

Pre-algebra

- Three ways to prove an implication are the *direct* method, the *contrapositive* method, and the *contradiction* method.
- The *Principle of Mathematical Induction*, which everyone should know, is used to prove statements for all integers in some set $S \subseteq \mathbb{Z}$ which is bounded below, such as \mathbb{N} .
- A *relation* \mathcal{R} on a set S is a subset of $S \times S$. Each relation on S can be represented as a directed graph: the vertex set is S and $a \longrightarrow b$ iff $a\mathcal{R}b$.
- An *equivalence relation* \sim on a set S is a relation on S which is *reflexive*, *symmetric*, and *transitive*.
- Every equivalence relation \sim on S *partitions* S into cells; the cells are the *equivalence classes* under \sim . Conversely, any partition on S induces an equivalence relation on S . Two elements $a, b \in S$ lie in the same cell iff $a \sim b$.
- The connected components of the directed graph associated with an equivalence relation correspond to the cells of the induced partition.
- If $\phi : X \rightarrow Y$ is a function between sets, $A \subseteq X$, and $B \subseteq Y$, you have the *image* of A , $\phi(A) \subseteq Y$, and the *inverse image* of B , $\phi^{-1}(B) \subseteq X$.
- A function $\phi : X \rightarrow Y$ is an *injection* if it is one-to-one, a *surjection* if it is onto, and a *bijection* if it is both.
- Every complex number $z \in \mathbb{C}$ can be written in *polar form*: $z = |z|(\cos \theta + i \sin \theta) = |z|e^{i\theta}$, where $|z|$ is the distance in the complex plane between 0 and z , and θ is the angle between the positive real axis and the vector from 0 to z , measured counter-clockwise. Polar form illustrates a geometric interpretation of complex multiplication: $z_1 z_2 = |z_1||z_2|(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$. In other words, their moduli are multiplied while their angles are added. Consequently, multiplication of complex numbers on the unit circle $U = \{z \in \mathbb{C} \mid |z| = 1\}$ is completely determined by the angles of the two numbers. And so the *n th roots of unity*, the solutions of $z^n = 1$, are the n complex numbers (including 1) spaced evenly around the unit circle.

Groups and Subgroups

- A *group* is a set G closed under a binary operation such that the operation is associative, G has an *identity* element, and each element in G has an *inverse* (in G).

- A *subgroup* of a group is a subset which is itself a group (under the same binary operation).
- The “typical” way to show a subset of a group is a subgroup is to show it is closed, contains the identity element, and contains all its inverses.
- Not every subset of a subgroup is a subgroup. Take any group G and $H = G - \{e\}$ for a counterexample.
- The simplest type of groups are *cyclic*; they can be generated by a single element.
- Each cyclic group is either isomorphic to \mathbb{Z} or \mathbb{Z}_n for some n .
- All subgroups of cyclic groups are cyclic.
- *Abelian* groups are those with commutative binary operations.
- All subgroups of abelian groups are abelian.
- Every cyclic group is abelian, but the converse is false; the smallest abelian non-cyclic group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- Every finitely-generated abelian group is isomorphic to a direct product of cyclic groups by the Fundamental Theorem of Finitely Generated Abelian Groups.
- Not all groups are finitely generated; \mathbb{Q} (under $+$, of course) has no finite generating set.
- Not all groups are abelian. The smallest non-abelian group is $S_3 \cong D_3$, but others include S_n ($n > 3$), D_n ($n > 3$), and $GL(n, \mathbb{R})$.
- A subgroup of a nonabelian group may be either abelian or nonabelian. Think of $\mathbb{Z}_2 \cong \{(1), (1, 2)\} \leq S_3$ for the former.
- Every subgroup $H \leq G$ partitions G into *left cosets* (each of the form gN for some $g \in G$) and also into *right cosets* (each of the form Ng for some $g \in G$). These partitions are not necessarily the same; for example, $H = \{\rho_0, \mu_1\}$ induces different partitions of S_3 .
- Lagrange’s Theorem concludes, in the case that G is finite, that $|H|$ must divide $|G|$ for every subgroup H . But if $n \mid |G|$, there is not necessarily a subgroup of G of order n (there *is* if G is abelian); it can be shown that A_4 has no subgroup of order 6 even though $6 \mid \frac{4!}{2}$.
- Given a generating set $X \subseteq G$, the Cayley graph of G with respect to X is the directed graph with vertex set G and edges which illustrate the multiplication of G . Every vertex has an edge entering and leaving it for each generator in X . Paths in the Cayley graph correspond to “words” in the generators, and closed paths correspond to words which equal the identity in G . G is abelian iff each path corresponding to the word $xyx^{-1}y^{-1}$ (for any $x, y \in X$) is closed.

Group Homomorphisms

- A *homomorphism* is a structure-preserving function from one group to another.
- Homomorphisms send identities to identities, inverses to inverses, and subgroups to subgroups. In addition, the inverse image (under a homomorphism) of a subgroup is a subgroup.
- Not every function from one group to another is a homomorphism. Take any function that doesn't map the identity of the domain to the identity of the codomain for a counterexample.
- If $\phi : G \rightarrow G'$ is a homomorphism, then $\phi(G)$ can be thought of as G "partially collapsed." If ϕ is an injection, then $G \cong \phi(G)$.
- An *isomorphism* is a bijective homomorphism.
- If $\phi : G \rightarrow G'$ is a group homomorphism, then

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

- If $\phi : G \rightarrow G'$ is a group homomorphism, then there is a bijection between the cosets of $\ker \phi$ and the elements of $\phi(G)$.
- An *automorphism* is an isomorphism from a group to itself. An *inner automorphism* is an automorphism of the form (for some $g \in G$) $i_g : G \rightarrow G$ given by $x \mapsto gxg^{-1}$.

