Abstract Algebra Notes

Cruz Godar

Math 481, 482, and 560, taught by Eric Brussel

I — Groups

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

a) $ab \in G$ for all $a, b \in G$.

b) $(ab)c = a(bc)$ for all $a, b, c \in G$.

c) There is an $e \in G$ with $ae = ea = a$ for all $a \in G$.

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

Definition: Let $n \in \mathbb{N}$. The **unit group of the integers modulo n** is $U(n) = \{a \in C_n \mid \gcd(a, n) = 1\}$, with the operation given by multiplication mod n.

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

Proposition: 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: 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: 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: 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: $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 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 $S^1 \leq C^*$.

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

a) $H \neq \varnothing$.

b) $ab \in H$ for all $a, b \in H$.

c) 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 $H \leq G$.

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

Definition: 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.

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

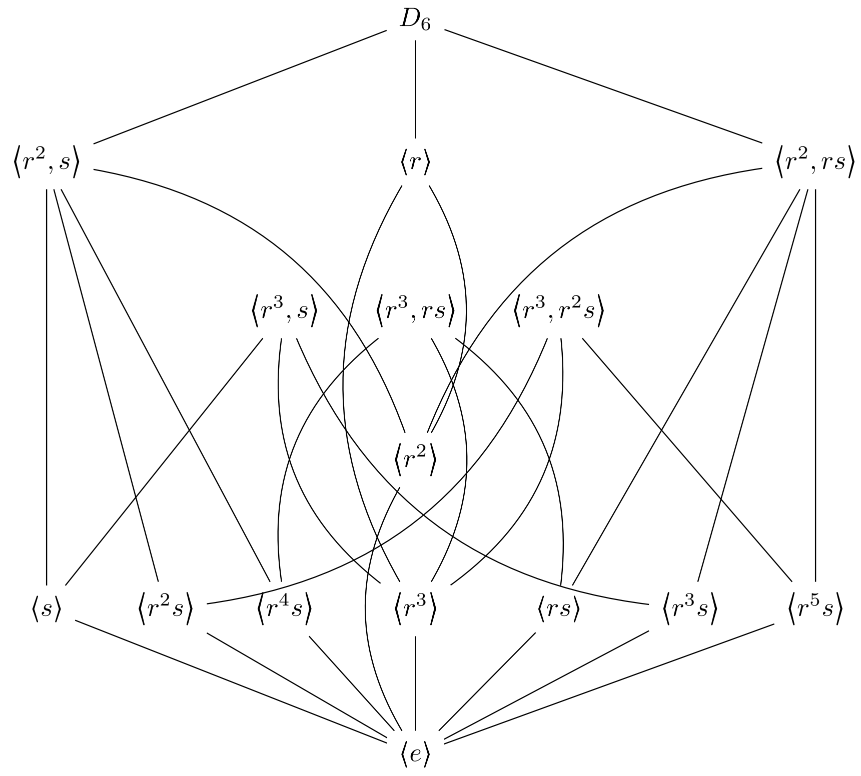
$$|1| = 1, \qquad |2| = 6, \qquad |4| = 3, \qquad |5| = 6, \qquad |7| = 3, \qquad |8| = 2.$$

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

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 $|a| = |a^{-1}|$.

Definition: 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:

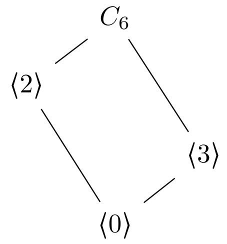


Theorem: A subgroup of a cyclic group is cyclic.

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 C_6 are $\langle 0\rangle$, $\langle 3\rangle$, $\langle 2\rangle$, and $\langle 1\rangle = C_6$.



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

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

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

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

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

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

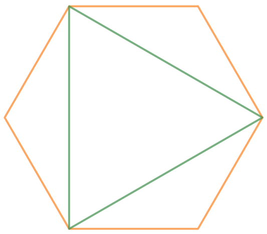
Proposition: Let G be a cyclic group and $a \in G$ such that $G \neq \langle a \rangle$. Then no element of $\langle a \rangle$ is a generator for G.

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 $\left|a^k\right| = \dfrac{|a|}{\gcd(k,|a|)} \leq |a| < |G|$, so no element of $\langle a \rangle$ is a generator for G.

Definition: 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: $C_4 \simeq \langle i \rangle \leq \mathbb{C}^*$, since the map $\varphi : C_4 \longrightarrow \langle i \rangle$ 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: Isomorphisms preserve identities, inverses, subgroups, and order (both of elements and groups).

Definition: The **symmetric group** of degree n is the group S_n of permutations on n elements, defined as $\{\sigma : \{1, ..., n\} \lhook\joinrel\twoheadrightarrow \{1, ..., n\}\}$, 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: 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: 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.

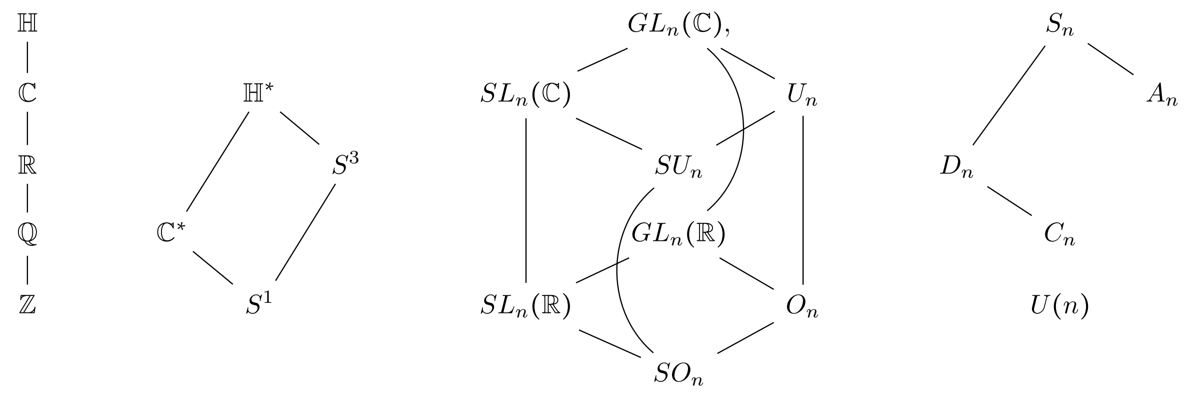
Definition: The **orthogonal group** of degree n is $O_n = \{A \in M_n(\mathbb{R}) \mid AA^{\mathrm{T}} = I\}$, and the **special orthogonal group** of degree n is $SO_n = \{A \in O_n \mid \det A = 1\}$. The **unitary group**, U_n, and **special unitary group**, SU_n, are defined identically, except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

Definition: 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 $S^3 = \{z \in \mathbb{H}^* \mid |z| = 1\} \leq \mathbb{H}^*$.

Example: Many of the elementary groups:



II — The Symmetric Group

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

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

Proposition: 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: Disjoint cycles commute.

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

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

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

Proposition: 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: 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: 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).

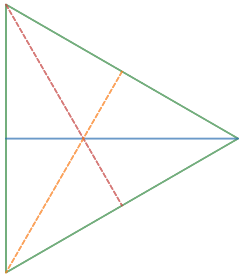
If (ab) and (cd) have one entry in common, then without loss of generality, $(cd) = (bd)$. Then $(ab)(cd) = (ab)(bd) = (abd)$.

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

a) $aH = bH$.

b) $b \in aH$.

c) $b^-1a \in H$.

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

Theorem: (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: Let G be a finite 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: Let G be a finite group and let $H \leq G$. Then $|H| \bigm| |G|$.

