Abstract Algebra Notes

Cruz Godar

Math 481, 482, and 483/560
Professor Brussel
Cal Poly, Fall 2017–Spring 2018

I — Groups

Definition 1.1: A **group** is a set G equipped with a binary operation such that

1. $ab \in G$ for all $a, b \in G$.
2. $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. There is an $e \in G$ with $ae = ea = a$ for all $a \in G$.
4. For all $a \in G$, there is an $a^{-1} \in G$ with $aa^{-1} = a^{-1}a = e$.

Example: One important type of group is a *symmetry group*, formed by taking the collection S_X of symmetries of a set X — that is, structure-preserving bijections from X to itself. If $X = \mathbb{R}$, for instance, then S_X contains translational symmetries and stretching/shrinking ones.

Definition 1.2: Let $n \in \mathbb{N}$. The **integers modulo n** are the set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$. $\mathbb{Z}_n$ is a group, with the operation given by addition mod n.

Definition 1.3: Let $n \in \mathbb{N}$. The group $\mathbf{U(n)}$ is defined as $U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$, with the operation given by multiplication mod n.

Definition 1.4: The **dihedral group** of degree n is the the group D_n of symmetries of a regular n-gon, given by $D_n = \{e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$, where r is a rotation counter-clockwise by $\frac{2\pi}{n}$, s is a reflection over the x-axis, and the operation is function composition. Note that $sr = r^{-1}s$.

Definition 1.5: The **symmetric group** of degree n is the group S_n of permutations on n elements, defined as $\{\sigma : \{1, ..., n\} \twoheadrightarrow \{1, ..., n\}\}$, where each σ is a bijection and the operation is given by function composition. We use **cycle notation** to denote elements of S_n: the element $(124) \in S_4$, for example, denotes the function σ with $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(4) = 1$, and $\sigma(3) = 3$.

Definition 1.6: The **general linear group** of degree n over k is $GL_n(k) = \{A \in M_n(k) \mid \det A \neq 0\}$, with the operation given by matrix multiplication. Typically, k is $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}$.

Definition 1.7: The **special linear group** of degree n over k is $SL_n(k) = \{A \in M_n(k) \mid \det A = 1\}$, with the operation again given by matrix multiplication.

Definition 1.8: The **orthogonal group** of degree n is $O_n = \{A \in M_n(\mathbb{R}) \mid AA^{\mathrm{T}} = I\}$, and the **special orthogonal group** of degree n is $SO_n = \{A \in O_n \mid \det A = 1\}$. The **unitary group**, U_n, and **special unitary group**, SU_n, are defined identically, except their matrices are taken from $M_n(\mathbb{C})$ and require that $A\overline{A}^{\mathrm{T}} = I$.

Definition 1.9: The **order** of a group G is $|G|$. A **finite group** is one that has finite order.

Definition 1.10: A group G is **Abelian** if $ab = ba$ for all $a, b \in G$.

Proposition 1.11: Let G be a group. Then $e \in G$ is unique.

Proof: Suppose there were $e, e' \in G$ such that $ae = ea = ae' = e'a = a$ for all $a \in G$. Then $ee' = e$ and $ee' = e'$, so $e = e'$.

Proposition 1.12: Let G be a group. If $ab = ac$ for $a, b, c \in G$, then $b = c$, and similarly, if $ab = cb$, then $a = c$.

Proposition 1.13: Let G be a group and $a \in G$. Then a^{-1} is unique.

Proof: If there were $a^{-1}, \left(a^{-1}\right)' \in G$ such that $aa^{-1} = a^{-1}a = a\left(a^{-1}\right)' = \left(a^{-1}\right)'a = e$, then $aa^{-1} = a\left(a^{-1}\right)'$, so $a^{-1}aa^{-1} = a^{-1}a\left(a^{-1}\right)'$, and so $a^{-1} = \left(a^{-1}\right)'$.

Definition 1.14: Let G be a group. A set $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if H is itself a group under G's operation.

Example: For all groups, $\{e\} \leq G$, called the *trivial subgroup*, and $G \leq G$.

Example: If X is a regular, nonoriented n-gon and X' is a regular, oriented n-gon (so reflections count as symmetries of X, but not of X'), then $S'_X \leq S_X$.

Definition 1.15: $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group with its operation given by stretching and rotating the plane — $z = re^{i\theta}$ represents the symmetry of stretching by r and rotating by θ (or equivalently, moving 1 to z). $S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\} = \{z \in \mathbb{C}^* \mid |z| = 1\}$ is also a group under the same operation, so $S^1 \leq C^*$.

Definition 1.16: The **quaternions** are the set

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ijk = -1\}.$$

$\mathbb{H}$ forms a group under addition, and $\mathbb{H}^*$ a group under multiplication. Similarly to S^1, we define the **unit 3-sphere** as $S^3 = \{z \in \mathbb{H}^* \mid |z| = 1\} \leq \mathbb{H}^*$.

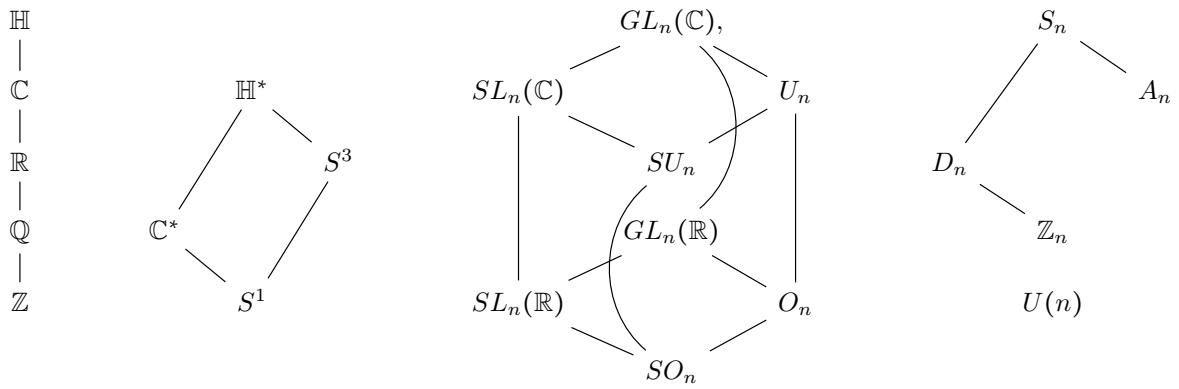
Proposition 1.17: Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if

1. $H \neq \varnothing$.
2. $ab \in H$ for all $a, b \in H$.
3. For all $a \in H$, $a^{-1} \in H$.

Proof: ($\Rightarrow$) If $H \leq G$, then the only statement to prove is that the identity of H is the same as that of G, so that we can be sure that $a^{-1} \in H$ is the same as a^{-1} in G. If the two identities are e_G and e_H, then $e_H e_G = e_H$ in G and $e_H e_H = e_H$ in H, so $e_H e_G = e_H e_H$ in G, and therefore $e_G = e_H$. Thus the inverses are the same, and so all three conditions are met.

($\Leftarrow$) Let $a, b, c \in H$ (which is valid, since H is nonempty). Then $a, b, c \in G$, so $(ab)c = a(bc)$. Also, since $a^{-1} \in H$ (and this is the inverse from G), $aa^{-1} = e_G \in H$. We already know H is closed under G's operation, so $H \leq G$.

Example: The major groups:



Definition 1.18: Let G be a group and $a \in G$. The **group generated by** a is $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Example: In D_n, $\langle r \rangle = \{e, r, r^2, ..., r^{n-1}\}$ and $\langle s \rangle = \{e, s\}$.

Definition 1.19: Let G be a group. The **order** of $a \in G$ is $|a| = |\langle a \rangle|$, or equivalently, the smallest $n \in \mathbb{N}$ such that $a^n = e$ if it exists, or ∞ if it does not.

Definition 1.20: The orders of the elements in $U(9) = \{1, 2, 4, 5, 7, 8\}$ are

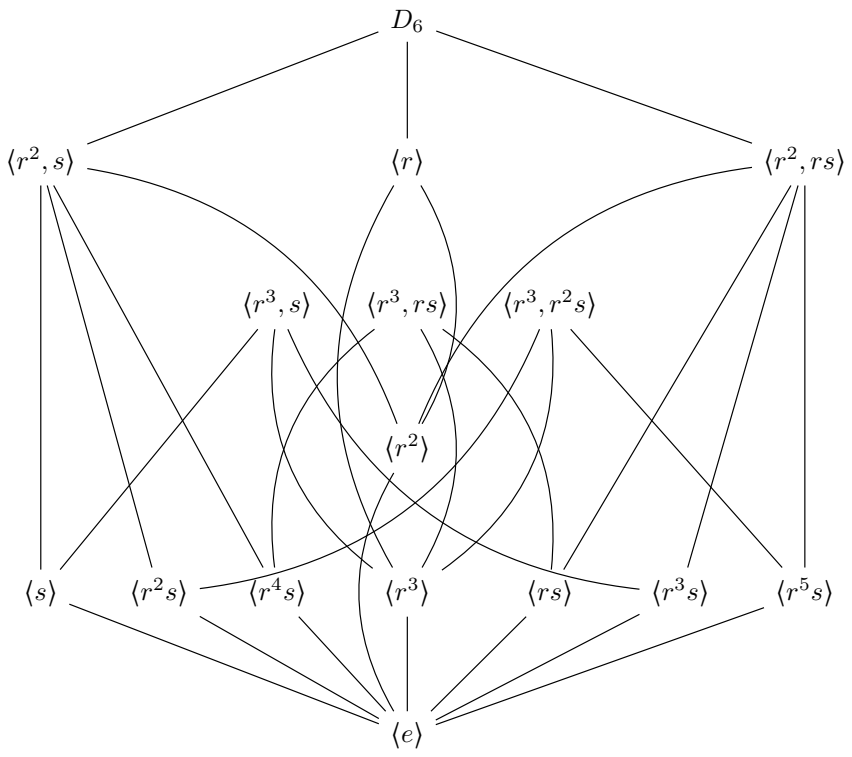
$$|1| = 1, \qquad |2| = 6, \qquad |4| = 3, \qquad |5| = 6, \qquad |7| = 3, \qquad |8| = 2.$$

Proposition 1.21: Let G be a group and $a \in G$. Then $|a| = \left|a^{-1}\right|$.

