group of a cube has 24 elements, since there are 6 faces each with stabilizer of order 4.

In fact G is isomorphic to S_4, acting on the long diagonals! To see this, note that a rotation fixing a face gives the permutation $\sigma = (1234)$, and a rotation fixing an edge gives the permutation (12). These two elements together generate S_4.

The cube is dual to the octahedron.

The dodecahedron. How large is the symmetry group of a dodecahedron? A face has stabilizer of order 5, and there are 12 faces, so $|G| = t \times 12 = 60$. Similarly there are 30 edges (since each has stabilizer 2) and 20 vertices (since 5 faces come together at each).

It turns out we have $G \cong A_5$. To see this, one can find *5 cubes* whose vertices lie on the vertices of a dodecahedron. There are 20 vertices all together, and each belongs to two cubes — which works out, since 5 cubes have $5 \cdot 8 = 40$ vertices all together.

It is important to note that not every symmetry of an inscribed cube extends to a symmetry of the dodecahedron. In fact we have $S_4 \cap A_5 = A_4$ under the embedding.

The dodecahedron is dual to the icosahedron.

37. *A non-Platonic solid.* The rhombic dodecahedron is *not* a Platonic solid. All its 12 faces are equivalent, and their stabilizer is of order 2, so $|G| = 24$. There are 14 vertices, but they are *not* all equivalent! In fact they fall into two classes of sizes $6 + 8 = 14$, and each of those divides 24.

38.

	G	$\|G\|$	V	E	F	$V - E + F$
Tetrahedron	A_4	12	4	6	4	2
Cube	S_4	24	8	12	6	2
Octahedron	S_4	24	6	12	8	2
Dodecahedron	A_5	60	20	30	12	2
Icosahedron	A_5	60	12	30	20	2
Rhombic Dodecahedron	S_4	24	6+8=14	12	12	2

39. *Higher Platonic solids.* (Daniel Allcock.) There are 6 4D Platonic solids, described in Coxeter's book, *Regular Polytopes.* (A $(d+1)$-dimensional solid is Platonic if its symmetries act transitively on faces of the same dimension, and each d-dimensional face is also Platonic, and its symmetries arise from those of the full polyhedron.)

They are: the simplex, the cube, the dual cube, a solid with 120 dodecahedral faces, its dual (with 600 tetrahedral faces), and a solid with 24 octahedral faces (self-dual). Their symmetry groups in the last two cases are $(2A_5 \times 2A_5)/2$ (of order $60 \cdot 120$) and a degree two extension of $(2A_4 \times 2A_4)/2$ (of order $24 \cdot 24$).

In dimensions 5 or more, there are only 3 Platonic solids: the simple, the cube and the dual to the cube.

40. *Kepler's Cosmology.* Kepler believed that the orbits of the planets were determined by the Platonic solids. Each eccentric orbit determines a thickened sphere or orb, centered at the Sun, that just enclosed it. The 5 Platonic solids thus correspond exactly to the gaps between the 6 planets known at that time. Between the orbits of Saturn and Jupiter you can just fit a cube; between Jupiter and Mars, a tetrahedron; between Mars and Earth, a dodecahedron; between Earth and Venus an icosahedron, and between Venus and Mercury, an octahedron.

    This theory is discussed in the *Mysterium Cosmographicum*, 1596. Using the astronomical data of Copernicus, Kepler found:

	Predicted	Actual
Jupiter/Saturn	577	635
Mars/Jupiter	333	333
Earth/Mars	795	757
Venus/Earth	795	794
Mercury/Venus	577	723

    See 'Kepler's Geometrical Cosmology', J. V. Field, University of Chicago Press, 1988.

41. *Quaternions.* Hamilton made the amazing discovery that you get a reasonable algebra by adjoining not one but 3 square-roots of unity to $\mathbb{R}$! But you have to give up commutativity.

    In this 'quaternion algebra', every number is of the form $a+bi+cj+dk$, where $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$.

    Then $G = \{\pm 1, \pm i, \pm j, \pm k\}$ gives a non-commutative group of order 8, called *the quaternion group.*

42. More Cayley graphs: groups of order 8. The dihedral group (D_4, f, r). Th group $\mathbb{Z}/2 \times \mathbb{Z}/4$.

    The quaternion group Q with generators i, j; 8 points on S^3! (Put $\pm 1, \pm i, \pm j$ on the vertices of an octahedron. Then put k in the center of the octahedron and $-k$ at infinity!)

43. *Plane isometries.* Finally we mention the important group $\mathrm{Isom}(\mathbb{E}^2)$ of isometries of the Euclidean plane. This group consists of all maps $f : \mathbb{E}^2 \to \mathbb{E}^2$ such that $d(f(P), f(Q)) = d(P, Q)$.

    Our groups D_n — the symmetries of a polygon – can be thought of as special cases of plane isometries. Some other subgroups of $\mathrm{Isom}(\mathbb{E}^2)$: $\mathbb{Z}^2$, the symmetries of a checkerboard with a rook (written R) on each square.

44. *Types of isometries.* Other than the identity, there are four types of plane isometry. An isometry *preserves orientation* if handwriting stays the same way.

    Orientation preserving, with a fixed-point P: rotation.
    Orientation preserving, with no fixed-point: translations.
    Orientation reversing, with a fixed-point: reflection.
    Orientation reversing, with no fixed-point: glide-reflection.

3.5 Abelian groups

45. *Least common multiple.* Recall that for $a, b \in \mathbb{Z}$, both nonzero, we defined the least common multiple of a and b to be the smallest $n > 0$ that is divisible by both a and b.

    Equivalently, $\langle \mathrm{lcm}(a, b) \rangle = a\mathbb{Z} \cap b\mathbb{Z}$.

    We have $\mathrm{lcm}(a, b) = ab/\gcd(a, b)$. For example, $\mathrm{lcm}(12, 15) = 12 \times 15/3 = 60$.

    The lcm can be easily computed from the prime factorizations of a and b.

46. *Products of groups.* If G, H are groups then $G \times H$ becomes a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1, h_2)$. If G and H are abelian then so is $G \times H$. Of course $|G \times H| = |G||H|$.

Example: the Cayley graph of $\mathbb{Z}/a \times \mathbb{Z}/b$ can be visualized as a torus.

47. *Orders of elements.* In $G \times H$ we have $\text{ord}(g,h) = \text{lcm}(\text{ord}(g), \text{ord}(h))$. (Since $(g,h)^n = (g^n, h^n) = (e,e)$ iff $\text{ord}(g)|n$ and $\text{ord}(h)|n$.)