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

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

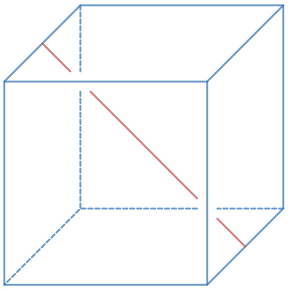
Corollary: Let $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

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

a) $|G| = |G'|$.

b) $\varphi(e_G) = e_{G'}$.

c) $\varphi(a^{-1}) = \varphi(a)^{-1}$.

d) $|\varphi(a)| = |a|$.

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

f) If G is Abelian, then so is G'.

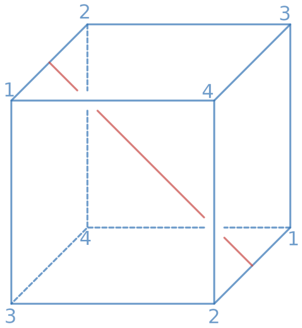
Theorem: (Cayley) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

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 $|G| \bigm| |S_4| = 24$, $|G| = 24$. 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: 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: 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 $\mathbb{Z} \simeq C_2$.

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

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

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

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

Definition: An **internal direct product** is a group G such that there exist two subgroups $H, K \leq G$ satisfying $HK = \{hk \mid h \in H, k \in K\} = G$, $H \cap K = \{e\}$, 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: $\simeq$ is an equivalence relation.

Proposition: $C_m \times C_n \simeq C_{mn}$ if and only if $\gcd(m, n) = 1$.

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

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

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

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

Proposition: 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: 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, $r^2 s$, and $r^4 s$ are all conjugate to one another, as are rs, $r^3 s$ and $r^5 s$.

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

Definition: Let G be a group and $N \lhd G$. 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: $D_6/\langle r^2, s\rangle \simeq C_2$.

$S_n/A_n = \{A_n, (12)A_n\} \simeq C_2$.

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

$\mathbb{Z}/5\mathbb{Z} \simeq C_5$.

IV — Morphisms

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

a) $\varphi(e_G) = \varphi(e_{G'})$.

b) $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$.

c) $\varphi(G) \leq G'$.

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, $\exp : \mathbb{R} \longrightarrow S^1$: $\exp(a + b) = e^{2\pi i(a+b)} = e^{2\pi i a}e^{2\pi i b} = \exp(a)\exp(b)$. (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: 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: 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: Let G and G' be groups and $\varphi : G \longrightarrow G'$ be a homomorphism. Then $\ker\varphi \triangleleft G$.

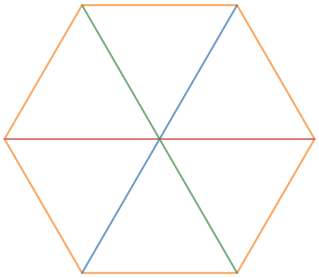
Proof: Since $\ker\varphi = \varphi^{-1}(\{e\})$ and $\{e\} \triangleleft G'$, $\ker\varphi \triangleleft G$.

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

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

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

Definition: 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: 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 $\psi(aN) = \varphi(a)$.

$$\begin{tikzcd}
& G/N \arrow[dr] & \\
G \arrow[ur] \arrow[rr] & & G'
\end{tikzcd}$$

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: (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: (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 $\dfrac{G/H}{N/H} \simeq G/N$.

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

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

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

Theorem: (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: 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: 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: 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: 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: 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 $\operatorname{Aut} G$ with a range of $\operatorname{Inn} G$. 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: There is a one-to-one correspondence between the sets $\operatorname{orb} x$ 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: 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: 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: 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: 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: 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: (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: A ***p*-group** is a group G with order $|G| = p^n$ for some prime p and some $n \in \mathbb{N}$.

Proposition: 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 $|G_a| \bigm| p^n$ for all $a \in G$, $p \bigm| |G_a|$ if $|G_a| \neq 1$, so $p \bigm| |G_a|$ if $a \notin Z(G)$. Thus $p| \sum_{[a],\ a\notin Z(G)} [G : G_a]$, and since $p|p^n$ $(n \neq 0)$, $p \bigm| |Z(G)|$. Since $p > 1$, $|Z(G)| \neq 1$.

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

Theorem: A group G is solvable if and only if the series of derived subgroups form a normal chain $\{e\} = G^{(t)} \triangleleft G^{(t-1)} \triangleleft \cdots \triangleleft G^{(2)} \triangleleft G^{(1)} \triangleleft G$, such that the quotient groups $G/G^{(1)}, G^{(1)}/G^{(2)}, ..., G^{(t-1)}/G^{(t)}$ are all abelian.

Proof: If G is solvable, then $G^{(t)} = \{e\}$ for some $t \in \mathbb{N}$. Thus all we need show is that the derived subgroups are normal and the quotients are abelian. $G' = \left\langle aba^{-1}b^{-1} \mid a, b \in G\right\rangle$. Now for any $g \in G'$ and $c \in G$, $cgc^{-1}g^{-1} \in G'$ by definition, and so $\left(cgc^{-1}g^{-1}\right)(g) = cgc^{-1} \in G'$. Thus $cG'c^{-1} = G'$, so $G' \triangleleft G$. Since $G^{(i)} = \left(G^{(i-1)}\right)'$, all of the derived subgroups from a normal chain. Now for any $cG', dG' \in G/G'$, $(cG')(dG')\left(c^{-1}G'\right)\left(d^{-1}G'\right) = \left(cdc^{-1}d^{-1}\right)G' = G'$, so $(cG')(dG') = (dG')(cG')$. Thus every quotient is normal.

The converse is clearly true, since $G^{(t)} = \{e\}$ for some $t \in \mathbb{N}$.

Theorem: Let G be a finite group and $N \triangleleft G$. Then G is solvable if and only if N and G/N are solvable.

Proof: ($\Rightarrow$) Suppose G is solvable and let $N \triangleleft G$. Then $N' \leq G'$, and similarly $N^{(i)} \leq G^{(i)}$ for all i. Since G is solvable, $G^{(t)} = \{e\}$ for some $t \in \mathbb{N}$, so $N^{(t)} = \{e\}$. Thus N is solvable, and an identical argument holds for G/N.

($\Leftarrow$) Suppose N and G/N are solvable. Choose a set $\{a_1, ..., a_k\}$ of coset representatives in G/N. Then $G = a_1N \sqcup \cdots \sqcup a_kN$, so every element in G can be expressed uniquely as a_in for some $n \in N$. Let $a_{i_1}n_1, a_{i_2}n_2 \in G$. Then we have

$$(a_{i_1}n_1)(a_{i_2}n_2)(a_{i_1}n_1)^{-1}(a_{i_2}n_2)^{-1} = a_{i_1}n_1a_{i_2}n_2n_1^{-1}a_{i_1}^{-1}n_2^{-1}a_{i_2}^{-1}.$$

Now N is normal, so $n_1a_{i_2} = a_{i_2}n_1'$ for some $n_1' \in N$. In this way, we can move all of the elements from G/N to the left of the product, giving us

$$(a_{i_1}n_1)(a_{i_2}n_2)(a_{i_1}n_1)^{-1}(a_{i_2}n_2)^{-1} = a_{i_1}a_{i_2}a_{i_1}^{-1}a_{i_2}^{-1}n,$$

where $n \in N$ is the product of the four shifted elements of N that end up on the right side of the expression. Since $a_{i_1}a_{i_2}a_{i_1}^{-1}a_{i_2}^{-1} \in (G/N)'$, $G' \leq (G/N)'(N)$. Continuing in this manner, $G^{(i)} \leq (G/N)^{(i)}(N)$ for all $iin\mathbb{N}$. Since G/N is solvable, $(G/N)^{(t)} = \{e\}$ for some $t \in \mathbb{N}$, so $G^{(t)} \leq (\{e\})(N) = N$. But N is solvable, so $N^{(s)} = \{e\}$ for some $s \in \mathbb{N}$. Thus $G^{(t+s)} \leq N^{(s)} = \{e\}$, so G is solvable.