Proof: Since $a^k = e$ if and only if $\left(a^k\right)^{-1} = e$, if and only if $\left(a^{-1}\right)^k = e$, the smallest $n \in \mathbb{N}$ such that $a^n = e$ will also be the smallest $m \in \mathbb{N}$ such that $\left(a^{-1}\right)^m = e$. Thus $|a| = \left|a^{-1}\right|$.

Definition 1.22: A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$, called a **generator** of G.

Example: The subgroup lattice of D_6:

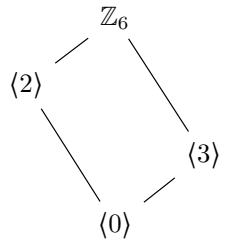


Theorem 1.23: A subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a\rangle$ and $H \leq G$. Then for all $h \in H$, $h = a^m$ for some $m \in \mathbb{Z}$. Let $S = \{m \in \mathbb{N} \mid a^m \in H\}$, let m_0 be the minimum element of S, and let $h = a^m \in H$ be arbitrary. Then $m = m_0q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < m_0$, so $a^m = a^{m_0q+r}$, or equivalently, $a^r = a^{m-m_0q}$. Since $a^m = h \in H$ and $a^{m_0q} = (a^{m_0})^q \in H$, $a^{m-m_0q} = a^r \in H$. Thus if $r \neq 0$, $r \in S$ by definition, but $r < m_0$, the smallest element in S. ↯ Thus $r = 0$, and so $h = (a^{m_0})^q$ for some $q \in \mathbb{Z}$. Since h was arbitrary, $H = \langle a^{m_0}\rangle$.

Example: Since $\mathbb{Z}$ is cyclic, every subgroup of $\mathbb{Z}$ is of the form $\langle a\rangle$ for $a \in \mathbb{Z}$.

Example: The subgroups of $\mathbb{Z}_6$ are $\langle 0\rangle$, $\langle 3\rangle$, $\langle 2\rangle$, and $\langle 1\rangle = \mathbb{Z}_6$.



Theorem 1.24: Let $G = \langle a \rangle$ be cyclic with $|G| = n$. Then for any $k \in \mathbb{N}$, $\left|a^k\right| = \frac{n}{\gcd(n,k)}$.

Proof: Let $d = \gcd(n, k)$. We claim $\langle a^k \rangle = \langle a^d \rangle$.

($\subseteq$) Since $d|k$, $k = dq$ for some $q \in \mathbb{Z}$. Then $a^k = \left(a^d\right)^q \in \langle a^d \rangle$, so $\langle a^k \rangle \subseteq \langle a^d \rangle$.

($\supseteq$) By Bezout's identity, $d = ks + nt$ for some $s, t \in \mathbb{Z}$, so $a^d = a^{ks+nt} = \left(a^k\right)^s (a^n)^t = \left(a^k\right)^s (e)^t = \left(a^k\right)^s \in \langle a^k \rangle$. Thus $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Now $\langle a^k \rangle = \langle a^d \rangle$, so in particular, $\left|a^k\right| = \left|a^d\right|$. We know $\left|a^d\right| = \frac{n}{d}$, since otherwise, if $\left|a^d\right| = m < \frac{n}{d}$, $a^{dm} = e$ amd $dm < n$, so $|G| = |a| < n$. ↯ Thus $\left|a^k\right| = \left|a^d\right| = \frac{n}{d}$.

Corollary 1.24.1: Let $G = \langle a \rangle$ with $|G| = n$. Then the generators of G are a^k with $\gcd(k, n) = 1$.

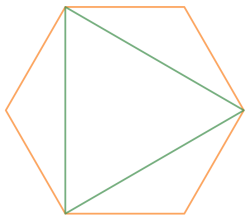
Proposition 1.25: Let G be a cyclic group and $a \in G$ such that $G \neq \langle a \rangle$. Then no element of $\langle a \rangle$ is a generator for G.

Proof: Suppose $|G| = n$. Since $\langle a \rangle \neq G$, $|a| < |G|$. Now every element of $\langle a \rangle$ is of the form a^k for some $k \in \mathbb{Z}$, and $\left|a^k\right| = \frac{|a|}{\gcd(k,|a|)} \leq |a| < |G|$, so no element of $\langle a \rangle$ is a generator for G.

Definition 1.26: Two groups G and H are **isomorphic** if there is a bijection $\varphi : G \longrightarrow H$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. φ is called an **isomorphism**, and we write $G \simeq H$.

Example: $\mathbb{Z}_4 \simeq \langle i \rangle \leq \mathbb{C}^*$, since the map $\varphi : \mathbb{Z}_4 \longrightarrow \measuredangle i\rangle$ given by $\varphi(a) = i^a$ is an isomorphism.

Example: Let $H = \{x \in D_6 \mid x \text{ preserves an inscribed triangle}\} \leq D_6$. Then $H \simeq D_3$.



Proposition 1.27: Isomorphisms preserve identities, inverses, subgroups, and order (both of elements and groups).

II — The Symmetric Group

Definition 2.1: A ***k*-cycle** is an element of S_n of the form $(a_1 \cdots a_k)$.

Definition 2.2: A **transposition** is a 2-cycle.

Proposition 2.3: Every element of S_n can be expressed as a product of disjoint cycles.

Example: To remove duplicate numbers, start with 1 and pass it through the permutation, then pass the result through, and so on. Since every permutation is a bijection by definition, every number will be sent to a unique other. Once the permutation results in 1 again, close the cycle and continue with the next lowest unused number. For instance, if $\sigma = (124)(314)$, $\sigma(1) = 1$, so we start again with 2: $\sigma(2) = 4$. Then $\sigma(4) = 3$, and $\sigma(3) = 2$, so the permutation is (243).

Proposition 2.4: Disjoint cycles commute.

Proposition 2.5: Every element of S_n can be expressed as a product of transpositions.

Proof: For an arbitrary $\sigma \in S_n$, express σ as a product of disjoint cycles. Then for an individual cycle $(a_1 \cdots a_k)$, $(a_1 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$.

Definition 2.6: Let $\pi \in S_n$. The **permutation matrix** for π is P_π, defined by $(P_\pi)_{ij} = 1$ if $\pi(j) = i$ and 0 if not.

Example: For $\pi = (243) \in S_4$,

$$P_\pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Proposition 2.7: All permutation matrices are orthogonal (that is, the columns form an orthonormal basis for $\mathbb{R}^n$, so $\det P_\pi = \pm 1$).

Definition 2.8: A permutation $\pi \in S_n$ is **even** if $\det P_\pi = 1$, and **odd** if $\det P_\pi = -1$.

Definition 2.9: The **alternating group** of degree n is $A_n = \{\pi \in S_n \mid \pi \text{ is even}\} \leq S_n$.

Proposition 2.10: For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Proof: Define $f : A_n \longrightarrow S_n \setminus A_n$ by $f(\pi) = (12)\pi$. Then $f^{-1}(\pi) = (12)\pi$, so f is invertible. Thus $|A_n| = |S_n \setminus A_n|$, so $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Theorem 2.11: Let $\pi \in S_n$. Then $\pi \in A_n$ if and only if π can be expressed as the product of evenly many transpositions. Moreover, when π is expressed in such a way, there are always the same number of transpositions (mod 2).

Proof: Suppose $\pi = \tau_1 \cdots \tau_k$, where each τ_i is a transposition. Then $P_\pi = P_{\tau_1} \cdots P_{\tau_k}$. Since P_{τ_i} has exactly 2 columns permuted from I_n, $\det P_{\tau_i} = -1$, so $\det P_\pi = (-1)^k$. Thus π is even if and only if k is even, proving both claims.

Theorem 2.12: Let $n \geq 3$. Then A_n is generated by 3-cycles.

Proof: Let $\pi \in A_n$. Then π is the product of evenly many transpositions. Group them in pairs, and consider an arbitrary pair, say $(ab)(cd)$.

If (ab) and (cd) have no common entries, then $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$ (which is valid, since $b \neq c$ by assumption).

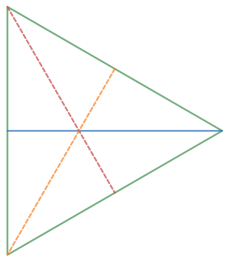
If (ab) and (cd) have one entry in common, then without loss of generality, $(cd) = (bd)$. Then $(ab)(cd) = (ab)(bd) = (abd)$.

Finally, if (ab) and (cd) share two entries, they are identical, so $(ab)(cd) = e$. Thus each pair is expressible as either one or two 3-cycles or the identity, and since we can omit the identities, π is the product of 3-cycles.