48. Corollary. If $\gcd(a,b) = 1$, then $G = \mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$.

    Proof. Consider the element $g = (1,1)$. Then $\text{ord}(g) = \text{lcm}(a,b) = ab/\gcd(a,b) = ab$, so g generates G and thus G is cyclic. ∎

    Thus even if a group is a product, it may be cyclic!

49. Example: $\mathbb{Z}/2 \times \mathbb{Z}/3 \cong \mathbb{Z}/6$.

    Example: $G = \mathbb{Z}/2 \times \mathbb{Z}/4$ is *not* isomorphic to $\mathbb{Z}/8$; indeed every element in $\mathbb{Z}/a \times \mathbb{Z}/b$ has order *at most* $\text{lcm}(a,b)$, which is less than ab if $\gcd(a,b) > 1$.

50. Theorem (Fundamental Theorem of Abelian Groups). Let G be a finitely-generated abelian group. Then there are prime numbers p_i and exponents e_i and an integer b such that

$$G \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_n^{e_n} \times \mathbb{Z}^b.$$

    This expression is unique up to the ordering of the factors. *The primes need not be distinct!*

51. Example. If n has prime factorization $n = p_1^{e_1} \dots p_n^{e_n}$, then

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_n^{e_n}.$$

    Notice that $\text{lcm}(p_1^{e_1}, \dots, p_n^{e_n}) = n$.

52. Example. In general, the isomorphism classes of abelian groups of order n correspond to the ways of factoring n into a product of powers of primes. The only abelian group of order 6 is $\mathbb{Z}/2 \times \mathbb{Z}/3$. For order 12, there are 2 groups, 4×3 and $2 \times 2 \times 3$. For order 360, there are 6

groups; $360 = 2^3 \times 3^2 \times 5$, and the factorizations are

$$\begin{aligned}
360 &= 2 \times 2 \times 2 \times 3 \times 3 \times 5, \\
360 &= 2 \times 4 \times 3 \times 3 \times 5, \\
360 &= 8 \times 3 \times 3 \times 5, \\
360 &= 2 \times 2 \times 2 \times 9 \times 5, \\
360 &= 2 \times 4 \times 9 \times 5, \\
360 &= 8 \times 9 \times 5.
\end{aligned}$$

Example. Any two generator group $G \subset \mathbb{R}^3$ is isomorphic to $\mathbb{Z}^n$, $n = 0$, $n = 1$ or $n = 2$. Proof: G has no torsion (other than the identity).

Example. How does an abelian group like $\mathbb{Q}$ fit into this scheme? $\mathbb{Q}$ *is not finitely-generated!* However it does have finitely-generated subgroups. E.g. what is the subgroup $\langle 1/3, 1/7\rangle \subset \mathbb{Q}$? It's a *cyclic group*, namely $\langle 1/21\rangle$. (That's because $\gcd(3,7) = 1$, and thus $3 \times 5 - 7 \times 2 = 1$, so $5/7 - 2/3 = 1/21 \in G$.)

Example. How does the trivial group fit into this scheme? It is the 'empty product', or $\mathbb{Z}^0$.

53. Theorem. A finite abelian group G is indecomposable iff $G \cong \mathbb{Z}/p^e$ for some p, e. (Indecomposable means if $G \cong A \times B$, then A or B is trivial.)

    Proof. If G is indecomposable then in the classification, only one term can occur, so $G \cong \mathbb{Z}/p^e$. Conversely, if $G = \mathbb{Z}/p^e$ and $G = A \times B$, then $|A| = p^a$ and $|B| = p^b$, where $a + b = e$, and thus the order of every element in G is at most $\mathrm{lcm}(p^a, p^b) = p^{\max(a,b)}$. But G has an element of order p^e, so $a = 1$ or $b = 1$ and the product is trivial.

54. *Prime factorization.* We can think of the preceding theorem as saying that the groups of the form $G = \mathbb{Z}/p^e$ are 'prime': they cannot be 'factored' as $G = G_1 \times G_2$ except in trivial ways. So the fundamental theorem of abelian groups is like the prime factorization of integers.

    The theorem can be proved in a similar way too: given a finite abelian group, we factor it as much as possible.

55. *Automorphisms.* For any group G, $\mathrm{Aut}(G)$ is *also* a group. In V_4 we have the symmetric relation $a + b + c = e$ and $a' = a$, $b' = b$, $c' = c$; from this we see that $\mathrm{Aut}(G) = S(\{a, b, c\}) = S(3)$!

56. Theorem. $\mathrm{Aut}(\mathbb{Z}/n) \cong (\mathbb{Z}/n)^*$.

    Proof. An automorphism ϕ is determined by $\phi(1) = k$. It has to send 1 to an element k that also generates $\mathbb{Z}/n$. If k and n are both divisible by some number $d > 1$, then all multiples of k would be divisible by d, so we'd get a proper subgroup. Thus we must have $\gcd(k, n) = 1$. Then k does generate.

    What is the group law? $\phi_k(\phi_\ell(1)) = k\ell$, so the group law is indeed multiplication. ∎

57. Example: in $\mathbb{Z}/100$, is multiplication by 3 an automorphism? (Yes). What is its order? (This is tricky! $3^{20} = 3486784401 = 1 \bmod 100$.)

58. Example: in how many ways is $\mathbb{Z}/10$ isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/5$? Answer: there are 4 generators for $\mathbb{Z}/10$, so there are 4 isomorphisms.

3.6 Homomorphisms and factor groups

1. *Group homomorphisms.* Let G and H be groups. A map $\phi : G \to H$ is a *homomorphism* if $\phi(ab) = \phi(a)\phi(b)$.

    The *trivial homomorphism* sends all of G to the identity.

2. Examples of homomorphisms.

    (a) Let $\phi : \mathbb{Z} \to \mathbb{Z}/n$ be reduction mod n.

    (b) Let $\phi : S_n \to \mathbb{Z}/2$ by parity.
    On $S_3 \cong D_3$, we have $\phi(r) = 0$, $\phi(f) = 1$; check that $\phi(rf) = 1 = \phi(fr^2)$.

    (c) For any element $a \in G$, we obtain a homomorphism $\phi : \mathbb{Z} \to G$ by $\phi(n) = a^n$.
    If a has order n, we also get a homomorphism $\phi : \mathbb{Z}/n \to G$. This map is $1 - 1$.

    (d) Let $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ by $\phi(A) = \det(A)$.

    (e) For any real numbers a, b, let $\phi : \mathbb{R}^2 \to \mathbb{R}$ be given by $\phi(x, y) = ax + by$.

    (f) Let $\phi : \mathbb{R} \to \mathbb{C}^*$ be given by $\phi(\theta) = \exp(i\theta)$.

(g) Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ be given by $\phi(x) = |x|$.