Theorem: 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 $Z(G) \triangleleft G$. 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: All odd-ordered groups are solvable.

Theorem: (Cauchy's Theorem) Let G be a finite group such that $p \bigm| |G|$ for some prime p. Then G contains an element of order p.

VI — Rings

Definition: 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: $\mathbb{Z}$, C_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: Let R be a ring. The **polynomial ring** $R[x]$ is the set of all polynomials in x with coefficients in R.

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

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

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

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

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

Proposition: 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 $(-1)a = -a$.

VII — Domains

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

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

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

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

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

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

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

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

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

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

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

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

Definition: 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: 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: Every ring contains a maximal ideal.

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

Theorem: $\mathbb{Q}$ 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: Let A be an integral domain. A subset $S \subseteq A$ is **multiplicative** if S is closed under multiplication.

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

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

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

a) $\nu(a) \leq \nu(ab)$ for all $a, b \in D$.

b) $\nu(0) = \infty$.

c) 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: 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: 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: 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: (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: 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 $(a) = (d)$. $\lightning$ 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: 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: 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: 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 $I_1 \subset I_2 \subset I_3 \subset \cdots$. $\lightning$

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

Definition: 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.

Lemma: 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 $q \in D$.

Theorem: All principal ideal domains are unique factorization domains.

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 $d_1, \ldots, d_n \in D$. Now we need only show this factorization is unique.

Suppose $a = d_1 \cdots d_n = c_1 \cdots c_m$ for irreducible elements $d_1, \ldots, d_n, c_1, \ldots, c_m \in D$. 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 $k \in \{1, \ldots n\}$. 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 $k \in \{1, \ldots n\}$, 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 $i \in \{1, \ldots, n-1\}$. 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: Let D be a unique factorization domain and let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$. 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: Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ 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: If $f \in \mathbb{Z}[x]$ is primitive and $\deg f = \deg[f]_p$, then $[f]_p$ is irreducible.

Proposition: 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 $\phi\,(a_0 + a_1x + \cdots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$.

Proposition: 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 $f = a_0 + a_1x + \cdots + a_nx^n$ 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: (Eisenstein's Criterion) Let D be a unique factorization domain, $p \in D$ prime, and $f = a_0 + a_1x + \cdots + a_nx^n \in D[x]$ 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: 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 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \dfrac{x^p - 1}{x - 1}$. 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: (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: (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 $bc \sim b'c'$. Thus $f = ugh$ for some unit $u \in D$, so f is reducible in $D[x]$. $\lightning$

Corollary: Let $p \in D[x]$ be primitive and suppose $q|p$ for some primitive, nonconstant $q \in D[x]$. Then $\frac{p}{q} \in D[x]$.

Proof: Since $q|p$, $p = qr'$ for some $r' \in k[x]$. But this means that p is reducible in $k[x]$, so it must also be reducible in $D[x]$, and by the proof, $p = u(qr)$ for some unit $u \in D$ and $r \in D[x]$, where $ur = r'$.

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

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

IX — Field Extensions

Definition: Let k be a field. A **field extension** of k is a field F, written F/k, such that $k \subseteq F$.

Definition: Let F/k be a field extension. The **degree** of F/k is $[F : k] = \dim_F k$, where $\dim_F$ is the vector space dimension over F.

Definition: A field extension is **finite** if it has finite degree.

Theorem: (Kronecker's Theorem) Let k be a field and $f \in k[x]$ be a nonconstant irreducible polynomial with $\deg f = n$. Then $E = \frac{k[x]}{(f)}$ is a field extension of k of degree n with a basis $\{1, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}\}$, where $\overline{x} = x + (f)$. Moreover, $\overline{x}$ is a root of f.

Proof: Since f is irreducible and $k[x]$ is a principal ideal domain, (f) is maximal, so E is a field. Define $\varphi : k \longrightarrow \frac{k[x]}{(f)}$ by $\varphi(a) = a + (f)$. Then $\ker \varphi$ is an ideal of the field k, so it is either (0) or k. But since f is nonconstant, the kernel cannot be k, so it is (0). Thus φ is injective, so $k \subseteq E$, and therefore E is a field extension of k.

Let $g \in E$. Then $g = r$ for some $r \in E$ with $\deg r < \deg f = n$, so $r \in \operatorname{span}\{1, x, x^2, ..., x^{n-1}\}$. Since $\overline{x} = x + (f)$, $g \in \operatorname{span}\{1, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}\}$. If $c_0 + c_1\overline{x} + \cdots + c_{n-1}\overline{x}^{n-1} = 0$, then each $c_i = 0$, so $\{1, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}\}$ is linearly independent, and therefore a basis for E over k. Finally, $f(\overline{x}) = f(x) + (f) = 0$ by definition.

Example: Let $F = \mathbb{Q}[\zeta_5]$. Then $[F : \mathbb{Q}] = \deg \Phi_5 = \deg x^4 + x^3 + x^2 + x + 1 = 4$.

Example: To find $\left[\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right]$, we first find a generator of $\mathbb{Q}\left(\sqrt[3]{2}\right)$ — a monic irreducible polynomial such that quotienting $\mathbb{Q}[x]$ by it gives $\mathbb{Q}\left(\sqrt[3]{2}\right)$. This is $x^3 - 2$, so $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$. Similarly, $\left[\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right] = 2$, since the generator is $x^2 + x + 1$. By properties of vector spaces, $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ cannot be contained in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, since $2 \nmid 3$. Thus the generator of $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ over $\mathbb{Q}\left(\sqrt[3]{2}\right)$ is still $x^2 + x + 1$. Therefore, $\left[\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right] = 6$, with a basis of

$$\left\{1, \sqrt[3]{2}, \sqrt[3]{4}, e^{\frac{2\pi i}{3}}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{4}\right\}.$$

Theorem: (Multiplicativity of Degree) Let k be a field and E/k a finite field extension with degree n. Let F/E be another finite extension with degree m. Then F/k has degree mn.

Proof: Let $\{e_1, ..., e_n\}$ be a basis for E over k and $\{f_1, ..., f_m\}$ a basis for F over E. It is simple (if tedious) to show that $\{e_1f_1, ..., e_1f_m, ..., e_nf_1, ..., e_nf_m\}$ is a basis for F over k and that therefore $[F : k] = mn$.

Proposition: Let $n \in \mathbb{N}$. If $m < n$ and $m|n$, then $\gcd(x^m - 1, \Phi_n(x)) = 1$.

Proof: If not, then $\mathbb{Q}(\zeta_m)$ would be a subfield of $\mathbb{Q}(\zeta_n)$ by multiplicativity of degree, so Φ_n would be reducible over $\mathbb{Q}$. $\lightning$

Corollary: Every root of Φ_n is a primitive nth root of unity.

Comment: Given a field extension k, we have created a field extension K for every polynomial $p \in k[x]$ such that the extension contains a root of p. Moreover, $K = k(\overline{x})$ is the smallest such extension — if F/k has a root z of p, then there is an injective homomorphism from $k(\overline{x})$ to F given by $f(\overline{x}) \longmapsto f(z)$.