III — Cosets and Lagrange's Theorem

Definition 3.1: Let G be a group, $H \leq G$, and $a \in G$. The **left coset** of H in G with representative a is the set $aH = \{ah \mid h \in H\}$, and right cosets are defined similarly.

Example: Let $H = \langle r \rangle \leq D_3$. Then $eH = rH = r^2H = \{e, r, r^2\}$ and $sH = rsH = r^2sH = \{s, rs, r^2s\}$. If $K = \langle s \rangle$, then $eK = sK = \{e, s\}$, $rK = rsK = \{r, rs\}$, and $r^2sK = \{r^2, r^2s\}$.



Here, K fixes the solid blue line, rK moves it to the red dashed line, and r^2K to the yellow dashed line. The red and yellow lines are called **conjugate substructures** to the blue line. Conjugate substructures can be found by applying every element of a group — or just those that generate distinct cosets — to the original substructure.

Example: The cosets of $S^1 \leq \mathbb{C}^*$ are all the concentric circles around the origin.

Comment: In general, left cosets are more important than right ones, since function composition operates right-to-left.

Proposition 3.2: Let G be a group and $H \leq G$. Then the following are equivalent:

1. $aH = bH$.
2. $b \in aH$.
3. $b^{-}1a \in H$.

Definition 3.3: Let G be a group and $H \leq G$. The **index** of H in G is $[G : H] = |\{aH \mid a \in G\}|$.

Theorem 3.4: (Lagrange) Let G be a group and $H \leq G$. Then the set of left cosets $\{aH \mid a \in G\}$ partitions G into subsets of equal cardinality.

Proof: For all $b \in G$, $b \in bH$, so $G \subseteq \bigcup aH$. And clearly $\bigcup aH \subseteq G$, so $G = \bigcup aH$. Now we claim $aH \cap bH$ is either aH or $\varnothing$ for all $a, b \in G$. Suppose $aH \cap bH \neq \varnothing$. Then there is a $c \in aH \cap bH$, so by the previous result, $cH = aH$ and $cH = bH$, and therefore $aH = bH$. Thus G is the disjoint union of the cosets of H, so they are a partition.

To show that all cosets have the same cardinality, define a function $f : aH \longrightarrow H$ by $f(ah) = h$. Then f is a bijection, so $|aH| = |H|$.

Corollary 3.4.1: Let G be a group and $H \leq G$. Then $|G| = [G : H]|H|$.

Proof: Since $G = \bigsqcup aH$, $|G| = \sum |aH| = \sum |H| = \sum_{k=1}^{[G:H]} |H| = [G : H]|H|$.

Corollary 3.4.2: Let G be a finite group and let $H \leq G$. Then $|H| \mid |G|$.

Corollary 3.4.3: Let G be a finite group and let $a \in G$. Then $|a| \mid |G|$.

Corollary 3.4.4: Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.

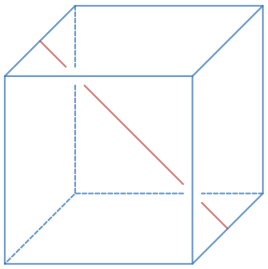
Corollary 3.4.5: Let $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: With $G = U(n)$, $|G| = |\{a \in \mathbb{N} \mid a < n, \gcd(a, n) = 1\}| = \varphi(n)$, so $a^{|G|} = a^{\varphi(n)} = 1$.

Corollary 3.4.6: Let $a \in \mathbb{N}$ and p prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: Find the order of the group of orientation-preserving symmetries of a regular cube.

Let G be this group and let $H \leq G$ be the subgroup fixing the red line.



There are six elements of G that fix the red line (pick one of the two vertices on the line to face up — then there are three symmetries that permute the three vertices adjacent to it, making six in total). And there are four conjugate substructures of the line, so there are four distinct cosets of H. Thus $[G : H] = 4$, and therefore $|G| = [G : H]|H| = 24$.

Theorem 3.5: There is only one cyclic group of each finite order, and only one of any infinite order, up to isomorphism.

Proof: Let G be cyclic with $|G| = n$. Then $G = \langle a \rangle$ for some $a \in G$, so the map $\varphi : G \longrightarrow \mathbb{Z}_n$ given by $a^k \longmapsto k \cdot 1$ is an isomorphism.

If G is infinite, then G must be countable, since it can be written as $\{e, a, a^2, ...\}$. Then there is an isomorphism given by $a^k \longmapsto k \cdot 1$. Not that it is *not* sufficient to claim that $G \simeq \mathbb{Z}$ since G is countable — that definition requires only a bijection, which need not be multiplicative.

Proposition 3.6: Let $\varphi : G \longrightarrow G'$ be an isomorphism. Then

1. $|G| = |G'|$.
2. $\varphi(e_G) = e_{G'}$.
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$.
4. $|\varphi(a)| = |a|$.

5. If $H \leq G$, then $\varphi(H) \leq \varphi(G) = G'$.

6. If G is Abelian, then so is G'.

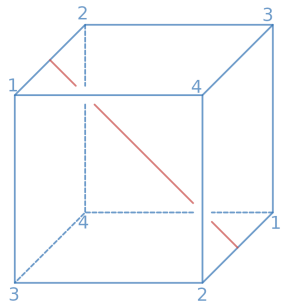
Theorem 3.7: (Cayley) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

Proof: Let $a \in G$ and define $\lambda_a : G \longrightarrow G$ by $\lambda_a(b) = ab$. Then if we number the elements of G from 1 to n, $\lambda_a \in S_n$. Let $G' = \{\lambda_a \in S_n \mid a \in G\}$. We claim $G \simeq G'$, where the isomorphism is given by $\lambda(a) = \lambda_a$.

Clearly, λ is onto, since $G' = \lambda(G)$ by definition. To show that λ is injective, suppose $\lambda(a) = \lambda(b)$. Then $\lambda_a = \lambda_b$, so in particular, $\lambda_a(e) = \lambda_b(e)$. Thus $a = b$. Finally, λ is multiplicative, since $\lambda(ab) = \lambda_{ab} = \lambda_a\lambda_b = \lambda(a)\lambda(b)$. Thus λ is an isomorphism, so $G \simeq G' \leq S_n$.

Example: Determine the rotation group of the cube.

Let the group be G. By our previous work, we know $|G| = 24$, and by Cayley's Theorem, we know $G \leq S_6$. But $|S_6| = 720$, and there are far too many order-24 subgroups of S_6 to determine the correct one (or even easily make a complete list). Instead, fix the four diagonals from the previous example and number the vertices 1—4 by which line they are contained in. Then each element of G must fix one of the four diagonals by the previous example, so $G \leq S_4$.



Now each rotation about one of the four diagonal axes fixes one number and permutes the other three, so it is a 3-cycle. Since we have all 8 possible 3-cycles from this method, G contains A_4. Draw a new line that connects the midpoints of the edges with endpoints 1 and 2 (shown in the above figure). A rotation about this axis fixes 3 and 4 and permutes 1 and 2, so $(12) \in G$. Thus $|G| \geq |A_4| + 1 = 13$, since $(12) \notin A_4$, and since $|G| \mid |S_4| = 24$, $|G| = 24$. Thus $G = S_4$.

Since we can form a regular octahedron by replacing each face of the cube with a vertex and each vertex with a face (that is, the cube and octahedron are *dual*), the rotation group of the octahedron is also S_4.

Definition 3.8: Let G be a group. An **automorphism** of G is an isomorphism from G to itself. Notice that every automorphism is completely determined by where it sends the generators of G, since $\varphi(a_1^{k_1} \cdots a_n^{k_n}) = \varphi(a_1)^{k_1} \cdots \varphi(a_n)^{k_n}$.

Definition 3.9: Let G be a group. The **automorphism group** of G is Aut G, the group of automorphisms of G.

Example: The automorphism group of $\mathbb{Z}$ is $\{e, \varphi\}$, where $e : 1 \longmapsto 1$ and $\varphi : 1 \longmapsto -1$. Thus Aut $\mathbb{Z} \simeq \mathbb{Z}_2$.

Example: For any group G, $\gamma_a : G \longrightarrow G$ defined by $\gamma_a(b) = aba^{-1}$ is an automorphism.

Definition 3.10: Let G be a group. The **inner automorphism group** of G is Inn $G = \{\gamma_a \mid a \in G\}$.

Definition 3.11: Let G and G' be groups. The **direct product** of G and G' is $G \times G' = \{(a, a') \mid a \in G, a' \in G'\}$, where the group operation is defined as $(a, a')(b, b') = (ab, a'b')$.

Proposition 3.12: Let G and G' be groups. Then $G \times G'$ is also a group, and $|G \times G'| = |G||G'|$.

Proposition 3.13: Let G and G' be groups and let $(a, a') \in G \times G'$. Then $|(a, a')| = \text{lcm}(|a|, |a'|)$.

Definition 3.14: An **internal direct product** is a group G such that there exist two subgroups $H, K \leq G$ satisfying $HK = \{hk \mid h \in H, k \in K\} = G$, $H \cap K$, and $hk = kh$ for all $h \in H$ and $k \in K$. In this case, $G \simeq H \times K$.

Example: $D_6 = \langle r^2, s\rangle\langle r^3\rangle$.

Proposition 3.15: $\simeq$ is an equivalence relation.