(h) Let $\phi : C^\infty[0,1] \to \mathbb{R}$ be given by $\phi(f) = \int_0^1 f(x)\,dx$.

(i) Let $\phi : S_4 \to S(\{x,y,z\}) \cong S_3$ map the symmetries of the cube into the space of permutations of the coordinate axes.

3. *Properties of homomorphisms.* Let $\phi : G \to H$. Then $\phi(G)$ is a subgroup of H. We have $\phi(a^{-1}) = \phi(a)^{-1}$. The identity maps to the identity.

4. *Normality.* A subgroup $K \subset G$ is *normal*, usually written $K \lhd G$, if $gH = Hg$ for all $g \in G$. Equivalently, if $gHg^{-1} = H$ for all $g \in G$.

   Example: $\langle r \rangle$ is normal in $G = S_3$, but $H = \langle f \rangle$ is not, since rHr^{-1} contains $rfr^{-1} = r^2 f \notin H$.

5. *Normality in abelian groups.* Theorem. Any subgroup of an abelian group is normal.

6. *The kernel.* The set of elements of G that are sent to the identity by a homomorphism $\phi : G \to H$ form the *kernel* of ϕ, denoted $\mathrm{Ker}(\phi)$.

   Theorem. $\mathrm{Ker}(\phi)$ is a *normal subgroup* of G.

   Proof. Check that ϕ is subgroup; that's easy. Now for normality, note that for $k \in K$, we have $\phi(gkg^{-1}) = \phi(g)\phi(g^{-1}) = e$, and thus $gKg^{-1} \subset K$ for any $g \in G$. But then $K = g(g^{-1}Kg)g^{-1} \subset gKg^{-1}$, and thus $K = gKg^{-1}$ for all g. ∎

7. Examples: the kernels in our various examples of homomorphisms are:

   (a) $n\mathbb{Z}$, for $\phi : \mathbb{Z} \to \mathbb{Z}/n$.

   (b) A_n, for $\phi : S_n \to \mathbb{Z}/2$.

   (c) $\langle r \rangle$, in the case of S_3.

   (d) $\mathrm{ord}(a)\mathbb{Z}$, for $\phi : \mathbb{Z} \to G$ by $\phi(n) = a^n$.

   (e) $SL_n(\mathbb{R})$, for $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$.

   (f) The line $\langle (bt, -at) \ : \ t \in \mathbb{R} \rangle$, for $\phi(x,y) = ax + by$; or $\mathbb{R}^2$ itself if $a = b = 0$.

   (g) $2\pi\mathbb{Z}$, for $\phi(\theta) = \exp(i\theta)$.

(h) $\{\pm 1\}$, for $\phi(x) = |x|$ on $\mathbb{R}^*$.

(i) The functions of mean zero, for $\phi(f) = \int_0^1 f(x)\,dx$.

(j) The Klein four subgroup generated by 180 degree rotations, for $\phi : S_4 \to S(\{x, y, z\}) \cong S_3$.

8. Theorem. Let $\phi : G \to H$ be given, and suppose $\phi(x_0) = y$. Then the set S of all solutions to the equation $\phi(x) = y$ is given by $S = \{x_0 k : k \in \operatorname{Ker}(\phi)\}$.

9. Example: define $\phi : \mathbb{R}^* \to \mathbb{R}^*$ by $\phi(x) = x^2$, so $\operatorname{Ker}\phi = \{\pm 1\}$. Then if $\phi(x_0) = y$, we have $\phi^{-1}(y) = x_0 \cdot \operatorname{Ker}\phi = \pm x_0$. "That plus or minus sign comes from the fact that ± 1 is the kernel of the squaring homomorphism."

10. Example: define $\phi : C^\infty[0,1] \to C^\infty[0,1]$ by $\phi(f) = f'$. Then $\operatorname{Ker}(\phi)$ consists of the constant functions, $f(x) = C$.

    Now let us try to find all solutions to the equation $\phi(f) = f'(x) = x$. One solution is given by $f_0(x) = x^2/2$. Thus all solutions are given by $f(x) = x^2/2 + C$.

11. Theorem. A homomorphism ϕ is injective iff $\operatorname{Ker}(\phi) = \{e\}$.

    Proof. If $\phi(g) = \phi(h)$ for some $g \neq h$, then $e \neq g^{-1}h \in \operatorname{Ker}(\phi)$. ■

12. Cor. If $\phi : G \to H$ has trivial kernel, then G is isomorphic to a subgroup of H, namely $\phi(G) \subset H$.

13. *Factor groups.* We have seen that $\operatorname{Ker}(\phi)$ is a normal subgroup. Now given a normal subgroup $H \subset G$, can we somehow find a homomorphism $\phi : G \to G_1$ such that $\operatorname{Ker}(\phi) = H$? Yes! $G_1 = G/H$.

14. Suppose H is a normal. Then given two left cosets, aH and bH, their product is again a left coset! That is, $aHbH = abHH = abH$. So we define $(aH) * (bH) = (aH)(bH) = abH$.

    Theorem (Fundamental Theorem of Factor Groups). Let $K \subset G$ be normal. Then:

    (a) The left cosets G/K form a group, and the natural map $\phi : G \to G/K$ is a surjective homomorphism with kernel K; and

(b) If $\phi : G \to H$ has kernel K, then $\phi(G) \cong G/K$.

Proof. (1) K itself is a two-sided identity (note that $KaK = aKK = K$. We have $(aK)^{-1} = a^{-1}K$, and associativity: $aKbKcK = (abc)K$. Thus G/K is a group, with identity K. The only things that map to the identity are elements of K.

(2) There is a map $\psi : G/K \to H$ such that $\psi(gK) = \phi(g)$. This map is a homomorphism, and it is injective by the definition of the kernel.
■

15. Example: $\mathbb{Z}/n$ is just $\mathbb{Z}/n\mathbb{Z}$. But it changes the way you think about it! For example, in $\mathbb{Z}/10$, the number 3 is really the coset $3 + 10\mathbb{Z} = \{\ldots, -7, 3, 13, \ldots\}$.

16. Corollary. If $\phi : G \to H$ is a surjective homomorphism, then $|H|$ divides $|G|$.

    Thus Lagrange's theorem holds for both *subgroups* and *quotient groups.*

17. Example: there is no map $\phi : \mathbb{Z}/12 \to \mathbb{Z}/5$, except for the trivial map.

    Example: if $\phi : \mathbb{Z}/22 \to S_{10}$, the image must have order 1 or 2 (11 does not divide $10! = |S_{10}|$).