Definition: Let k be a field. An element z is **transcendental** over k if $\ker \varepsilon_z = \{0\}$, and **algebraic** if not.

Proposition: If z is transcendental over a field k, then $k[z] \simeq k[x]$.

Proof: $\ker \varepsilon_z = \{0\}$, so $k[x] \simeq \frac{k[x]}{\ker \varepsilon_z} \simeq k[z]$.

Definition: Let k be a field and z an element possibly not in k. The **minimum polynomial** for z over k is the unique monic irreducible polynomial $m_{z/k}$ with $m_{z/k}(z) = 0$. Notice that if $f(z) = 0$ for some polynomial $f \in k[x]$, then $m_{z/k}|f$.

Definition: Let k be a field and z an element possibly not in k. The **degree** of z over k is $\deg(z/k) = [k(z) : k]$.

Definition: Let k be a field. Two elements z, z' are **conjugate** over k if $m_{z/k} = m_{z'/k}$.

Definition: A ring F is **algebraic** over a field k if $k \subseteq F$ and every $z \in F$ is algebraic over k.

Definition: A field k is **algebraically closed** if every element algebraic over k is contained in k.

Theorem: Finite extensions are algebraic.

Proof: Let E/k be a field extension and let $z \in E$. Since E/k is finite, $[E : k] = n$ for some $n \in \mathbb{N}$. Then $1, z, z^2, ..., z^n$ cannot all be linearly independent, so there is a polynomial $p \in k[x]$ with $\deg p \leq n$ such that $p(z) = 0$. Thus z is algebraic over k.

Theorem: If z is algebraic over a field k, then $k[z] = k(z)$.

Proof: Since z is algebraic over k, there is a polynomial in $k[x]$ with z as a zero. Let $m_{z/k}$ be the polynomial with lowest degree with z as a zero. Then $m_{z/k}$ is necessarily irreducible, so $(m_{z/k})$ is a maximal ideal, since $k[x]$ is a principal ideal domain (because polynomial long division makes it a Euclidean domain). Thus $k[z] = k[x]/(m_{z/k})$ is a field, so it is closed under inverses. Thus $k[z] = k(z)$.

Theorem: Let E/k be a field extension. Then E/k is finite if and only if it is algebraic and finitely generated — that is, $E = k[z_1, ..., z_n]$ for some $z_1, ..., z_n$.

Proof: ($\Rightarrow$) Assume $[E : k]$ is finite. Then if $y \in E$, $k(y)$ is a subfield of E, so by multiplicativity of degree, $[k(y) : k] | [E : k]$. Thus $[k(y) : k]$ is finite, so it is algebraic.

Since $[E : k]$ is finite, there is a finite basis $\{e_1, ..., e_n\}$ for E over k by definition. Then $E = k[e_1, ..., e_n]$.

($\Leftarrow$) Now suppose E/k is algebraic and finitely generated. Then $E = k[z_1, ..., z_n]$ for some $z_1, ..., z_n \in E$, and so $k \subseteq k[z_1] \subseteq k[z_1, z_2] \subseteq \cdots \subseteq k[z_1, ..., z_n] = E$. Since z_1 is algebraic over k, $k[z_1] = k(z_1)$ and $[k(z_1) : k]$ is finite. Similarly, $[k(z_1, z_2) : k(z_1)] = [k(z_1)(z_2) : k(z_1)]$ is finite, so by multiplicativity of degree, so is $[k(z_1, z_2) : k]$. By induction, $[E : k]$ is finite.

Theorem: Let E/k be a field extension. Then the set of elements of E algebraic over k is a field.

Proof: Let $F = \{z \in E \mid z/k \text{ is algebraic}\}$ and let $a, b \in F$. Then $\ker \varepsilon_x \neq \{0\}$, so there is a minimal polynomial $m_{a/k}$ with $\frac{k[x]}{(m_{a/k})} \simeq k[a]$. By Kronecker's theorem, $[k[a] : k] = [k(a) : k]$ is finite. Since b is algebraic over k it is also algebraic over $k(a)$. Thus $k(a, b)/k(a)$ is finite, so by multiplicativity of degree, $k(x, y)/k$ is too. Thus $k(x, y)$ is algebraic over k, so by definition, all of its elements are algebraic, and therefore in F. Thus $x + y, x - y, xy, \frac{x}{y} \in F$, so F is a field.

Definition: Let E/k and F/k be field extensions. A ***k*-embedding** of E into F is a ring homomorphism $\varphi : E \longrightarrow F$ such that $\varphi|_k = id_k$, the identity map on k.

$$\begin{tikzcd}
E \arrow[rr, "\varphi"] \arrow[dr, dash] & & F \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

A ***k*-automorphism** is a k-embedding of E into itself.

Definition: Let E/k be a field extension. The **Galois group** of E/k, written $\text{Gal}(E/k)$, is the set of k-automorphisms of E.

Definition: Let K/E be a field extension of E/k. An **extension** of a k-embedding $\varphi : E \longrightarrow F$ is a ring homomorphism $\phi : K \longrightarrow F$ such that $\phi|_E = id_E$.

$$\begin{tikzcd}
K \arrow[rr, "\phi"] \arrow[d, dash] & & F \arrow[d, equal] \\
E \arrow[rr, "\varphi"] \arrow[dr, dash] & & F \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Example: To compute the Galois group of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, let σ be an element in the group. Then $\sigma\left(\sqrt[3]{2}\right)^3 = \sigma(2) = 2$, since $2 \in \mathbb{Q}$, and $\sigma\left(\sqrt[3]{4}\right) = 4$, so ς fixes $\mathbb{Q}$, $\sqrt[3]{2}$, and $\sqrt[3]{4}$. Thus $\sigma = id$, so $\text{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right) = \{e\}$.

Comment: If E/k is a finite extension and $\varphi : E \longrightarrow F$ is a k-embedding, $\ker\varphi = \{0\}$, since otherwise φ would no longer be a homomorphism. Thus $E \simeq \varphi(E)$, and in particular, $[E : k] = [\varphi(E) : k]$.

Comment: k-embeddings preserve minimal polynomials: let E/k be a finite extension and $\varphi : E \longrightarrow F$ a k-embedding. Then if $z \in E$ is algebraic over k and $p(z) = 0$ for some $p \in k[x]$, $\varphi(p(z)) = 0$, and since $\varphi_k = id$, $p(\varphi(z)) = 0$. Thus $\varphi(z)$ is a root of $m_{z/k}$, and by the properties of homomorphisms, $\varphi(z)$ must have a minimal polynomial of the same degree as z. Thus $m_{z/k} = m_{\varphi(z)/k}$.

Theorem: (The Extension Lemma) Let $\varphi : k \longrightarrow k'$ be an isomorphism, let E/k' be an extension, and let $p \in k[x]$ be irreducible with $\varphi(p) \in k'[x]$. If $\varphi(p)$ has n distinct roots $z_1, ..., z_n$, and $k(\overline{x}) = k[x]/(p)$, then there are n extensions of φ that map $k(\overline{x})$ to E, denoted $\phi_1, ..., \phi_n$, such that $\phi_i(\overline{x}) = z_i$.

$$\begin{tikzcd}
k(\overline{x}) \arrow[r, "\phi_i"] \arrow[d, dash] & E \arrow[d, dash] \\
k \arrow[r, "\varphi"] & k'
\end{tikzcd}$$

Proof: Define $\phi_i' : k[x] \longrightarrow E$ by $\phi_i' = \varepsilon_{z_i}(\varphi)$. Since $\varepsilon_{z_i}(\varphi(p)) = 0$ by hypothesis, $\ker \phi_i' = (p)$ (since p must be the minimal polynomial for z_i). Now define $\phi_i : k[x]/(p) \longrightarrow E$ by the first isomorphism theorem. All the ϕ_i must be distinct, since $\phi_i(\overline{x}) = z_i$ and the z_i are distinct. Moreover, there are no other extensions, since if $\phi : k(\overline{x}) \longrightarrow E$ is one, then $\phi(\overline{x})$ is a root of $\varphi(p)$, since p is the minimum polynomial for $\overline{x}$. Thus $\phi = \phi_i$ for some i.