Proposition 3.16: $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Proposition 3.17: Let H and K be groups. Then $H \times K \simeq K \times H$.

Proposition 3.18: If $H \simeq H'$ and $K \simeq K'$, then $H \times K \simeq H' \times K'$.

Definition 3.19: Let G be a group. Two elements $b, c \in G$ are **conjugate** if $c = aba^{-1}$ for some $a \in G$.

Definition 3.20: Let G be a group. Two subgroups $H, K \leq G$ are **conjugate** if $K = aHa^{-1}$ for some $a \in G$.

Proposition 3.21: Conjugacy is an equivalence relation.

Proof: Let G be a group. For all $b \in G$, $b = ebe^{-1}$. If $c = aba^{-1}$ for some $a, b, c \in G$, then $b = \left(a^{-1}\right) c \left(a^{-1}\right)^{-1}$. Finally, if $c = aba^{-1}$ and $d = a'c(a')^{-1}$ for some $a, a', b, c, d \in G$, then $d = (a'a)b(a'a)^{-1}$.

Theorem 3.22: Let G be a group, $a, b \in G$, and $H \leq G$. Then $|b| = |aba^{-1}|$, $|H| = |aHa^{-1}|$, and $H \simeq aHa^{-1}$.

Example: For D_6, $r^{-1} = srs = srs^{-1}$, so r and $r^{-1} = r^5$ are conjugate. Similarly, r^2 and r^4 are conjugate. Since $r^3 \in Z(D_6)$, it is only conjugate to itself. s, r^2s, and r^4s are all conjugate to one another, as are rs, r^3s and r^5s.

Example: In S_5, (12345) and (13524) are conjugate by the amazing conjugation trick. Similarly, so are any two elements with the same cycle structure.

Comment: In a sense, conjugate elements and subgroups have the same "type".

Definition 3.23: A subgroup $H \leq G$ is **normal** is $H = aHa^{-1}$ for all $a \in G$, or, equivalently, $aH = Ha$ for all $a \in G$. We write $H \lhd G$.

Definition 3.24: A group is **simple** if it contains no nontrivial normal subgroups.

Example: All Abelian groups are normal, since $aHa^{-1} = aa^{-1}H = H$. In particular, $Z(G) \lhd G$ for all groups G.

Example: $\{e, (12)(34), (13)(24), (14)(23)\} \lhd S_4$.

Proposition 3.25: Let G be a groups and $N \triangleleft G$. Then the set product $(aN)(bN) = abN$.

Definition 3.26: Let G be a group and $N \triangleleft G$. The quotient group of G by N is $G/N = \{aN \mid a \in G\}$ under the composition law $(aN)(bN) = abN$, with identity N and inverse $(aN)^{-1} = a^{-1}N$. Note that $|G/N| = [G : N]$.

Example: $D_6/\langle r^2, s\rangle \simeq \mathbb{Z}_2$.

$S_n/A_n = \{A_n, (12)A_n\} \simeq \mathbb{Z}_2$.

For $K = \{e, (12)(34), (13)(24), (14)(23)\}$, $S_4/K \simeq D_3$.

$\mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}_5$.

IV — Morphisms

Definition 4.1: Let G and G' be groups. A **homomorphism** between G and G' is a function $\varphi : G \longrightarrow G'$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. Notice that every isomorphism is a homomorphism.

Proposition 4.2: Let G and G' be groups and $\varphi : G \longrightarrow G'$ be a homomorphism. Then:

1. $\varphi(e_G) = \varphi(e_{G'})$.
2. $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$.
3. $\varphi(G) \leq G'$.

Example: Examples of homomorphisms:

Vector space linear transformations: $T(v + w) = Tv + Tw$.

The determinant, $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$: $\det AB = (\det A)(\det B)$.

The complex modulus, $|\cdot| : \mathbb{C}^* \longrightarrow \mathbb{R}^+$: $|ab| = |a||b|$.

The exponential map, $\exp : \mathbb{R} \longrightarrow S^1$: $\exp(a + b) = e^{2\pi i(a+b)} = e^{2\pi ia}e^{2\pi ib} = \exp(a)\exp(b)$. (Remember that the group action in S^1 is complex multiplication!)

For a group G with $|G| = n$, the map from Cayley's theorem, $\lambda : G \longrightarrow S_n$: $\lambda(ab) = \lambda_{ab} = \lambda_a\lambda_b = \lambda(a)\lambda(b)$.

Theorem 4.3: Let G and G' be groups, $\varphi : G \longrightarrow G'$ be a homomorphism, and $H' \leq G'$. Then $\varphi^{-1}(H') = \{h \in G \mid \varphi(h) \in H'\} \leq G$. Moreover, if $H' \lhd G'$, then $\varphi^{-1}(H') \lhd G$.

Proof: Let $H = \varphi^{-1}(H')$. Since $e_G \in G$ and $\varphi(e_G) = e_{G'} \in H'$, $e_G \in H$ by definition.

Let $a, b \in H$. Then $\varphi(a), \varphi(b) \in H'$, so $\varphi(a)\varphi(b) = \varphi(ab) \in H'$. Thus $ab \in H$.

Finally, let $a \in H$. Then $\varphi(a) \in H$, so $\varphi(a)^{-1} = \varphi\left(a^{-1}\right) \in H'$. Thus $a^{-1} \in H$, and so $H \leq G$.

Now suppose $H' \lhd G'$ and let $a \in G$ be arbitrary. Then $a\left(\varphi^{-1}(H')\right)a^{-1} = \varphi^{-1}\left(\varphi(a)H'\varphi\left(a^{-1}\right)\right) = \varphi^{-1}H')$, since $H' \lhd G'$. Since $H = \varphi^{-1}(H')$, $aHa^{-1} = H$. Thus $H \lhd G$.

Definition 4.4: Let G and G' be groups and $\varphi : G \longrightarrow G'$ be a homomorphism. The **kernel** of φ is the set $\ker\varphi = \{a \in G \mid \varphi(a) = e_{G'}\}$.

Proposition 4.5: Let G and G' be groups and $\varphi : G \longrightarrow G'$ be a homomorphism. Then $\ker\varphi \lhd G$.

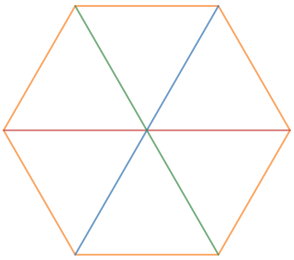
Proof: Since $\ker\varphi = \varphi^{-1}(\{e\})$ and $\{e\} \lhd G'$, $\ker\varphi \lhd G$.

Example: With $\varphi : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ defined by $\varphi(A) = \det A$, $\ker\varphi = SL_n(\mathbb{R})$, so $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.

Proposition 4.6: Let $\varphi : G \longrightarrow G'$ be a homomorphism and let $a \in G$. Then $|\varphi(a)| \,\big|\, |a|$ and $|\varphi(a)| \,\big|\, |G'|$.

Proposition 4.7: Let G be a group such that each element $a \in G$ permutes a set of conjugate substructures $\{y_1, ..., y_d\}$. Then there is a homomorphism $\varphi : G \longrightarrow S_d$.

Example:



Here, $\varphi : D_6 \longrightarrow S_3$.

Theorem 4.8: (The First Isomorphism Theorem) Let G and G' be groups and let $\varphi : G \longrightarrow G'$ be a homomorphism. Then $G/(\ker \varphi) \simeq \varphi(G)$.

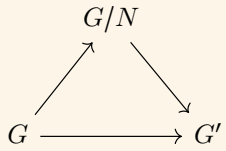
Proof: Let $N = \ker \varphi$ and define $\psi : G/N \longrightarrow G'$ by $\psi(aN) = \varphi(a)$. ψ is well-defined, since if $aN = bN$, then $b^{-1}a \in N = \ker \varphi$, so $\varphi(b)^{-1}\varphi(a) = e$, or equivalently, $\psi(aN) = \psi(bN)$. Moreover, since $\psi(aNbN) = \psi(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN)\psi(bN)$, ψ is a homomorphism.

Now suppose $\psi(aN) = \psi(bN)$. Then $\varphi(a) = \varphi(b)$, so $\varphi(b^{-1}a) = e$. Then $b^{-1}a \in \ker \varphi = N$, so $aN = bN$. Thus ψ is injective, and certainly it is surjective onto its range, so $\psi|_{\varphi(G)} : G/N \longrightarrow \varphi(G)$ is an isomorphism.

Definition 4.9: Let G be a group and $N \triangleleft G$. The **canonical projection** is $\gamma : G \longrightarrow G/N$, defined by $g \longmapsto gN$.

Definition 4.10: A **commutative diagram** is a collection of sets and maps between them such that for any two sets A and B in the diagram, all paths of compositions from A to B are equal as functions.

Theorem 4.11: Let G and G' be groups and $\varphi : G \longrightarrow G'$ be a homomorphism. Then the following diagram commutes, where γ is the canonical projection of G onto G/N and ψ is as before, defined by $\psi(aN) = \varphi(a)$.



Example: Let $\varphi : V \longrightarrow V'$ be a linear transformation between vector spaces and let $W = \ker \varphi$. Then $V/W \simeq \varphi(V)$.

With $\varphi = \det$, $GL_n/SL_n \longrightarrow \mathbb{R}^*$.

With $\varphi(a+bi) = \sqrt{a^2+b^2}$, $\mathbb{C}^*/S^1 \simeq \mathbb{R}^+$.