18. Theorem. There is a nontrivial map $\phi : \mathbb{Z}/a \to \mathbb{Z}/b$ iff $\gcd(a, b) > 1$.

    Proof. Suppose ϕ is nontrivial, and let $G = \phi(\mathbb{Z}/a)$, $d = |\phi(\mathbb{Z}/a)| > 1$. Then $d|a$ since G is a *quotient group* of $\mathbb{Z}/a$, and $d|b$ since G is a *subgroup* of $\mathbb{Z}/b$. Thus $1 < d \le gcd(a, b)$.

    Conversely, if $d = \gcd(a, b) > 1$, then we can then we can define $\phi(x) = (b/d)x$. If x is changed by a multiple of a, then $\phi(x)$ is changed by a multiple of $(b/d)a = b(a/d) = 0 \bmod b$, so ϕ is well-defined; and $\phi(1) = b/d \neq 0 \bmod b$, so ϕ is nontrivial. ■

19. Exercise. (Fraleigh, 3.2(21)). If G is abelian then G/H is abelian. What is wrong with a proof that starts "let a and b be elements of G/H"?

3.7 Generators and relations

20. *Introduction to free groups.* Any one generator G group admits a *surjective* map $\phi : \mathbb{Z} \to G$. Thus $\mathbb{Z}$ is the 'biggest' group with one generator — every other cyclic group is a quotient of it.

    What is the biggest group you can make with two generators?

21. *The free group on 2 generators.* Answer: Consider all finite words in the letters a, a', b and b'. A word is *reduced* if it does not contain aa', $a'a$, bb' or $b'b$. An arbitrary word can be reduced by repeatedly cancelling out (removing) these 2-letter subwords whenever they occur. Example: $ab'aa'ba \to ab'ba \to aa$.

    Let G be the set of all reduced words. Multiplication is defined by concatenation followed by reduction. The inverse of a word is obtained by writing it down backwards and exchanging the primed and unprimed variables.

    The result is the *free group* $\mathbb{Z} * \mathbb{Z} = \langle a, b\rangle$.

22. *Trees.* The Cayley graph of the free group is an infinite tree.

23. Theorem. Let G' be a group that can be generated by two elements x and y. Then there is a unique surjective map $\phi : \mathbb{Z} * \mathbb{Z} \to G'$ with $\phi(a) = x$ and $\phi(b) = y$.

    This means G' can be described as $G/\operatorname{Ker}\phi$.

24. Example. Let $H \subset G = \mathbb{Z} * \mathbb{Z} = \langle a, b\rangle$ be the subgroup generated by *all commutators*, $[g, h] = ghg^{-1}h^{-1}$. Since the set of commutators is closed under conjugation, so is H. Therefore H is *normal.*

    What is G/H? Construct a map $\phi : G \to \mathbb{Z}^2$ sending a to $(1, 0)$ and b to $(0, 1)$. Since every commutator is in the kernel, we actually get a map $\phi : G/H \to \mathbb{Z}^2$. Now construct a map $\psi : \mathbb{Z}^2 \to G/H$, sending (i, j) to $a^i b^j$. Since G/H is abelian, this map is a homomorphism. Clearly the compositions are the identity, so G/H is isomorphic to $\mathbb{Z}^2$.

25. *Group presentations.* By $G = \langle g_1, \ldots , g_n \ : \ r_1, \ldots , r_m\rangle$ we denote F/N where F is the free group on generators $g_1, \ldots , g_n$, and $N \subset F$ is the smallest normal subgroup containing $R = \{r_1, \ldots , r_m\}$.

Another way to put it is that N is the set of *consequences* of the relations R. Here a consequence of R means either

(a) the identity e (the trivial consequence),
(b) an element $r \in R$,
(c) the product of two consequences,
(d) the inverse of a consequence, or
(e) fxf^{-1} where $f \in F$ and x is a consequence.

Clearly if we have a group in which the elements of R represent the identity, so do the consequences of R. Now it is easy to see that the consequences form a normal subgroup, and in fact they are exactly N, the smallest normal subgroup containing R.

26. Theorem. To give a homomorphism $\psi : G \to H$, where $G = \langle g_1, \ldots, g_n : r_1, \ldots, r_m \rangle$, it suffices to give values $h_i = \psi(g_i) \in H$ for each generator, and check that $\psi(r_i) = e$ for each relations.

    Proof. Let F be the free group on generators $\langle g_1, \ldots, g_n \rangle$. The h_i determine a homomorphism $\phi : F \to H$. By assumption, $r_i \in \mathrm{Ker}(\phi)$ for each relation. Since the kernel is a normal subgroup, it *contains* the smallest normal subgroup N containing the relations r_i. But by definition, $F/N \cong G$, so ϕ descends to a map $\psi : F/N \to H$.

27. *Present* $\mathbb{Z}^2$. Let $G = \langle a, b \ : \ ab = ba \rangle$. Then G is abelian, and there is a map to $\mathbb{Z}^2$, which is obviously surjective. There is also an inverse map, which is a homomorphism because G is abelian. Both compositions give the identity, so $G \cong \mathbb{Z}^2$.

28. *The checkerboard.* It is useful to compare the Cayley graphs of the free group $\langle a, b \rangle$ and of the free abelian group $\langle a, b \ : \ ab = ba \rangle$. The relation gives loops in the second graph.

29. *Dihedral groups.* As an example, let's consider the group

$$G = \langle f, r \ : \ f^2 = r^n = e, rf = fr^{-1} \rangle.$$

    Using the relations, every word can be represented in the form $r^i f^j$ where $0 \le i < n$ and $j = 0, 1$. Thus G has *at most* $2n$ elements.

    Define the obvious homomorphism $\phi : G \to D_n$. Then ϕ is onto, so by counting we see it is an isomorphism.

30. *The infinite dihedral group.* Let $D_\infty = \langle f, r \ : \ rf = fr^{-1} \rangle$. We can think of D_∞ as acting on $\mathbb{R}$ as the boundary of an 'infinite polygon', with vertices at the integers, by $f(x) = -x$, $r(x) = x+1$. Then $frf(x) = -((-x)+1) = x - 1 = r^{-1}(x)$ as required.

31. *Another presentation for D_∞.* Let $G = \langle a, b \ : \ a^2 = b^2 = e \rangle = \mathbb{Z}/2 * \mathbb{Z}/2$. It is easy to draw the Cayley graph of G; it's a straight line, just like the boundary of an infinite polygon.

    Theorem. D_∞ and G are isomorphic.

    Proof. Define a map $\phi : G \to D_\infty$ by $\phi(a) = f$, $\phi(b) = rf$. Then clearly $\phi(a^2) = e$ and $\phi(b^2) = rfrf = rr^{-1} = e$, so ϕ is a homomorphism.