Basics of Rings and Subrings

- A *ring* R is an additive abelian group with an additional multiplicative structure which is associative and distributes (both left and right) over the additive operation. Write 0 for the additive identity and 1 for the multiplicative identity, if there is one.
- If a ring has 1, it is called *unity*. Elements with multiplicative identities are called *units*. A nonzero element $a \in R$ is a *zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$.
- Not all rings are commutative. For example, $M_2(\mathbb{R})$, which has $2^4 = 16$ elements, is a noncommutative ring (with 1).
- Not all rings have 1. For example, $2\mathbb{Z}$ is a commutative ring without 1.
- $M_2(2\mathbb{Z})$ is a noncommutative ring without 1.
- \mathbb{Z}_6 is a nice example of a finite ring, since it has both units (1 and 5) and zero divisors (2, 3, and 4).

- A *subring* is a subset of a ring that is itself a ring. To show $S \subseteq R$ is a subring of R , it suffices to show $(S, +) \leq (R, +)$ and S is closed under multiplication.
- If R has 1 and S is a subring of R , then it is possible for S to have a multiplicative identity different from that of R . For example, $\{0, 2, 4\}$ forms a subring of \mathbb{Z}_6 , but 4 acts as the multiplicative identity in $\{0, 2, 4\}$. So $\{0, 2, 4\}$ is a subring with 1 but not a sub(ring with 1).
- The *characteristic* of a ring R , $\text{Char}(R)$, is the least positive integer n such that $\forall r \in R, n \cdot r = 0$. If no such n exists, then $\text{Char}(R) = 0$. So $\text{Char}(\mathbb{Z}_m) = m$, while $\text{Char}(\mathbb{Z}) = 0$.

Ring Homomorphisms

- A *ring homomorphism* is structure-preserving function from one ring to another. It must preserve both the additive and multiplicative structures of the ring, so it has two properties while a group homomorphism only has one property. These two properties guarantee that the distributive laws are preserved.
- If $\phi : R \rightarrow R'$ is a ring homomorphism, then

$$\ker \phi = \{r \in R \mid \phi(r) = 0\}.$$

- If $\phi : R \rightarrow R'$ is a ring homomorphism, then not only is $\ker \phi$ a subring of R , but it also possesses the property that $\forall r \in R, \forall k \in \ker \phi, kr, rk \in \ker \phi$.

Special rings

- R is a *division ring* or *skew field* if every nonzero element of R is a unit.
- R is a *field* if it is a commutative division ring.
- R is an *integral domain* if it is a commutative ring with $1 \neq 0$ and it contains no zero divisors.
- \mathbb{Q}, \mathbb{R} , and \mathbb{C} are all fields. If p is prime, then \mathbb{Z}_p is a field. \mathbb{Z} is not a division ring (and hence not a field) but it is an integral domain. The quaternions are a division ring but not a field. (There are no finite division rings that aren't fields; this is not obvious.)
- Every field is an integral domain, but the converse is false (consider \mathbb{Z}).
- Every finite integral domain is a field, but the converse is false. (Obviously; consider \mathbb{Q} .)

- Every integral domain D embeds into its *field of quotients*, F . F is the “smallest” field containing D in the sense that if L is any other field containing D , then F is isomorphic to a subfield of L .

$$\begin{array}{ccc}
 & & L \\
 & & \uparrow \\
 F & \xrightarrow{\psi(\cong)} & \psi(F) \\
 \uparrow & & \uparrow \\
 D & \xlongequal{\quad} & D
 \end{array}$$

Polynomial rings

- If R is a commutative ring with 1 and x is an indeterminate, then the set of polynomials in x with coefficients in R , denoted $R[x]$, is a commutative ring with 1. We are mostly interested in the case where R is a field.
- If $F \leq E$ are fields and $\alpha \in E$, then the map $\phi_\alpha : F[x] \rightarrow E$ given by $f(x) \mapsto f(\alpha)$ is a homomorphism, called *evaluation at α* . If $f(\alpha) = 0$, we say α is a *zero* of f .
- If F is a field, then $F[x]$ is an integral domain, and a version of the division algorithm holds for $F[x]$, where the degree function $\deg : F[x] \rightarrow \mathbb{N} \cup \{-\infty\}$ is used to determine the “size” of an element of $F[x]$. As a consequence, we have the *Factor Theorem*, which states that $a \in F$ is a zero of $f(x) \in F[x]$ iff $(x - a) \mid f(x)$, and also we have the fact that a nonzero polynomial in $F[x]$ of degree n can have at most n zeros.
- *Irreducible* polynomials in $F[x]$ play the same role as prime numbers do in \mathbb{Z} . In particular (among other things),
 - ◇ every nonconstant polynomial can be factored uniquely (up to order and constant factors) as a product of irreducibles.
 - ◇ If $p(x)$ is irreducible and $p(x) \mid f(x)g(x)$, then $p(x) \mid f(x)$ or $p(x) \mid g(x)$.
- In the special case where $F = \mathbb{Q}$, we have some particular results:
 - ◇ $f(x) \in \mathbb{Z}[x]$ factors nontrivially over \mathbb{Q} iff it factors nontrivially over \mathbb{Z} (with the factors having the same degrees).
 - ◇ If $f(x) \in \mathbb{Z}[x]$ satisfies $f(0) \neq 0$, and f has a zero in \mathbb{Q} , then f has a zero m in \mathbb{Z} and $m \mid f(0)$.
 - ◇ We also have the *Eisenstein criterion* to test whether or not a polynomial in $\mathbb{Z}[x]$ is irreducible over \mathbb{Q} .