With $\varphi(a) = e^{2\pi i a}$, $\mathbb{R}/\mathbb{Z} \simeq S^1$.

Theorem 4.12: (The Second Isomorphism Theorem) Let G be a group, $H \leq G$, and $N \lhd G$. Then HN is a group, $H \cap N \lhd H$, and $H/(H \cap N) \simeq (HN)/N$, where the isomorphism is given by $\varphi(h(H \cap N)) = hN$.

Theorem 4.13: (The Third Isomorphism Theorem) Let G be a group and $H, N \lhd G$ such that $H \subseteq N$. Then $N/H \lhd G/H$ and $\frac{G/H}{N/H} \simeq G/N$.

Theorem 4.14: (The Correspondence Theorem) Let G and G' be groups and $\varphi : G \longrightarrow G'$ a surjective homomorphism. Then φ is a bijection between $\{H \leq G \mid \ker \leq H\}$ and $\{H' \leq G'\}$. Moreover, if $N' \lhd G'$, then $\varphi^{-1}(N') \lhd G$.

Proof: Since φ is surjective, for all $h' \in H'$, there is a $g \in G$ such that $\varphi(g) = h'$. Thus $\varphi(\varphi^{-1}(H')) = H'$. Now let $h \in H$. Since $\varphi^{-1}(\varphi(H)) = H$. Thus φ is a bijection,

Definition 4.15: Let G be a group and $a \in G$. The **conjugacy class** of a is $[a] = \{gag^{-1} \mid g \in G\}$.

Proposition 4.16: Let G be a group. Then $G = \bigsqcup_{a \in G} [a]$.

Proposition 4.17: Let G be a group, $a \in G$, and $G_a = \{g \in G \mid gag^{-1} = a\}$. Then $[G : G_a] = |[a]|$.

Theorem 4.18: (The Class Equation) Let G be a group. Then $|G| = \sum [G : G_a]$, where the sum is over the $a \in G$ that produce distinct conjugacy classes.

V — Group Actions

Definition 5.1: Let G be a group, X a set, and S_X the group of permutations of X. An **action** of G on X is a homomorphism $\varphi : G \longrightarrow S_X$. We say that X is a G-set, and write $a(x)$ instead of $(\varphi(a))(x)$ for $x \in X$. In this sense, every element of G is a function on X.

Definition 5.2: Let G be a group acting on a set X. The **stabilizer** of $x \in X$ is the set $G_x = \{a \in G \mid a(x) = x\} \leq G$.

Definition 5.3: Let G be a group acting on a set X, with the action given by φ. The **kernel** of the action is $\ker \varphi$.

Definition 5.4: Let G be a group acting on a set X. The **orbit** of $x \in X$ is $\operatorname{orb} x = \{a(x) \mid a \in G\}$.

Definition 5.5: Let G be a group acting on a set X. The **fixed point set** corresponding to the action is $X^G = \{x \in X \mid a(x) = x \text{ for all } a \in G\}$.

Example: D_6 acts on the regular hexagon, $\mathbb{C}^*$ acts on the plane, and $SO(3)$ acts on $\mathbb{R}^3$.

Example: If G is the group of symmetries of a structured set X and Y is a substructure of X, then G acts on the set of conjugate substructures of Y.

Example: A group G acts on itself by left multiplication, giving the isomorphism from G to a subgroup of $S_{|G|}$.

Example: A group G acts on the set of left cosets of a subgroup $H \leq G$ by left multiplication, which gives the homomorphism from G to $S_{|G/H|}$.

Example: A group G acts on itself by conjugation, giving the homomorphism from G to Aut G with a range of Inn G. This is called the *adjoint action*. For $a \in G$, G_a is called the *centralizer* of a and is denoted $C(a)$. The kernel of the action is the center of the group, $Z(G)$. The orbit of $a \in G$ is a's conjugacy class, $[a]$.

Theorem 5.6: There is a one-to-one correspondence between the sets orb x and G/G_x, and between the $a(x)$ and aG_x. In particular, the number of distinct orbits of x is $[G : G_x]$, and therefore, $[G : G_x] = |[x]|$.

Proposition 5.7: Let G be a group acting on a set X, $a \in G$, and $x \in X$. Then $G_{a(x)} = aG_xa^{-1}$.

Definition 5.8: Let G be a group acting on a set X. G acts **transitively** on X if for all $x, y \in X$, there is an $a \in G$ such that $a(x) = y$.

Theorem 5.9: Let G be a group acting transitively on a set X. Let $x_0 \in X$ and $G_0 = G_{x_0}$, and for all $x \in X$, let $a_x \in G$ be such that $a_x(x_0) = x$. Then the action of G on X is equivalent to the action of G on G/G_0, in that there is a bijection from X to G/G_0 given by $x \longmapsto a_xG_0$, and $a(x) = y$ if and only if $a(a_xG_0) = a_y(G_0)$ for all $a \in G$.

Proof: The bijection exists immediately by the one-to-one correspondence between orb $x_0 = X$ (since the action is transitive) and G/G_0. For the second statement, $a(x) = y$ if and only if $aa_xG_0(x_0) = a((a_xG_0)(x_0)) = y$, since a_xG_0 is the set of elements that send x_0 to x. But this happens if and only if $a(a_xG_0) = a_yG_0$, since a_yG_0 is the set of elements that send x_0 to y.

Comment: By this theorem, we can treat any transitive action as an action on the left cosets of some subgroup. Therefore, all actions on geometric objects can be transformed into pure algebra by fixing a base point and considering the left cosets of its stabilizer subgroup.

Definition 5.10: Let G be a group acting on a set X. G acts **freely** on X if for all $x \in X$, $G_x = \{e\}$.

Definition 5.11: Let G be a group acting on a set X. X is a **principal homogeneous set** for G if G acts freely and transitively on X.

Example: The punctured line $\mathbb{E} \setminus \{0\}$ is a principal homogeneous set for $\mathbb{R}^*$.

The punctured plane $\mathbb{E}^2 \setminus \{0\}$ is a principal homogeneous set for $\mathbb{C}^*$.

The punctured 3-space $\mathbb{E}^3 \setminus \{0\}$ is *not* a principal homogeneous set for the group of symmetries of $\mathbb{E}^3$ that preserve the orientation, scale, and the origin, since it is impossible to rotate the 2-sphere without fixing a point, and therefore the symmetry group cannot act freely.

The punctured 4-space $\mathbb{E}^4 \setminus \{0\}$ is a principal homogeneous set for $\mathbb{H}^*$.

Theorem 5.12: (The Class Equation) Let G be a group. Then

$$|G| = |Z(G)| + \sum_{[a],\ a \notin Z(G)} [G : G_a].$$

Proof: $[G : G_a] = 1$ if and only if $[a] = \{a\}$, if and only $a \in Z(G)$.

Example: Does S_4 have a normal subgroup of order 8? The class equation for S_4 is $24 = 1+6+8+6+4$, counting the center, 2-cycles, 3-cycles, 4-cycles, and (2, 2)-cycles, respectively. A normal subgroup is the union of conjugacy classes. But every subgroup contains the identity, and there is no way to union conjugacy classes to result in a subgroup of order 8 that includes e.

Definition 5.13: A ***p*-group** is a group G with order $|G| = p^n$ for some prime p and some $n \in \mathbb{N}$.

Proposition 5.14: Every nontrivial p-group has a nontrivial center.

Proof: Let G be a nontrivial p-group. Then $|G| = p^n = |Z(G)| + \sum_{[a],\ a \notin Z(G)} [G : G_a]$. Since $|G_a| \mid p^n$ for all $a \in G$, $p \mid |G_a|$ if $|G_a| \neq 1$, so $p \mid |G_a|$ if $a \notin Z(G)$. Thus $p \mid \sum_{[a],\ a \notin Z(G)} [G : G_a]$, and since $p | p^n$ $(n \neq 0)$, $p \mid |Z(G)|$. Since $p > 1$, $|Z(G)| \neq 1$.

Definition 5.15: Let G be a group. The **commutator subgroup** of G is $G' = \langle [a, b] \mid a, b \in G \rangle$, where $[a, b] = aba^{-1}b^{-1}$.

Proposition 5.16: Let G be a group and G' the commutator subgroup. Then $G' \lhd G$, G/G' is abelian, and if $N \lhd G$ and G/N is abelian, then $G' \leq N$.

Definition 5.17: Let G be a group. The ***i*th derived subgroup** of G if $G^{(i)} = \left(G^{(i-1)}\right)'$, where $G^{(1)} = G'$.

Definition 5.18: A group G is **solvable** if $G^{(n)} = \{e\}$ for some $n \in \mathbb{N}$.

Example: Every abelian group G is solvable, since $G' = \{e\}$.

Comment: In some sense, solvable groups are built up from abelian groups, but they are far more common than abelian groups while still sharing many nice properties.

Definition 5.19: A group G is **perfect** if $G' = G$.

Theorem 5.20: All p-groups are solvable.