    Now define a map $\psi : D_\infty \to G$ by $\psi(f) = a$ and $\psi(r) = ba$. Then $\psi(f^2) = a^2 = e$ and

    $$\psi(fr^{-1}) = a(ba)' = aa'b' = b' = b = (ba)a = \psi(rf),$$

    so ψ is a homomorphism. We then compute $\psi \circ \phi(a) = a$,

    $$\psi \circ \phi(b) = \psi(rf) = baa = b,$$

    so $\psi \circ \phi$ is the identity. Similarly $\phi \circ \psi$ is the identity, so these two groups are isomorphic.

32. *Generators and relations of S_n.* Theorem. S_n has generators $\tau_i = (i, i+1)$, $i = 1, \ldots n-1$, with relations

    $\tau_i^2 = e$;
    $\tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1}$; and
    $\tau_i \tau_j = \tau_j \tau_i$ if $|i - j| > 1$.

    Proof. To check the main relation, let $(i, i+1, i+2) = (i, j, k)$; then we have: $(ij)(jk)(ij) = (ik) = (jk)(ij)(jk)$. So there is a map of the group above to S_n, and since adjacent permutations generate, it is *onto*.

    Now by the picture of changing crossings, it is clear that any two diagrams of the same permutation differ by these relations. ∎

33. Cor. The parity of an element in S_n is well-defined.

Proof. The relations preserve parity. Alternatively, define a map from S_n to $\mathbb{Z}/2$ by sending each τ_i to one, and observe that the relations are satisfied. ∎

34. *Trivial groups.* It is not always easy to tell whether or not a presentation is just giving the trivial group. For example, $\langle a : a^{12} = e, a^{25} = e \rangle$ is trivial.

4 Knot Theory

4.1 Knots and links

1. *Introduction.* What is a knot? It is a smooth closed curve in 3-space. A knots is not allowed to cross itself. A knot can be moved a little so it is a polygon. We do not allow wild knots.

   Two knots K_0 and K_1 are *equivalent* if you can make a smoothly moving family of knots K_t that connects them. You can imagine this motion taking place in discrete steps, $K_0, \ldots, K_n$, where K_i and K_{i+1} differ by a triangle move.

   A *link* is defined similarly as a finite number of disjoint closed loops.

2. *Knot projections.* A useful way to discuss knots is by projections: you put the knot almost in a plane, with pairs of strands meeting at crossings.

   Any knot can be given a knot projection; in fact a generic projection will work. You just have to avoid the directions tangent to the knot, and the directions of lines passing through the knot in 3 points (taken with multiplicities). Each forms a one-dimensional set.

3.

4. *Examples.*

   (a) The unknot. There are several projections. Any knot projection with 0, 1 or 2 crossings is the unknot. Any knot projection you can draw without anticipating crossings is the unknot.

(b) The trefoil knot, 3_1.

(c) The figure-eight knot, 4_1.

(d) The (p, q)-torus knot. You start with q strands and form a braid of the form β^p, where β is a cyclic permutation; then close. If p and q are relatively prime, you get a knot. The $(1, 3)$ torus knot is the unknot; $(2, 3)$ is the trefoil.

(e) The unlink on two components.

(f) The Hopf link.

(g) The Borromean rings, after the Renaissance family crest of the Borromeas.

5. *History.* Lord Kelvin conjectured that atoms are knots in ether. Tait and Little undertook the tabulation of knots. In recent times biologists have discovered that DNA is often knotted. The classification of 3-dimensional spaces is intimately tied up with knot theory.

6. *Showing two knots are the same.* Suppose K_1 and K_2 are projections that happen to correspond to the same knot. Then you can transform K_1 to K_2 be a sequence of *Reidemeister moves* (or their inverses). These moves are:

   I Transform one strand into a loop with one crossing. The singularity is a cusp.

   II Transform two parallel strands by adding two crossings. The singularity is a tangency.

   III Transform three strands preserving the number of crossings. The singularity is a triple-point.

   The Reidemeister moves can be remembered by the number of strands they involve. Planar isotopy is also allowed. The Reidemeister moves also work for links.

7. *Proof.* One way to approach the proof is to consider what kinds of singularities can arise as you view a generic knot projection during isotopy. The generic singularities are cusps, tangencies and triple points, accounting for the 3 moves.

8. Example: Draw a trefoil with one crossing wrong. This can be undone by the sequence III, I, II.

   Example: Tangle up the trefoil.

   Example: For each crossing of 6_3, change it and simplify the result.

4.2 Linking number and tricoloring

1. *Oriented knots and links.* A knot or link is *oriented* if we have chosen a direction (usually indicated by an arrow) to traverse each component. A link with n components has 2^n possible orientations.

2. *Showing two links are different.* Let $L = K_1 \cup K_2$ be a two component oriented link. The *linking number* $\ell(K_1, K_2)$ is defined as follows: at each crossing between K_1 and K_2, count $+1$ if it is a right-hand turn to get onto the overpass, otherwise -1. Add up and divide by two; this is $\ell(K_1, K_2)$.

3. Theorem. The linking number is an *invariant* of L. Even though it is defined using a projection, the answer for two different projections is the same.

   Proof. Type I moves don't involve both components. A type two moves creates a pair of crossings of opposite sign. And type III doesn't really change any pair of strands, only the configuration of all three. ∎

4. Examples: the unlink, Hopf link and Whitehead link.

5. *Unoriented links.* The *absolute value* of the linking number is independent of orientation.

6. *Tricoloring.* We still haven't shown there are any real knots. To do this, let's say a *tricoloring* of a knot or link projection is an assignment of colors R, G, B to the arcs such that:

   1) at least 2 colors are used; and at each crossing either
   2a) all three strands have the same color or
   2b) all three strands have different colors.

7. Theorem. If one projection of a knot or link can be tricolored, then they all can.

   Proof. We must check the Reidemeister moves.

   > (I) The entire loop must be a single color.
   > (II) If the parallel strands are colored R and G, then we color the underloop B.
   > (III) If 3 colors appear, then a crossing where 3 colors are the same either appears or disappears.

   In all 3 cases, if 2 colors were used before, then 2 are used after (see especially 2, which can increase the number of colors from 2 to 3).

8. Example. The unknot cannot be tricolored.

   Example. The trefoil *can* be tricolored. Thus the trefoil is really knotted!

   Example. The figure 8 knot cannot be tricolored. Thus tricoloring is not powerful enough to detect all knots.

9. *Connect sum and colorings.* Example. The connect sum of 2 trefoils can be tricolored in 11 different ways. (!) The point is that we can use a 1-coloring on one factor so long as it hooks up with a 3-coloring on the other factor.

   The *number* of tricolorings is also an invariant of the knot or link.

10. Example. Let L be the unlink on 2 components. Then L can be tricolored with 2 colors — if drawn with no crossings — and with 3 colors — if drawn with 2 crossings.