Corollary: Let E/k be a field extension containing exactly n roots of the irreducible polynomial $p \in k[x]$. If the roots are $z_1, ..., z_n$, then there are exactly n k-embeddings $\psi_i : k(z_1) \longrightarrow E$, and they are given by $\psi_i = \phi_i \circ \phi_1^{-1}$ — that is, $\psi_i(g(z_1)) = g(z_i)$.

Example:

$$\begin{tikzcd}
\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) \arrow[r, shift left, "\phi_i"] \arrow[r, shift right] \arrow[d, dash, "2"] & \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) \arrow[d, equal] \\
\mathbb{Q}\left(\sqrt[3]{2}\right) \arrow[r, shift left=2, "\varphi_i"] \arrow[r] \arrow[r, shift right=2] \arrow[d, dash, "3"] & \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"] & \mathbb{Q}
\end{tikzcd}$$

The second level comes from the extension lemma, and so we can see that

$$\left[\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right] = 6.$$

X — Splitting Fields

Definition: A polynomial **splits** over a field if it factors into linear factors over that field.

Definition: Let k be a field and $p \in k[x]$. The **splitting field** for p is the field extension of k of smallest degree in which p splits.

Definition: Let k be a field and $p \in k[x]$. The **Galois group** of p is the Galois group of its splitting field.

Example: Compute the splitting field for $f(x) = x^5 - 1 \in \mathbb{Q}[x]$: First we factor f into $(x-1)(x^4+x^3+x^2+x+1)$, and since the first factor is already linear, we can ignore it. Now we have

$$\begin{tikzcd}
\mathbb{Q}(\zeta_5) \arrow[r, "\varphi_i"] \arrow[d, dash] & \mathbb{Q}(\zeta_5) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"] & \mathbb{Q}
\end{tikzcd}$$

since $\mathbb{Q}\left(\zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\right) = \mathbb{Q}\left(\zeta_5\right)$. Since the roots z_i are exactly ζ_5^i for $i \in \{1,2,3,4\}$, we can define φ_i by $\varphi_i(\zeta_5) = \zeta_5^i$. By the extension lemma, this is a complete list of automorphisms of $\mathbb{Q}\left(\zeta_5\right)$ that fix $\mathbb{Q}$, and since there are four roots, we know that $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_5\right)/\mathbb{Q}\right) \leq S_4$. Since $|\varphi_2| = 4$, $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_5\right)/\mathbb{Q}\right) = \mathrm{Gal}\left(x^5 - 1\right) = \mathbb{Z}/4$.

Example: Compute $\mathrm{Gal}\left(x^4 - 2/\mathbb{Q}\right)$: the splitting field is $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$, and $\left[\mathbb{Q}\left(\sqrt[4]{2}, i\right) : \mathbb{Q}\right] = 8$:

$$\begin{tikzcd}
\mathbb{Q}\left(\sqrt[4]{2}, i\right) \arrow[rr, shift left, "\phi_k"] \arrow[rr, shift right] \arrow[d, dash, "2"] & & \mathbb{Q}\left(\sqrt[4]{2}, i\right) \arrow[d, equal] \\
\mathbb{Q}\left(\sqrt[4]{2}\right) \arrow[rr, shift left=3, "\varphi_j"] \arrow[rr, shift left=1] \arrow[rr, shift right=1] \arrow[rr, shift right=3] \arrow[dr, dash, "4"] & & \mathbb{Q}\left(\sqrt[4]{2}, i\right) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

We now have a group with 8 elements. In particular, there is a map $s \in \mathrm{Gal}\left(x^4 - 2/\mathbb{Q}\right)$ such that $s\left(\sqrt[4]{2}\right) = \sqrt[4]{2}$ and $s(i) = -i$, and there is another map $r \in \mathrm{Gal}\left(x^4 - 2/\mathbb{Q}\right)$, where $r\left(\sqrt[4]{2}\right) = \sqrt[4]{2}i$ and $r(i) = i$. Then $\mathrm{Gal}\left(x^4 - 2/\mathbb{Q}\right) = \langle r, s\rangle = D_4$.

Theorem: (The Existence of Splitting Fields) Let k be a field and $p \in k[x]$ a monic polynomial of degree n. Then there is a field extension E/k that is a splitting field for p, and $[E:k] \leq n!$.

Proof: Let $p_1(x)$ be an irreducible factor of p and let $K_1 = k[x]/(p_1)$. Then p_1 has a root z_1 in K_1 and $[K_1 : k] = \deg p_1 \leq n$, and $p(x) = (x - z_1)q_1(x)$ in $K_1[x]$.

Now let p_2 be an irreducible factor of q_1 in $K_1[x]$ and let $K_2 = K_1[x]/(p_2)$. Then K_2 is a field extension of K_1, and therefore of k. Now p_2 has a root z_2 in K_2, and $[K_2 : K_1] = \deg p_2 \leq \deg q_1 \leq n - 1$. Repeat this process until we reach K_n, which contains every root of p and satisfies $[K_n : k] \leq n!$.

$$\begin{tikzcd}
K_n \arrow[d, dash, "\leq 1"] \\
\vdots \arrow[d, dash, "\leq n-1"] \\
K_1 \arrow[d, dash, "\leq n"] \\
k
\end{tikzcd}$$

Theorem: (The Uniqueness of Splitting Fields) Let k be a field and let $p \in k[x]$ be a polynomial of degree n. If p splits completely in some field L/k, then the splitting field of p is uniquely determined as a subset of L. Moreover, any two splitting fields of p are k-isomorphic — that is, isomorphic with the map fixing k.

Proof: If p splits completely in L, then the roots of p are uniquely determined, since $L[x]$ is a principal ideal domain, and therefore a unique factorization domain. Thus the splitting field for p is both uniquely determined and contained in L.

To prove the second claim, let E/k be a splitting field for p. Since we already constructed a splitting field K_n for p in the previous theorem, we need only show that $E \simeq K_n$. Let $z_1, ..., z_n$ be the roots of p. Then $k[x]/(p_1) \simeq k(z_1) \simeq K_1$, with some isomorphism $\varphi_1 : K_1 \longrightarrow k(z_1)$. By the extension lemma, there is an isomorphism $\varphi_2 : K_2 \longrightarrow k(z_1)(z_2) = k(z_1, z_2)$ that fixes $k(z_1) = K_1$. Repeat to create an isomorphism $\varphi_n : K_n \longrightarrow k(z_1, ..., z_n) = E$ with $\varphi_n|_k = id$.

$$\begin{tikzcd}
K_n \arrow[rr, hook, two heads, "\varphi_n"] \arrow[d, dash] & & k(z_1,...,z_n) \arrow[d, dash] \\
\vdots \arrow[d, dash] & & \vdots \arrow[d, dash] \\
K_2 \arrow[rr, hook, two heads, "\varphi_2"] \arrow[d, dash] & & k(z_1,z_2) \arrow[d, dash] \\
K_1 \arrow[rr, hook, two heads, "\varphi_1"] \arrow[dr, dash] & & k(z_1) \arrow[dl, dash] \\
& k &
\end{tikzcd}$$

Theorem: (The Permutation Action) Let k be a field and $p \in k[x]$ an irreducible polynomial of degree n, and let E/k be the splitting field of p. Then $\text{Gal}(E/k)$ acts faithfully and transitively on the roots of p — that is, no element of $\text{Gal}(E/k)$ fixes all the roots of p except the identity (so $\text{Gal}(E/k)$ is isomorphic to a subgroup of S_n), and if z and z' are roots of p, then there is a $\sigma \in \text{Gal}(E/k)$ such that $\sigma(z) = z'$.