Proof: Suppose not. Then there is a group G that is the smallest-order nonsolvable p-group. Since $G' \leq G$, $|G'| \leq |G|$, so $G' = G$, since otherwise G' would be a smaller-order nonsolvable p-group. Now let $\overline{G} = G/ZG$, which is a group, since $Z(G) \lhd G$. Since G is a nontrivial p-group, $Z(G) \neq \{e\}$, so $|\overline{G}| < |G|$. Since $G = G'$, every element of G is of the form $([a_1, b_1]) \cdots ([a_i, b_i]])$, and since $|G| > |\overline{G}|$, there is an onto homomorphism from G to $\overline{G}$ given by $[a, b] \longmapsto [a, b]Z(G)$, so every element of $\overline{G}$ is of the form $[a, b]Z(G)$. Thus $\overline{G} = \overline{G}'$, so $\overline{G}^{(n)} = \overline{G}$ for all $n \in \mathbb{N}$. Since G is a p-group, $|G| = p^k$ for some $k \in \mathbb{N}$, and since $Z(G) \leq G$, $|Z(G)| = p^l$ for some $l \in \mathbb{N}$. Thus $|\overline{G}| = |G/Z(G)| = p^{k-l}$, and so $\overline{G}$ is a p-group. But G is the smallest-order nonsolvable p-group, so $\overline{G}$ must be solvable. But $\overline{G}^{(n)} = \overline{G}$ for all $n \in N$, so $\overline{G} = \{e\}$. But $\overline{G} = G/Z(G)$, so $G = Z(G)$, and so G is abelian, and therefore solvable. ↯

Theorem 5.21: All odd-ordered groups are solvable.

Theorem 5.22: Let G be a finite group and let p be a prime such that $p \mid |G|$. Then G contains an element of order p.

VI — Rings

Definition 6.1: A **ring** is a nonempty set R with two binary operations $+$ and $\cdot$, such that $(R, +)$ is an abelian group, R is closed under $\cdot$, $\cdot$ is associative, and for all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Example: $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $M_n R$ for any ring R, and the set of functions on a given set are all rings.

Definition 6.2: Let R be a ring. The **polynomial ring** $R[x]$ is the set of all polynomials in x with coefficients in R.

Definition 6.3: A **ring with 1** is a ring with a multiplicative identity.

Definition 6.4: Let R be a ring with 1. A **unit** of R is an element of R with a multiplicative inverse.

Definition 6.5: Let R be a ring with 1. The **group of units** of R is $R^\times = \{a \in R \mid a \text{ is a unit}\}$.

Definition 6.6: A **commutative ring** is a ring with commutative multiplication.

Proposition 6.7: Let R be a ring. Then $0a = a0 = 0$ for all $a \in R$.

Proof: $0a = (0+0)a = 0a + 0a$, so $0a = 0$.

Proposition 6.8: Let R be a ring. Then $(-a)b = -(ab)$ for all $a, b \in R$.

Proof: $ab + (-a)b = (a + (-a))b = 0b = 0$, so $(-a)b = -(ab)$.

Proposition 6.9: Let R be a ring. Then $(-a)(-b) = ab$ for all $a, b \in R$.

Proof: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

Proposition 6.10: Let R be a ring with 1. Then $(-1)a = -a$ for all $a \in R$.

Proof: $a + (-1)a = (1 + (-1))a = 0a = 0$, so $(-1)a = -a$.

Corollary 6.10.1: Let R be a ring with 1. Then $(-1)(-1) = 1$.

VII — Domains

Definition 7.1: A **division ring** is a ring R with 1 such that $R^\times = R \setminus \{0\}$.

Definition 7.2: A **field** is a commutative division ring.

Definition 7.3: An **integral domain** is a commutative ring with 1 such that if $ab = 0$, then either $a = 0$ or $b = 0$.

Definition 7.4: Let R be a ring. A **zero divisor** in R is a nonzero element $a \in R$ such that for some nonzero $b \in R$, either $ab = 0$ or $ba = 0$.

Proposition 7.5: Let R be a ring. Then $S \subseteq R$ is a subring if and only if $S \neq \varnothing$, $(S, +) \leq (R, +)$, and S is closed under multiplication.

Proposition 7.6: Let R be a commutative ring and let $a \in R$ be a nonzero non-zero divisor. Then if $ab = ac$, $b = c$.

Proof: Since $ab = ac$, $ab - ac = a(b - c) = 0$. Since $a \neq 0$ is not a zero divisor, $b - c = 0$. Thus $b = c$.

Corollary 7.6.1: Let R be an integral domain. Then if $ab = ac$ for $a, b, c \in R$ with $a \neq 0$, $b = c$.

Theorem 7.7: (Wedderburn) All finite integral domains are fields.

Proof: Let D be a finite integral domain. Then $D = \{a_1, ..., a_n\}$ with the a_i distinct. Let $a_i \in D$. If $a_i a_j = a_i a_k$ for some $a_j, a_k \in D$, then $a_j = a_k$, which is impossible, since the elements of D are distinct. Thus $|\{a_i a_1, ..., a_i a_n\}| = |D|$, and since this cardinality is finite, $\{a_i a_1, ..., a_i a_n\} = D$. Now $1 \in D$ since it is an integral domain, so $a_i a_j = 1$ for some $a_j \in D$. Thus a_i^{-1} exists for all $a_i \in D$, so D is a field.

Theorem 7.8: (Artin-Zorn) All finite division rings are fields.

Definition 7.9: Let R be a ring with 1. The **characteristic** of R is $\operatorname{char} R = |1|$ in $(R, +)$. If $|1|$ is infinite, $\operatorname{char} R = 0$.

Example: char $\mathbb{Z}$ = char $\mathbb{Q}$ = 0, and char $\mathbb{Z}_n = n$.

Definition 7.10: Let R and S be rings. A **ring homomorphism** between R and S is a function $\varphi : R \longrightarrow S$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Definition 7.11: Let R be a ring and $a \in R$. The **evaluation homomorphism** at a is $\varepsilon_a : \mathbb{Z}[x] \longrightarrow R$, defined by $\varepsilon_a(p(x)) = p(a)$.

Definition 7.12: Let φ be a ring homomorphism. The **kernel** of φ is $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$.

Proposition 7.13: Let R and S be rings and $\varphi : R \longrightarrow S$ a ring homomorphism. Then $\ker\varphi \leq (R, +)$.

Definition 7.14: Let R be a ring. An **ideal** of R is a subset $I \subseteq R$ such that $I \leq (R, +)$ and $ar, ra \in I$ for all $a \in I$ and $r \in R$.

Definition 7.15: Let R be a ring and $a \in R$. The **ideal generated by a** is $(a) = aR$.

Definition 7.16: Let R be a ring. A **principal ideal** of R is an ideal $I \subseteq R$ such that $I = (a)$ for some $a \in R$.

Definition 7.17: A **principal ideal domain**, or **PID**, is an integral domain in which all ideals are principal.

Theorem 7.18: Let R be a ring and $I \subseteq R$ an ideal. Then the quotient $R/I = \{a + I \mid a \in R\}$ is a ring.

Proof: Let $a + I, b + I \in R/I$. Then $(a + I)(b + I) = ab + aI + bI + I = ab + I \in R/I$, so R/I is closed under multiplication. Clearly, multiplication in R/I is associative and distributes over addition, so all that remains to be shown is that it is well-defined. Suppose $a + I = a' + I$ and $b + I = b' + I$. Let $x = a - a' \in I$ and $y = b - b' \in I$. Then $a'b' + I = ab - ay - xb + xy = ab + I$.

Theorem 7.19: Let R and S be rings and $\varphi : R \longrightarrow S$ a homomorphism. Then $R/\ker\varphi \simeq \varphi(R)$.

Proof: Define $\psi : R/\ker\varphi \longrightarrow \varphi(R)$ by $\psi(a + \ker\varphi) = \varphi(a)$. By the first isomorphism theorem for groups, ψ is a group isomorphism, and since $\psi((a + \ker\varphi)(b + \ker\varphi)) = \psi(ab + \ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a + \ker\varphi)\psi(b + \ker\varphi)$ for $a, b \in R$, ψ is a ring isomorphism too.

Proposition 7.20: Let R be a ring with 1. Then $\mathbb{Z}/\langle \text{char } R\rangle \simeq \langle 1_R\rangle$.

Proof: Define $\varphi : \mathbb{Z} \longrightarrow R$ by $\varphi(k) = k(1_R)$. Then $\varphi(\mathbb{Z}) = \langle 1_R\rangle$ and $\ker\varphi = \langle \text{char } R\rangle$, so $\mathbb{Z}/\langle \text{char } R\rangle \simeq \langle 1_R\rangle$.

Theorem 7.21: Let $\varphi : R \longrightarrow S$ be a surjective homomorphism. Then there is a one-to-one correspondence between the ideals of R containing $\ker\varphi$ and the ideals of S, given by $I \longmapsto \varphi(I)$ and $J \longmapsto \varphi^{-1}(J)$.

Comment: Moreover, if R is a ring and $I \subseteq R$ is an ideal, then there is a one-to-one correspondence between the ideals of R that contain I and the ideals of R/I, given by $J \longmapsto J + I$.

Definition 7.22: Let R be a ring. A **maximal ideal** of R is an ideal $I \subseteq R$ such that there is no ideal $J \subseteq R$ with $I \subset J \subset R$.

Definition 7.23: Let R be a ring. A **prime ideal** of R is an ideal $I \subset R$ such that for all $ab \in I$, either $a \in I$ or $b \in I$.

Definition 7.24: Let R be a ring. An element $p \in R$ is **prime** if $p \neq 0$ and (p) is a prime ideal.

Definition 7.25: Let R be a ring. An element $r \in R$ is **irreducible** if r is not a unit and whenever $r = ab$, either $a \in R^\times$ or $b \in R^\times$.