4.3 The fundamental group

1. *Examples of* $\pi_1(X)$. The disk, the annulus, the circle, the figure eight, the torus, the torus with a hole, a surface of genus two.

2. *The knot group.* This is the group of flight plans for airplanes leaving from a base located outside the knot and flying around it.

   Examples: For the unknot, $G(K) = \mathbb{Z}$. For the unlink on two components, $G(L) = Z * Z$.

3. *Presenting a knot or link group.* There is one generator for each arc of the knot projection. To each arc we associate a generator of $\pi_1(\mathbb{R}^3 - K)$ that makes a right-handed underpass for that arc. (This means as one moves along the generator, one can make a safe right-hand turn to get on the superhighway.)

   Now write ab for the loop that does a first, then b. Then when c crosses over $a - b$, so that we have a right-hand underpass, we get $ac = cb$. At a left-handed underpass, we get $ca = bc$.

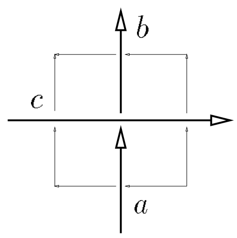

Figure 1. Proof that $ac = cb$ at safe underpass.

4. *The trefoil knot group.* We can now finally return to the trefoil knot. In the picture with all safe crossings, the group is

$$G(K) = \langle a, b, c \ : \ ab = bc, bc = ca, ca = ab \rangle.$$

5. *Mapping $G(K)$ to $\mathbb{Z}$.* This is easy: define $\phi(a) = \phi(b) = \phi(c) = 1$. It works for every knot group.

6. *Mapping $G(K)$ to S_3.* Notice that S_3 has 3 transpositions, call them A, B, C; they are all the odd permutations. They must satisfy $AB = CA$, since ABA is odd, it can't be A (else $A = B$) and it can't be B (else S_3 is commutative). Mapping (a, b, c) to (A, B, C) we see G admits S_3 as a quotient!

   Cor. The trefoil knot really *is* knotted.

7. Theorem. The tricolorings of a knot correspond one-to-one to the surjective homomorphisms $\phi : G(K) \to S_3$.

   Proof. Let A, B, C be the three flips in S_3 as before. Since the generators of $G(K)$ correspond to arcs, we can use the three colors to define a map $\phi : G(K) \to S_3$ on the generators. Then the tricoloring condition shows that each relation in $G(K)$ is satisfied. So we can map the generators for strands of color A to flip a, etc. Since at least two colors are used, we get a surjective map.

Similarly, if we have a surjection, then the generators (all being conjugate) must go to flips, else the image would be in the abelian subgroup of rotations. We then obtain a coloring. ∎

Note: for a link the statement above is not quite true. A homomorphism that kills one component of a link does not correspond to a coloring. That is the tricolorings correspond to maps to S_3 that send all generators of the Wirtinger presentation to flips.

8. *Changing presentations.* To prove $G(K)$ is a knot invariant, not just an invariant of the knot projection, it is important to understand elementary (or Tietze) moves on a presentation. There are just two:

   (1) $\langle g_i \,:\, r_i\rangle \iff \langle g_i \,:\, r_i, s\rangle$, where s is a consequence of the given relations. That means s is a product of conjugates of the r_i.

   (2) $\langle g_i \,:\, r_i\rangle \iff \langle g_i, h \,:\, r_i, h = w(g_1, \ldots , g_n)\rangle$, where $w(\cdot)$ is a word in the generators g_i. This means we can add a new generator so long as we add a relation putting it in the group generated by the (g_i).

9. *Example.* The trefoil group can be simplified to 2 generators, one relation.

10. *Invariance of $G(K)$.* Theorem. Equivalent projections of a knot (or link) give isomorphic groups $G(K)$.

    Proof. We must check the Reidemeister moves. (I) A loop gives $\langle a, b \,:\, aa = ba\rangle$, so we can use Tietze move (2) to eliminate b.

    (II) Suppose the arc a is underpassed by (b, c, d). Then we get from the 2 crossings the relations $ba = ac, ac = da$. From this we derive $b = d$ (Tietze 1), then eliminate c, d (Tietze 2). We are left with a, b and no relations, which is the contribution of two parallel arcs.

(III) Let the topmost arc be c, NW to SE, over (a, d), SW to NE, with finally (b, f, e) passing W to E under a and c. The 3 crossings give the relations

$$R = \langle ac = cd, ab = fa, fc = ce \rangle.$$

See Figure 2.

We can obtain the relation $aba' = cec' = f$, and then eliminate f, giving the new set of relations

$$R' = \langle ac = cd, aba' = cec' \rangle$$

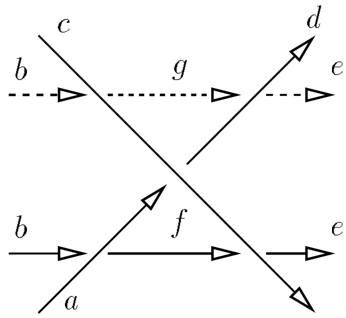

Figure 2. Reidemeister move III.

After the Reidemeister move we get a new arc g and relations

$$S = \langle ac = cd, bc = cg, dg = ed \rangle.$$

We can obtain the relation $c'bc = d'ed = g$, and eliminate g, obtaining

$$S' = \langle ac = cd, c'bc = d'ed \rangle.$$

We now must show the two sets of relations R' and S' are equivalent. To see this, we will use the relation $ac = cd$, present in each group. Then the relation $c'bc = d'ed$ in S', implies the relation $(ac)c'bc(ac)' = (cd)d'ed(cd)'$, which simplifies to the relation $aba' = cec'$ in R'. The process can be reversed, so indeed the groups are isomorphic.

11. *Search for cycles.* If we want to find a quotient $\phi : G(K) \to F$, it is *very useful* to note that the standard generators of a knot group are all conjugates. Thus the images of these generators must also be conjugate, and generate F (if ϕ is to be surjective.)

    With this in mind, we can see that a natural choice for the trefoil group is S_3, the symmetries of a triangle, since it has three edges. We map each generator to the flip of the edge, and this gives ϕ.

12. *The figure 8 group.* We have the presentation

    $$G = \langle a, b, c, d \ : \ da = bd, ba = ac, bc = db, dc = ca \rangle.$$

    Now the elements a, b, c, d are *all conjugate* in G. So if we try to find a map $\phi : G \to F$, where F is a finite group, then the images of a, b, c, d all have the same order — and indeed they are all conjugate. So we need a group with 4 conjugate elements, that generate the group.

    A nice candidate is $F = A_4$, the symmetries of a tetrahedron T. The motivation is that T has 4 faces, corresponding to the generators of G, just like the edges of the triangle did for the trefoil knot.