Proof: Let $X = \{z_1, ..., z_n\} \subseteq E$ be the roots of p, and let $\sigma \in \text{Gal}(E/k)$. Since p is a polynomial, $p(\sigma(z_i)) = \sigma(p(z_i))$, and $\sigma(p(z_i)) = \sigma(0) = 0$, so $\sigma(z_i) \in X$. Thus σ permutes X.

Now since $\text{Gal}(E/k)$ acts on X, there is a homomorphism $\alpha : \text{Gal}(E/k) \longrightarrow S_n$ by definition. And $\ker \alpha = \{\sigma \in \text{Gal}(E/k) \mid \sigma(z_i) = z_i \text{ for all } i\}$, so any $\sigma \in \ker \alpha$ fixes k and all z_i, and therefore fixes $k(z_1, ..., z_n) = E$. Thus $\ker \alpha = \{id\}$, so by the first isomorphism theorem, $\text{Gal}(E/k) \simeq \text{range } \alpha \leq S_n$. Thus $\text{Gal}(E/k)$ acts faithfully on the roots of p.

Now let z and z' be roots of p. Let $K = K_n$ be the splitting field from the proof of existence and $\phi = \varphi_n : K \longrightarrow E$ be the isomorphism from the proof of uniqueness. Then $\phi(\overline{x}) = z_1$ from the construction of ϕ, but the choice of z_1 in that construction was arbitrary, since p is irreducible. Thus there is another isomorphism $\phi' : K \longrightarrow E$, where $\phi'(\overline{x}) = z'$. Let $\sigma = \phi' \circ \phi^{-1}$. Then $\sigma(z) = z'$ and $\sigma \in \text{Gal}(E/k)$ (since $\text{Gal}(E/k)$ is isomorphic to a subgroup of S_n), and so $\text{Gal}(E/k)$ acts transitively on the roots of p.

Corollary: Only transitive subgroups of S_n can potentially be Galois groups of splitting fields.

XI — Finite Fields

Definition: A **finite field** is a field with finite cardinality.

Theorem: Let k be a finite field. Then $|k| = p^n$ for some prime p and $n \in \mathbb{N}$. Moreover, k is the splitting field for $x^{p^n} - x$ over C_p — it consists exactly of the roots of $x^{p^n} - x$.

Proof: Define a ring homomorphism $\varphi : \mathbb{Z} \longrightarrow k$ by $\varphi(m) = m \cdot 1$ — that is, $1 \in k$ added to itself m times. Since k is a field, it is an integral domain, so if $ab = 0$, then either $a = 0$ or $b = 0$. Thus $\ker \varphi$ is prime, since $\varphi(ml) = ml \cdot 1 = (m \cdot 1)(l \cdot 1) = \varphi(m)\varphi(l)$ by the distributive property for fields, so if $\varphi(ml) = 0$, either $\varphi(m) = 0$ or $\varphi(l) = 0$. Moreover, since k is finite, $\ker \varphi \neq (0)$. Since $\mathbb{Z}$ is a principal ideal domain, $\ker \varphi = (p)$ for some prime number $p \in \mathbb{Z}$. Then $C_p \simeq \mathbb{Z}/(p) \simeq \varphi(\mathbb{Z}) \subseteq k$, so $C_p \subseteq k$. Thus k is a C_p vector space, and since k is finite, it is of finite dimension. Thus $k \simeq C_p^n$ for some $n \in \mathbb{N}$, and so $|k| = p^n$.

Now if $a \in k^\times$, then $|a| \bigm| |k^\times| = p^n - 1$ by Lagrange's theorem, so $a^{p^n - 1} = 1$. Thus $a^{p^n-1} - 1 = 0$, so a is a root of $x^{p^n-1} - 1$, and therefore also of $(x)\left(x^{p^n-1} - 1\right) = x^{p^n} - x$. And $0 \in k$ is also a root of this polynomial, so every element in k is a root of $x^{p^n} - x$. Since there are p^n roots and $|k| = p^n$, k is the smallest field containing all those roots, so it is the splitting field for $x^{p^n} - x$ by definition.

Theorem: Let p be a prime and $n \in \mathbb{N}$. Then there is a unique field with cardinality p^n up to isomorphism: the splitting field of $x^{p^n} - x$ over $\mathbb{Z}$.

Proof: By the existence and uniqueness theorems, there is a unique splitting field E for $x^{p^n} - x$ over C_p. All we need show is that $|E| = p^n$.

Let $K = \{a \in E \mid a^{p^n} = a\}$. Then if $a, b \in K$, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, since we are over C_p, and so $(a+b)^{p^n} = a + b$. Thus $a + b \in K$. Also, $(ab)^{p^n} = a^{p^n} b^{p^n} = ab$, so $ab \in K$. Since, $a^{p^n} - a = 0$, $(a)\left(a^{p^n-1} - 1\right)$, so if $a \neq 0$, then $a^{p^n-1} = 1$. Thus $a^{-1} = a^{p^n-2}$, and since $\left(a^{p^n-2}\right)^{p^n} = \left(a^{p^n}\right)^{p^n-2} = a^{p^n-2}$, $a^{p^n-2} \in K$. Thus K is a field. Since K obviously contains all the roots of $x^{p^n} - x$, $x^{p^n} - x$ splits completely in K, and therefore $E \subseteq K$. But $K \subseteq E$, so $E = K$.

There is one more technical thing to check. We have shown that E contains exactly the roots of $x^{p^n} - x$, but if $x^{p^n} - x$ has repeated roots, then $|E| < p^n$. However, this cannot be the case, since if there were a repeated root z, then $\frac{\mathrm{d}}{\mathrm{d}x}\left[x^{p^n} - x\right] = \frac{\mathrm{d}}{\mathrm{d}x}\left[(x-z)^2 q(x)\right] = 2(x-z) + (x-z)^2 q'(x)$ for some $q(x)$, and so $\frac{\mathrm{d}}{\mathrm{d}x}\left[x^{p^n} - x\right]\Big|_{x=z} = 0$. But $\frac{\mathrm{d}}{\mathrm{d}x}\left[x^{p^n} - x\right] = p^n x^{p^n-1} - 1 = -1 \neq 0$, so this cannot be the case. Thus $|E| = p^n$.

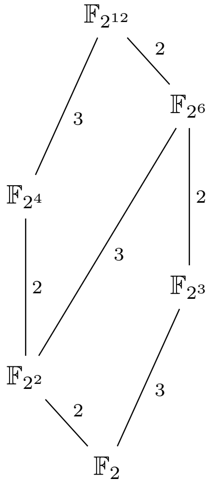
Definition: $\mathbb{F}_n$ is the unique finite field with n elements, if it exists.

Proposition: $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m|n$.

Proof: ($\Rightarrow$) If $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then $n = [\mathbb{F}_{p^n} : \mathbb{F}] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]m$, so $m|n$.