Theorem 7.26: Let R be a commutative ring with 1 and let $I \subseteq R$ be an ideal. Then I is maximal if and only if R/I is a field.

Proof: ($\Rightarrow$) Assume I is maximal. Then by the Correspondence theorem, R/I has no proper nontrivial ideals — that is, its only ideals are (0) and R/I. It follows quickly that R/I is a division ring, and we know already that is a commutative ring with 1, so it is a field.

($\Leftarrow$) Suppose I is not maximal. Then there is an ideal J of R with $I \subset J \subset R$. But then $J + I$ is an ideal of R/I, so R/I is not a field.

Comment: This theorem lays the groundwork for constructing fields from arbitrary rings — in particular, we will use it to construct fields from $\mathbb{Q}[x]$.

Theorem 7.27: Every ring contains a maximal ideal.

Theorem 7.28: Let R be a commutative ring with 1 and let $I \subseteq R$ be an ideal. Then I is a prime ideal if and only if R/I is an integral domain.

Proof:

$$\begin{aligned} I \text{ is a prime ideal} &\Leftrightarrow ab \in I \Rightarrow a \in I \text{ or } b \in I \\ &\Leftrightarrow ab + I = I \Rightarrow a + I = I \text{ or } b + I = I \\ &\Leftrightarrow (a + I)(b + I) = I \Rightarrow a + I = I \text{ or } b + I = I \\ &\Leftrightarrow (a + I)(b + I) = (0) + I \Rightarrow a + I = (0) + I \text{ or } b + I = (0) + I \\ &\Leftrightarrow I \text{ is an integral domain.} \end{aligned}$$

Definition 7.29: Let R be a commutative ring with 1. The **spectrum** of R, denoted Spec R, is the set of prime ideals of R.

Theorem 7.30: $\mathbb{Q}$ is the smallest field containing $\mathbb{Z}$.

Proof: Let $\frac{a}{b} \in \mathbb{Q}$. Then for any field k containing $\mathbb{Z}$, $\frac{a}{b} = a\left(\frac{1}{b}\right) = a\left(b^{-1}\right) \in k$, since k is closed under multiplicative inverses. Thus $\mathbb{Q} \subseteq k$.

Comment: We would like to construct the smallest ring containing a given integral domain and certain multiplicative inverses from it.

Definition 7.31: Let A be an integral domain. A subset $S \subseteq A$ is **multiplicative** if S is closed under multiplication.

Definition 7.32: Let A be an integral domain and let $S \subseteq A$ be multiplicative with $1 \in S$. The **localization** of A at S is $A\left[S^{-1}\right] = \left\{\frac{a}{s} \mid a \in A, s \in S\right\}$, where $\frac{a_1}{s_1} = \frac{a_2}{s_2}$ if $a_1 s_2 = a_2 s_1$.

Proposition 7.33: Let A be an integral domain and let $S \subseteq A$ be multiplicative with $1 \in S$. Then $A\left[S^{-1}\right]$ is a ring when addition is defined as $\frac{a}{s} + \frac{b}{t} = \frac{as+bt}{st}$ and multiplication as $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$. In this case, $\frac{0}{1} = 0$, $\frac{1}{1} = 1$, and $-\left(\frac{a}{s}\right) = \frac{-a}{s}$. Moreover, if $0 \in S$, then $A\left[S^{-1}\right] = \{0\}$, and if $0 \notin S$, then $A\left[S^{-1}\right]$ is an integral domain containing A.

Proof: To show that + is well-defined, suppose $\frac{a}{s} = \frac{b}{t}$. Then $at = bs$. Now let $c \in A$ and $u \in S$. Since $at = bs$, $atu^2 + cstu = bsu^2 + cstu$, so $(au + cs)(tu) = (bu + ct)(su)$. Thus $\frac{a}{s} + \frac{c}{u} = \frac{au+cs}{su}$ and $\frac{b}{t} + \frac{c}{u} = \frac{bu+ct}{tu}$, and so + is well-defined. The other ring axioms follow quickly.

Suppose $0 \in S$. Then for all $\frac{a}{s} \in A\left[S^{-1}\right]$, $\frac{a}{s} = \frac{0}{0}$ by definition, and $\frac{0}{0} = \frac{0}{1} = 0$, so $A\left[S^{-1}\right] = \{0\}$.

Now suppose $0 \notin S$. We already know that $A\left[S^{-1}\right]$ is a commutative ring with 1, so we need only show it has no zero divisors. Let $\frac{a}{s}, \frac{b}{t} \in A[S^{-1}]$ with $\frac{ab}{st} = 0 = \frac{0}{1}$. Since $0 \notin S$ and S is multiplicative, $st \neq 0$. Thus $ab = 0$, and since A is an integral domain, either $a = 0$ or $b = 0$. Thus $A\left[S^{-1}\right]$ is an integral domain, and $A \simeq \left\{\frac{a}{1} \mid a \in A\right\} \subseteq A\left[S^{-1}\right]$.

Definition 7.34: Let A be an integral domain, $\mathfrak{p}$ a prime ideal, and $S = A \setminus \mathfrak{p}$. The **local ring** $A_{\mathfrak{p}} = A\left[S^{-1}\right]$.

Definition 7.35: Let A be an integral domain and $S = A \setminus \{0\}$. The **field of fractions** of A is $\operatorname{Frac} A = A\left[S^{-1}\right]$.

Definition 7.36: Let k be a field. The **field of rational functions** in k is $k(x) = \operatorname{Frac} k[x]$.

Proposition 7.37: Let A be an integral domain. Then $\operatorname{Frac} A$ is the smallest field containing A.

Definition 7.38: A **Euclidean domain** is an integral domain D equipped with a function $\nu : D \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ such that

1. $\nu(a) \leq \nu(ab)$ for all $a, b \in D$.
2. $\nu(0) = \infty$.
3. If $a, b \in D$ with $a \neq 0$, then there are $q, r \in D$ with $b = aq + r$ and either $r = 0$ or $\nu(r) < \nu(a)$.

Theorem 7.39: Every Euclidean domain is a principal ideal domain.

Proof: Let D be a Euclidean domain and let $I \subseteq D$ be an ideal with $I \neq (0)$. Since ν maps into the nonnegative integers, there is $a \in I$ such that $\nu(a) \leq \nu(b)$ for all $b \in I$. Finally, let $i \in I$. Since D is a Euclidean domain, there are $q, r \in D$ such that $i = aq + r$ and either $r = 0$ or $\nu(r) < \nu(a)$. Since $a \in I$ and I is an ideal, $aq \in I$, so $r = i - aq \in I$ too. Thus $\nu(r) \geq \nu(a)$, since $\nu(a)$ was minimal in $\nu(I)$, and therefore r must be 0. Thus $i = aq \in (a)$, so $I \subseteq (a)$, and clearly $(a) \subseteq I$, so $I = (a)$ and is therefore a principal ideal.

Definition 7.40: Let A be an integral domain and let $a, b \in A$. a **divides** b, written $a|b$, if there is a $k \in A$ such that $b = ak$.

Definition 7.41: Let A be an integral domain and let $a, b \in A$. A **greatest common divisor** of a and b is an element $d \in A$ such that $d|a$, $d|b$, and if $c|a$ and $c|b$, then $c|d$. Notice that d may not be unique.

Theorem 7.42: (The Euclidean Algorithm) Let A be a principal ideal domain. Then $\gcd(a, b)$ exists for all $a, b \in A$, and there are $s, t \in A$ such that $\gcd(a, b) = as + bt$.

Proof: Since A is a principal ideal domain, $(a) + (b) = (d)$ for some $d \in A$. Since $a \in (a) + (b) = (d)$, $d|a$, and similarly, $d|b$. Now suppose $c|a$ and $c|b$ for some $c \in A$. Then $a = ck$ and $b = cl$ for some $k, l \in A$, and since $d \in (d) = (a) + (b)$, $d = as + bt = (ck)s + (cl)t$ for some $s, t \in A$. Thus $c|d$, and so $d = \gcd(a, b) = as + bt$.

Comment: Not every principal ideal domain is a Euclidean domain, though examples can be somewhat exotic. One such domain is $\mathbb{Z}\left[\sqrt{-19}\right]$.

Theorem 7.43: In a principal ideal domain, irreducible elements are prime.

Proof: Let D be a principal ideal domain and let $a \in D$ be irreducible. We will show that (a) is maximal, and therefore prime.

Suppose there were an ideal $I \subseteq D$ with $(a) \subseteq I$ and $I \neq D$. Since $I = (d)$ for some $d \in D$, $a \in (d)$, so $a = dk$ for some $k \in D$. Since d is not a unit and a is irreducible, k must be a unit. But then $d = ak^{-1} \in (a)$, so $(a) = (d)$. ↯ Thus (a) is maximal.

Example: Let $z = e^{\frac{2\pi i}{5}}$. Then $\varepsilon_z : \mathbb{Q}[x] \longrightarrow \mathbb{C}$ given by $f(x) \longmapsto f(z)$ has a nontrivial kernal, since $x^5 - 1 \in \ker \varepsilon_z$. It can be shown that $\ker \varepsilon_z = (p)$ is a prime ideal. Then p is irreducible, so (p) is maximal, and therefore $\mathbb{Q}[z] \simeq \mathbb{Q}[x]/(p)$ is a field.

Theorem 7.44: Let $z \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Then there is a unique monic, irreducible polynomial $p(x) \in \mathbb{Q}[x]$ such that $p(z) = 0$ and $\mathbb{Q}[z]$ is a field.