    The clockwise rotations of a face are the permutations $(123), (134), (243)$ and (142). Any two faces stand in the same relation, so we may as well send a to (123) and d to (134).

    Then the first relations gives $b = dad' = (432)$, and the second gives $c = a'ba = (421)$. We can then check that the last two relations are satisfied.

13. *Geometric check.* Another way to think about the relations in the figure 8 group is to let a, b, c, d correspond to faces A, B, C, D of the tetrahedron. Then an equation like $b = dad'$ is equivalent to $B = d(A)$. So we get the relations $B = d(A), C = a'(B), D = b(C)$ and $D = c(A)$. Once A and D are chosen, the first two relations specify C and B, and then we can check the last two.

14. *Trefoil $\neq$ Figure Eight.* Theorem. There is no surjection from the trefoil group to A_4. Thus the unknot, the trefoil and the figure eight knot are all distinct.

    Proof. Let $\phi : G \to A_4$ be a surjective homomorphism from the trefoil group to A_4. Since the generators are all conjugate, they all have the same order, which must be 1, 2 or 3. But the elements of order 2 in A_4 generate a proper V_4 subgroup, so the order must be 3. Moreover two generators must map to different elements, else the image would be $\mathbb{Z}/3$.

Up to symmetry we can then take the images of the generators to be $a = (123)$ and $b = (134)$. Then the relations $ab = bc = ca$ imply $c = b'ab = (432)$, but we then find $bc = (321) \neq ca = (431)$.

15. *Hopf link.* The Hopf link L is *less knotted* than the unlink, since $G(L) \cong \mathbb{Z} \oplus \mathbb{Z}$. As a trick, one can weave the commutator through two unlinked carabiner, in such a way that the loop comes free when the carabiner are linked! (Cf. homework on computing $G(L)$.)

16. Theorem. The linking number for $L = K_1 \cup K_2$ corresponds to the abelianization of the element of $\pi_1(\mathbb{R}^3 - K_1)$ represented by K_2.

    (Cf. Homework on computing a map $G(K) \to \mathbb{Z}$.)

    Proof. The proof is a little tricky. Working with a link projection, one can first change crossings of K_2 with itself so K_2 becomes the unknot. This change does not change our projection-based calculation of the linking number (obviously), nor does it change the image of K_2 in $\pi_1(\mathbb{R} - K_1)$ (obviously).

    Now re-arrange the projection so K_2 is a counter-clockwise round circle. It is then clear that the number of outward-heading crossings of K_1 with K_2 is the same as the number of inward-heading crossings.

    Count the crossings in 4 groups, TO, BO, TI, BI, where T/B means K_1 is on top/bottom, and O/I means it is headed out/in. Letting P be the link number in π_1, and L the linking number from the diagram, we have

$$\begin{aligned} TO + BO &= TI + BI \\ L &= (TO + BI - TI - BO)/2 \quad \text{and} \\ P &= TO - TI. \end{aligned}$$

Using the first equation we have $P = BI - BO$; averaging these two expressions for P, we obtain $P = L$. ∎

17. Theorem (Gordon-Luecke) Let $(G(K), H(K))$ be a knot group and a subgroup $H(K) \cong \mathbb{Z}$ generated by a meridian. Then K is equivalent to K', or its mirror image, iff there is an isomorphism $G(K) \cong G(K')$ sending $H(K)$ to $H(K')$.

    The $H(K)$ is needed for the square and granny knots, which have isomorphic groups. Often the $H(K)$ is unnecessary.

4.4 Knot polynomials

1. *Introduction.* Our final knot/link invariant will be a *Laurent polynomial* $X(L)$ in one variable A, discovered (in a different form) by Vaughn Jones less than 20 years ago (1984).

   To define it we begin with the Kaufmann bracket $\langle L \rangle$, also a polynomial, defined for a knot projection by:

   (i) $\langle O \rangle = 1$;
   (ii) $\langle L \rangle = A\langle L_r \rangle + A^{-1}\langle L_\ell \rangle$; and
   (iii) $\langle L \cup O \rangle = -(A^2 + A^{-2})\langle L \rangle$.

   Here L_r and L_ℓ are obtain from L by focusing on one undercrossing and replacing it with safe, right on-ramps (L_r) or unsafe, left onramps (L_ℓ). The circle O denotes the unknot.

2. Example. For the unknot with one twist, $\langle L \rangle = -A^3$ (or $-A^{-3}$, depending on the direction of the twist).

3. Example. For the Hopf link, we have

$$\langle H \rangle = -A^4 - A^{-4}.$$

4. Exercise: why is $\langle L \rangle$ well-defined? Why doesn't it depend, for example, on the order in which we resolve crossings?

5. *Reidemeister II.* This move leaves $\langle L \rangle$ unchanged, as an easy computation shows.

6. *Reidemeister III.* By resolving the middle crossing in two different ways, then applying move II, we see that Reidemeister move III also leaves $\langle L \rangle$ unchanged.

In fact, equations (ii) and (iii) are chosen just to insure that I and II leave the bracket invariant, and (i) is just a normalizing factor.

7. *Reidemeister I.* Now let L_s denote L with a safe loop added by Reidemeister move I. Then we have

$$\langle L_s \rangle = (-A^3)\langle L \rangle.$$

8. *The writhe.* To account for these changes, we use another invariant of a projection that is affected by move I but not moves II or III. This is the *writhe* $w(L)$ or 'self-linking number' of a knot or link, obtained by adding up the signs of *all* self-crossings.

   Note that the writhe of a *knot* does not depend on an orientation — while the writhe of a link *does*. It is *not* an invariant of the knot; for example, a single twist gives the unknot writhe ± 1.

   The writhe is unaffected by moves II and III for the same reason that the linking number is an invariant. But Reidemeister move I changes it: we have

$$w(L_s) = w(L) + 1.$$

9. *The polynomial $X(L)$.* We can combine the writhe with the bracket polynomial to get an honest invariant of an oriented link, namely:

$$X(L) = (-A^3)^{-w(L)}\langle L \rangle.$$

   The reason this works is that:

$$\begin{aligned} X(L_s) &= (-A^3)^{-w(L_s)}\langle L_s \rangle \\ &= (-A^3)^{-w(L_s)-1}(-A^3)\langle L \rangle \\ &= X(L). \end{aligned}$$

10. *The Hopf link revisited.* Give both components the same orientation; then both crossings are positive, so we must multiply the bracket by $(-A^3)^{-2} = A^{-6}$, and we then obtain $X(H) = -A^{-2} - A^{-10}$.

11. *Knot without orientations.* Reversing the orientation does *not* change the writhe of a knot, and does not affect the bracket polynomial. Thus $X(K)$ is an invariant of *unoriented* knots.