($\Leftarrow$) Suppose $m|n$. For any $q \in \mathbb{N}$, $p^{mq} - 1 = (p^m)^q - 1 = (p^m - 1)\left(p^{m(q-1)} + p^{m(q-2)} + \cdots + p^m + 1\right)$. In particular, with $q = \frac{n}{m}$, $p^n - 1 = (p^m - 1)\left(p^{n-m} + p^{n-2m} + \cdots + p^m + 1\right)$. Thus $(p^m - 1)\,|\,(p^n - 1)$. Now for any nonzero $z \in \mathbb{F}_{p^m}$, $z^{p^m - 1} = 1$, so $z^{p^n - 1} = 1$. Thus $z \in \mathbb{F}_{p^n}$.

Example: The field extensions of $\mathbb{F}_2$ up to $\mathbb{F}_{2^{12}}$:



Definition: Let p be a prime and $n \in \mathbb{N}$. The **Frobenius automorphism** is the map $\phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ given by $\phi(a) = a^p$.

Proposition: The Frobenius automorphism is in fact an automorphism, and it fixes $\mathbb{F}_p$.

Proof: Let $\phi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ be defined by $\phi(a) = a^p$ for $n \in \mathbb{N}$ and p prime. First, ϕ fixes $\mathbb{F}_p$, since any nonzero $a \in \mathbb{F}_p$ is also an element of $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$. $\mathbb{F}_p^\times$ is a group under multiplication, so $|a| \,\Big|\, \left|\mathbb{F}_p^\times\right| = p - 1$. In particular, $a^{p-1} = 1$, so $a^p = a$. Thus $\phi(a) = a^p = a$, so $\phi|_{\mathbb{F}_p} = id$.

To show ϕ is an isomorphism, let $a, b \in \mathbb{F}_{p^n}$. Then $\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b)$ and $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$, so ϕ is multiplicative. Now we need only show that ϕ is a bijection. If $\phi(a) = \phi(b)$ for $a, b \in \mathbb{F}_{p^n}$, then $a^p = b^p$, so $(a^p)^{p^{n-1}} = (b^p)^{p^{n-1}}$, and therefore $a = b$, so ϕ is injective. And if $a \in \mathbb{F}_{p^n}$, then $\phi\left(a^{p^{n-1}}\right) = a^{p^n} = a$, so ϕ is surjective. Thus ϕ is, in fact, an automorphism.

Theorem: Let p be a prime and $n \in \mathbb{N}$. Then $\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right) = \langle \phi \rangle \simeq C_n$, where ϕ is the Frobenius automorphism.

Proof: We already know that $\phi \in \operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. To find the order of ϕ, suppose $\phi^i = id$ for some $i \in \mathbb{N}$. Then for all $x \in \mathbb{F}_{p^n}$, $x^{p^i} = x$. But this polynomial only has p^i roots, and we know that there are p^n elements of $\mathbb{F}_{p^n}$, so $i = n$. However, $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so by the extension lemma, there are n $\mathbb{F}_p$-automorphisms of $\mathbb{F}_{p^n}$, so $|\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. Thus $\operatorname{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle \simeq C_n$.

XII — Separability

Comment: Let k be as field and $p \in k[x]$. If E is the splitting field of p, we are not necessarily guaranteed that $|\mathrm{Gal}(E/k)| = [E:k]$: for example, if $k = \mathbb{F}_P(t)$ and $p(x) = x^p - t$, then $E = k\left(\sqrt[p]{t}\right)$ and $[E:k] = p$, but $\mathrm{Gal}(E/k) = \{e\}$, since $x^p - t = \left(x - \sqrt[p]{t}\right)^p$, so there is only one root to permute.

Comment: Even if E/k is a finite extension, we are not guaranteed a $z \in E$ with $E = k(z)$: for example, with $k = \mathbb{F}_2(s,t)$ and $E = k(\sqrt{s}, \sqrt{t})$, then any element $z \in E$ satisfies $z = a_0 + a_1\sqrt{s} + a_2\sqrt{t} + a_3\sqrt{st}$, so $z^2 = a_0^2 + a_1^2 s + a_2^2 t + a_3^2 st \in k$. Thus every element of E has degree 2 over k, but $[E:k] = 4$.

Definition: Let k be a field. An irreducible polynomial $p \in k[x]$ is **separable** if p has no repeated roots in its splitting field.

Definition: Let k be a field and E/k be a field extension. An element $z \in E$ is **separable** if $m_{z/k}$ is separable.

Definition: Let k be a field. A field extension E/k is **separable** if $z \in E$ is separable for all z. E/k is **purely inseparable** if no $z \in E$ is separable.

Example: In $\mathbb{F}_p(t)$, $x^p - t$ is not separable, so neither is $\sqrt[p]{t}$. This means that $E = k\left(\sqrt[p]{t}\right)$ is not a separable extension.

Comment: Galois theory is a theory of separable extensions.

Definition: A field k is **perfect** if either char $k = 0$ or char $k = p > 0$ and $\phi : a \longmapsto a^p$ is an automorphism of k.

Example: $\mathbb{Q}$ and $\mathbb{F}_p$ are perfect.

Theorem: If k is perfect, then any irreducible polynomial $p \in k[x]$ is separable.

Proof: Let $p \in k[x]$ be irreducible, let E/k be the splitting field for p, and let $z \in E$ be a root of p. Suppose $p(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then $p'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. Now either $p' = 0$ or $\deg p' < \deg p$. Since $\ker \varepsilon_z = (p)$, $p'(z) = 0$ if and only if $p | p'$ or $p' = 0$. But if $p | p'$, then $\deg p \leq \deg p'$, so this cannot happen. Thus $p'(z) = 0$ if and only if $p' = 0$.

Now we can approach the theorem statement. We know $p(x) = (x-z)^m q(x)$ for some $m \in \mathbb{N}$ and q such that $q(z) \neq 0$. We need only show $m = 1$. With this representation of p, $p'(x) = m(x-z)^{m-1} q(x) + (x-z)^m q'(x)$. If $p'(z) = 0$, then $m - 1 \geq 1$, since $q(z) \neq 0$, so $m \geq 2 > 1$. Thus $p' = 0$ if and only if p is not separable.

Since k is perfect, either char $k = 0$ or char $k = c > 0$ and $\phi : a \longmapsto a^c$ is an automorphism of k. If char $k = 0$, then $p' \neq 0$, since p is obviously nonconstant. If char $k = c > 0$, then $p'(x) = 0$ if and only if $p(x) = g(x^c)$ for some $g \in k[x]$. But since ϕ is an automorphism of k, $g(x^c) = h(x)^c$ for some $h \in k[x]$. Thus $p(x) = h(x)^c$, which implies that p is not irreducible. ↯

In both cases, $p' \neq 0$, so p is separable.

Definition: Let k be a field and E/k a field extension. The **separable degree** $[E:k]_s$ of E/k is the number of k-embeddings of E into any splitting field L that contains E.

Comment: By the extension lemma, the separable degree is multiplicative.

Comment: If k is a field and E/k is a splitting field, then $[E:k]_s = |\mathrm{Gal}(E/k)|$.

Proposition: An element z is separable over k if and only if $[k(z):k]_s = [k(z):k]$.

Proof: If z/k is separable, then $m_{z/k}$ has no repeated roots in its splitting field. Then there are $[k(z):k] = \deg m_{z/k}$ roots of $m_{z/k}$, and since none is repeated, a k-embedding of $k(z)$ into a splitting field for $m_{z/k}$ can send z to any of the $[k(z):k]$ of them. Thus $[k(z):k]_s = [k(z):k]$.

Proposition: Let k be a field. Then an element z is separable over k if and only if $k(z)/k$ is a separable extension.