Theorem 7.45: Let D be a principal ideal domain and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals. Then $I_n = I_{n+1} = I_{n+2} = \cdots$ for some $n \in \mathbb{N}$.

Proof: Let $I = I_1 \cup I_2 \cup I_3 \cup \cdots$. Then I is an ideal, so $I = (d)$ for some $d \in D$. Clearly, $d \in I_n$ for some n, so since each I_k is an ideal, $I_n = I_{n+1} = \cdots = I$.

Theorem 7.46: In a principal ideal domain, every proper ideal is contained in a maximal ideal.

Proof: Let D be a principal ideal domain and $I_1 \subset D$ a proper ideal. If I_1 is not contained in any maximal ideal, then there is an infinite ascending chain $I_1 \subset I_2 \subset I_3 \subset \cdots$. ↯

Definition 7.47: Let R be a ring and $a, b \in R$. If $a = bu$ for some unit $u \in R$, we write $a \; b$.

Definition 7.48: A **unique factorization domain** is an integral domain D in which every nonzero nonunit element of D is expressible as a finite product of irreducible elements in D, and this factorization is unique up to multiplication by units.

Theorem 7.49: All principal ideal domains are unique factorization domains.

Lemma 7.49.1: Let D be a principal ideal domain and let $a \in D$ be a nonzero nonunit. Then $a = pq$ for some $p, q \in D$ with p irreducible.

Proof: Since D is a principal ideal domain, $(a) \subseteq (p)$ for some maximal ideal (p). Then p is prime, so it is irreducible, and since $a \in (p)$, $a = pq$ for some $q \in D$.

Proof: Let D be a principal ideal domain and let $a_1 \in D$ be a nonzero nonunit. By the lemma, let $d_i \in D$ be irreducible such that $a_1 = d_1 a_2 = (d_1 d_2) a_3 \cdots = (d_1 \cdots d_i) a_{i+1}$ for all $i \in \mathbb{N}$. Then each $a_{i+1} | a_i$, so $(a_i) \subseteq (a_{i+1})$ for all $i \in \mathbb{N}$. Since D is a principal ideal domain, this chain terminates, so $(a_n) = (a_{n+1})$ for some $n \in \mathbb{N}$. Then a_{n+1} must be a unit, since otherwise the lemma would guarantee another ideal, and so $a_1 = d_1 \cdots d_n$ for irreducible elements $d_1, ..., d_n \in D$. Now we need only show this factorization is unique.

Suppose $a = d_1 \cdots d_n = c_1 \cdots c_m$ for irreducible elements $d_1, ..., d_n, c_1, ..., c_m \in D$. Without loss of generality, suppose $m \leq n$. We will proceed by strong induction.

If $m = 1$, then $c_1 = d_1 \cdots d_n$. Since c_1 is prime, $c_1 | d_k$ for some $k \in \{1, ...n\}$. Since $d_k | c_1$ and c_1 is irreducible, n must be 1. Therefore, $a = d_1 = c_1$. $\lightning$

Now suppose that the theorem holds for all products of less than m irreducibles. Then if $c_1 \cdots c_m = d_1 \cdots d_n$, $c_m | d_1 \cdots d_n$, so $c_m \ d_k$ for some $k \in \{1, ...n\}$, since c_m is irreducible. Thus $d_k = u c_m$ for some unit $u \in D$, so $c_1 \cdots c_m = d_1 \cdots d_{k-1} d_{k+1} \cdots d_n u c_m$, since D is commutative, and since D is an integral domain, we can cancel the c_m, leaving $c_1 \cdots c_{m-1} = d_1 \cdots d_{k-1} d_{k+1} \cdots d_n u$. Since $c_1 \cdots c_{m-1}$ is a unique factorization, there is a one-to-one correspondence between the c_i and the d_j — without loss of generality, $c_i \ d_i$ for all $i \in \{1, ..., n-1\}$. Notice that this correspondence also implies that $n = m$. Now $a = d_1 \cdots d_n = c_1 \cdots c_n = d_1 \cdots d_{n-1} c_n u'$ for some unit $u' \in D$. By cancellation, $c_n \ d_n$, so the original factorization is unique up to units.

VIII — Polynomials

Definition 8.1: Let D be a unique factorization domain and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$. The **content** of f is $c(f) = gcd(a_0, a_1, ..., a_n)$. A polynomial is **primitive** if $c(f)$ is a unit.

Definition 8.2: Let $f = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$ and let $p \in \mathbb{N}$ be prime. The **reduction mod p** of f is $[f]_p = [a_0]_p + [a_1]_p x + \cdots + [a_n]_p x^n$.

Proposition 8.3: If $f \in \mathbb{Z}[x]$ is primitive and $\deg f = \deg [f]_p$, then $[f]_p$ is irreducible.

Proposition 8.4: Let R and S be commutative rings with 1 and let $\varphi : R \longrightarrow S$ be a homomorphism. Then there is a homomorphism $\phi : R[x] \longrightarrow S[x]$ given by $\phi(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1) x + \cdots + \varphi(a_n) x^n$.

Proposition 8.5: Let D be a unique factorization domain and let $d \in D$. Let $\phi : D[x] \longrightarrow \left(\frac{D}{(d)}\right)[x]$ be the homomorphism given by the previous proposition. If $f = a_0 + a_1 x + \cdots + a_n x^n$ is primitive, $d \nmid a_n$, and $\phi(f)$ is irreducible, then f is irreducible.

Proof: Suppose not. Then $f = gh$ for some $g, h \in D[x]$. Since f is primitive, g and h must be nonconstant, and since $d \nmid a_n$, $\deg f = \deg \phi(f)$, so $\deg g + \deg h = \deg \phi(g) + \deg \phi(h)$. Since $\deg g \geq \deg \phi(g)$ and $\deg h \geq \deg \phi(h)$, $\deg g = \deg \phi(g)$ and $\deg h = \deg \phi(h)$. Thus $\phi(f) = \phi(g)\phi(h)$, and so $\phi(f)$ is reducible. $\lightning$

Theorem 8.6: (Eisenstein's Criterion) Let D be a unique factorization domain, $p \in D$ prime, and $f = a_0 + a_1 x + \cdots + a_n x^n \in D[x]$ primitive. If $p | a_i$ for all $i \in \{0, ..., n-1\}$, $p \nmid a_n$, and $p^2 \nmid a_0$, then f is irreducible.

Proof: Suppose not. then $f = gh$ for $g, h \in D[x]$, and since f is primitive, g and h are nonconstant. Let $\phi : D[x] \longrightarrow \left(\frac{D}{(p)}\right)[x]$ be reduction mod p. Then $\phi(f) = [a_n]_p x^n = \phi(g)\phi(h)$, so the constant terms of g and h must both be divisible by p. But then $p^2 | a_0$. $\lightning$

Theorem 8.7: Let $p \in \mathbb{N}$ be prime. Then $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible in $\mathbb{Z}[x]$.

Proof: Let $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$. Then

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{1}{x}\left(x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x\right) \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}. \end{aligned}$$

Now $p \left| \binom{p}{k} \right.$ for all $k \in \{1, ..., p-1\}$, $p \nmid 1$, and $p^2 \nmid \binom{p}{p-1} = p$, so by Eisenstein's criterion, $f(x+1)$ is irreducible. But with $u = x - 1$, $f(u+1) = f(x)$ is irreducible.

Proposition 8.8: (Gauss's Lemma I) Let D be a principal ideal domain and let $f, g \in D[x]$. Then $c(fg) = c(f)c(g)$.

Proof: Let $p \in D$ be prime and let ϕ be reduction mod p. Since (p) is maximal, $D/(p)$ is a field, so it is also an integral domain. Thus $\phi(f)\phi(g) = 0$ if and only if $\phi(f) = 0$ or $\phi(g)$, so $p | fg$ if and only if $p | f$ or $p | g$, and so $c(fg) = c(f)c(g)$.

Theorem 8.9: (Gauss's Lemma II) Let D be a principal ideal domain and $k = \text{Frac } D$. If $f \in D[x]$ is nonconstant and irreducible, then it is also irreducible in $k[x]$.

Proof: Suppose not. Then $f = g_k h_k$ for some nonconstant $g_k, h_k \in k[x]$. By clearing the denominators and factoring out the content, there are primitive, nonconstant polynomials $g, h \in D[x]$, where $g = \frac{b}{b'} g_k$ and $h = \frac{c}{c'} h_k$. Then $\frac{bc}{b'c'} f = gh$, so $(bc)f = (b'c')gh$. Since g and h are both primitive, so is gh by Gauss's lemma I. Since f is irreducible in $D[x]$, it is primitive, so bc $b'c'$. Thus $f = ugh$ for some unit $u \in D$, so f is reducible in $D[x]$. $\lightning$

Proposition 8.10: If D is a unique factorization domain, then so is $D[x]$.

Definition 8.11: Let $n \in \mathbb{N}$. The ***n*th roots of unity** are the n complex solutions to $x^n - 1$, written ζ_n^i, where $\zeta_n = e^{frac2\pi in}$.

Definition 8.12: Let $n \in \mathbb{N}$. The **primitive *n*th roots of unity** are the nth roots of unity ζ_n^i with i relatively prime to n.

Definition 8.13: The ***n*th cyclotomic polynomial** is the unique monic irreducible polynomial that generates $\ker \varepsilon_{\zeta_n}$, written $\Phi_n(x)$.