12. *Mirror images.* If we replace K by its mirror image $-K$, then we $\langle -K \rangle$ is just $\langle K \rangle$ with A replaced by A^{-1}. Similarly, $w(-K) = -w(K)$ — safe and unsafe crossings are interchanged. Therefore $X(-K)(A)$ is $X(K)(A^{-1})$.

13. *The positive trefoil.* Let T be the trefoil 3_1^+, with all 3 crossings positive. Then $w(T) = 3$. The bracket polynomial is given by

    $$\langle T \rangle = A^{-7} - A^{-3} - A^{5}.$$

    Multiplying by $(-A^3)^{-3}$, we obtain

    $$X(T) = -A^{-16} + A^{-12} + A^{-4}.$$

    The fact that the polynomial is *not* symmetric proves that trefoils come in two types, right and left handed! That is,

    $$X(-T) = A^{4} + A^{12} - A^{16}.$$

    (*Note:* Adams' table shows 3_1^-, the mirror image of 3_1^+.)

14. *The figure eight knot.* Start with K the projection of 4_1 in Adams' tables, then change the crossings at the top. The two resulting knots are the Hopf link with a safe twist and the positive trefoil. Using the rule for Reidemeister move I, we find

    $$\langle K \rangle = A\langle H_s \rangle + A^{-1}\langle T \rangle = A(-A^3)\langle H \rangle + A^{-1}\langle T \rangle.$$

    We already computed $\langle H \rangle = -A^{-4} - A^{4}$ and $\langle T \rangle = A^{-7} - A^{-3} - A^{5}$, from which we find:

    $$\langle K \rangle = A^{-8} - A^{-4} + 1 - A^{4} + A^{8}.$$

    In addition, $w(K) = 0$, so we get $X(K) = \langle K \rangle$.

15. *Jones' polynomial.* In all our examples of $X(T)$ we see only 4th powers of A. To get a simpler expression, the *Jones polynomial* $V(L)$ is defined by replacing A with $t^{-1/4}$. Thus

    $$V(3_1^+) = t + t^3 - t^4,$$

    and

    $$V(4_1) = t^{-2} - t^{-1} + 1 - t + t^2.$$

16. *Computational complexity.* The most straightforward computation of $X(K)$ takes 2^c steps where c is the number of crossings of K.

17. *Quantum field theory.* One can think of the crossings of a knot as undergoing fluctuations, to different states with different energies. Weighting the states by their energies we get the *partition function* which is the knot polynomial. The variable is then related to the temperature of the system (statistical mechanics).

18. *An unsolved problem.* The Jones polynomial, or its variant $X(K)$, gives different answers for every knot with 9 or fewer crossings.

    The *only known knot* with $X(K) = 1$ is the unknot.

4.5 Immersed spheres

1. *The time traveler.* Suppose at noon we begin to travel in time, making the dial move on the clock in side our time machine. It goes around and around, maybe forward, maybe back — but at the end the clock says 12:00 again. Now we have traveled a definite integral numbers of half-days n – this is the *winding number* of the hand around the clock. The actual return is to the present plus $n/2$ days. (Even though n may be negative.)

2. *Circle eversion.* Can you turn the circle inside out? Consider changing closed immersed loops in the plane by the three Reidemeister moves. Then it turns out to be possible to evert the circle — just apply II followed by two I's.

   Now let's rule out I's, since they can't be done continuously without pinching. Then the circle cannot be everted!

3. *Degree.* To prove that C and $-C$ are not equivalent, we must put an arrows on our loops. Now given an arrow, we can walk around the loop, with a clock whose hour hand points in the direction of travel. If we start at an upward heading point, then we begin and end at 12:00. The *degree* of the loop is the (signed) number of 12 hour periods our clock has turned by the time we come back.

   The degree is always an integer. So if you move the loop gradually, this integer can never change! But $d(-C) = -d(C)$ so the circle cannot be everted.

4. *Smiles and frowns.* One way to compute the degree is to count the number of frowns, minus the number of smiles, where the time is 3pm.

5. *Turning the sphere inside out.* Incredibly, a 2-sphere can be turned inside out through immersions.

5 Summary

1. **Sets.**

   (a) Axioms. $A \in B$.

   (b) Paradoxes. Let $S = \{A : A \notin A\}$. Then is $S \in S$? The barber of Seville.

   (c) $0 = \{\}$, $n + 1 = n \cup \{n\}$.

   (d) Sizes of infinity (Cantor): $|\mathcal{P}(A)| > |A|$. A line ($\mathbb{R}$) is bigger than $\mathbb{N}$.

   (e) Schröder-Bernstein. $|A| \leq |B|$ and $|B| \leq |A|$ implies $|A| = |B|$.

2. **Groups.**

   (a) Axioms.

   (b) Isomorphism. Classification of groups of order up to 7.

   (c) Cyclic groups. Every subgroup of $\mathbb{Z}$ is cyclic. $\langle a, b\rangle = \gcd(a, b)\mathbb{Z}$. $(a\mathbb{Z}) \cap (b\mathbb{Z}) = \mathrm{lcm}(a, b)\mathbb{Z}$. a generates $\mathbb{Z}/n$ iff $\gcd(a, n) = 1$.

   (d) The Cayley graph.

   (e) Lagrange: $H \leq G \implies |H|$ divides $|G|$. The order of any quotient of G also divides $|G|$.

   (f) Group actions. $|A| = |G|/|\operatorname{Stab}(a)|$.

   (g) Examples: $\mathbb{Z}/n$, S_3, S_n, A_n (sliding puzzle), D_n, V_4, the quaternion group Q_8, $SL_2\mathbb{Z}$, the free group on 2 generators.

   (h) 5 Platonic solids, 3 groups: A_4, S_4, A_5. Kepler.

   (i) Homomorphism and quotient groups.

   (j) Normal subgroups and group presentations.

3. **Knots.**

   (a) Isomorphism (equivalence).

   (b) Knot and link projections and Reidemeister moves.

   (c) The unknot, unlink, Hopf link, trefoil, figure eight and Borromean rings.

   (d) Tricoloring — an invariant.

   (e) Linking number.

   (f) The knot and link group.

   (g) The fundamental group of space.

   (h) The Wirtinger presentation for $G(K)$.

   (i) The trefoil group maps to S_3, the figure eight group maps to A_4, the Hopf link has $G(L) = \mathbb{Z}^2$, the unlink has $G(L) = \mathbb{Z} * \mathbb{Z}$.

   (j) The carabiner trick.

   (k) Knot polynomials. The bracket and the writhe.

   (l) Unsolved problem: does $X(K) = 1$ imply K is unknotted?

   Turning the sphere inside out.