Proof: If $k(z)/k$ is separable, then every element of $k(z)$ is separable over k, so in particular, z is separable. To prove the other direction, suppose z is separable over k and let $w \in k(z)$. Now $[k(z):k]_s = [k(z):k]$ by the previous proposition, and clearly, z is separable over $k(w)$, since $m_{z/k(w)} | m_{z/k}$. Thus $[k(z):k(w)] = [k(z):k(w)]_s$, so $[k(z):k] = [k(z):k(w)][k(w):k]_s$ and $[k(z):k] = [k(z):k(w)][k(w):k]$. Thus $[k(w):k] = [k(w):k]_s$, so w is separable over k. Thus $k(z)/k$ is separable.

Lemma: Let k be a finite field. Then $k^\times$ is cyclic.

Proof: Any polynomial $x^d - 1 \in k[x]$ can have at most d roots. If there is an element a of order d in $k^\times$, then all d elements in $\langle a \rangle$ has order dividing d, so they are all roots of $x^d - 1$. Thus all the elements of order d in $k^\times$ are contained in $\langle a \rangle$. In particular, the number of elements of order exactly d is $\varphi(d)$, since $\langle a \rangle \simeq C_d$. Now if ${k^\times}_d$ is the subset of $k^\times$ of elements of order d and $n = |k^\times|$, then $n = \sum_{d|n} |{k^\times}_d| \leq \sum_{d|n} \varphi(d) = n$. Thus there is an element of every order $d|n$, so in particular, there is an element of order n. Thus $k^\times$ is cyclic.

Theorem: (They Choose a Leader) Let k be a field, E/k a finite extension, and $v, w \in E$ separable over k. Then $k(v,w)/k$ is separable, and $k(v,w) = k(z)$ for some $z \in E$.

Proof: First, suppose k is finite. Then E is finite, so $k(v,w)$ is too. Thus $k(v,w)^\times$ is cyclic, so it has a generator z. Since every element of $k(v,w)^\times$ is a power of z by definition, $k(v,w) = k(z)$. And since k is perfect, z is separable over k because its minimal polynomial is irreducible by definition. By the previous proposition, $k(z)/k$ is separable.

If k is infinite, things are more complicated. First, let L be a splitting field containing $k(v,w)$ and let $n = [K(v,w) : k(v)]$ and $m = [k(v) : k]$. Since $k(v,w)$ is separable over k, so is $k(v)$, so $n = [k(v,w) : k(v)]_s$ and $m = [k(v) : k]_s$. Thus there are exactly mn k-embeddings of E into L, say $\sigma_1, ..., \sigma_{mn}$.

Now let

$$p(x) = \prod_{1 \le i < j \le mn} (\sigma_i(v + wx) - \sigma_j(v + wx)).$$

Since σ_i and σ_j are distinct on v and w, no factor of p is zero. Thus $p \neq 0$, and in a bizarre argument, since p can only have finitely many roots and k is infinite, there must be a $c \in k$ with $p(c) \neq 0$. Let $z = v + wc$ — then $\sigma_i(z) \neq \sigma_j(z)$ for any $i \neq j$, since $p(c) \neq 0$, and therefore every σ_i is a distinct k-embedding of $k(z)$ into L. Thus $[k(z) : k]_s = mn$, but $[k(z) : k] \ge [k(z) : k]_s = mn$ and $k(z) \subseteq k(v,w)$, so $[k(z) : k] \le mn$. Thus $[k(z) : k] = [k(z) : k]_s = mn$, and so $k(z)$ is separable and $k(z) = k(v,w)$.

Definition: Let k be a field and let E/k be a finite extension. An element $z \in E$ is **primitive** if $E = k(z)$.

Theorem: (The Primitive Element Theorem) Every finite, separable extension has a primitive element.

Proof: Let k be a field and let $E = k(z_1, ..., z_n)$ be a finite extension of k, where $z_1, ..., z_n$ are separable over k. By $n - 1$ applications of the previous theorem, $k(z_1, ..., z_n) = k(z)$ for some separable z, so E has a primitive element.

Theorem: (The Separable Structure of Finite Extensions) Let k be a field and let E/k be a finite extension. Then $F = \{z \in E \mid z/k \text{ is separable}\}$ is a separable subfield of E. Moreover, E/F is purely inseparable, so $[F : k] = [F : k]_s = [E : k]_s$.

XIII — The Fundamental Theorem of Galois Theory

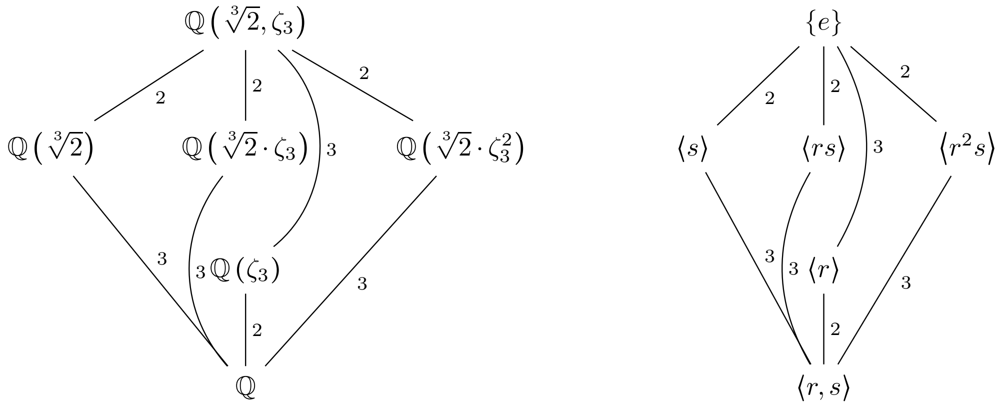
Definition: Let k be a field. An extension E/k is **Galois** if E is a separable splitting field over k.

Definition: Let k be a field and E/k an extension, and let $H \leq \mathrm{Gal}(E/k)$. The **fixed field** of H is $E^H = \{z \in E \mid \sigma(z) = a \text{ for all } \sigma \in H\}$.

Comment: E^H is indeed a field, since being fixed by a ring homomorphism commutes with all the field operations.

Comment: We would like to establish a correspondence between fixed fields of E and subgroups of $\mathrm{Gal}(E/k)$.

Example: Let $p(x) = x^3 - 2$. Then its splitting field over $\mathbb{Q}$ is $E = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$, and its Galois group is D_3. Now we have $E^{\langle r\rangle} = \mathbb{Q}(\zeta_3)$, $E^{\langle s\rangle} = \mathbb{Q}\left(\sqrt[3]{2}\right)$, $E^{\langle rs\rangle} = \mathbb{Q}\left(\sqrt[3]{2}\cdot\zeta_3\right)$, and $E^{\langle r^2 s\rangle} = \mathbb{Q}\left(\sqrt[3]{2}\cdot\zeta_3^2\right)$. Obviously, $E^{\{e\}} = E$ and $E^{\langle r,s\rangle} = \mathbb{Q}$. Drawing a diagram for these extensions and their corresponding subgroups of D_3, we see that the subgroup lattice is exactly upside-down, and the degrees of the field extensions even match the indices of the subgroups.



$\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$
$\mathbb{Q}\left(\sqrt[3]{2}\right)$
$\mathbb{Q}\left(\sqrt[3]{2}\cdot\zeta_3\right)$
$\mathbb{Q}\left(\sqrt[3]{2}\cdot\zeta_3^2\right)$
$\mathbb{Q}(\zeta_3)$
$\mathbb{Q}$
2
2
2
3
3
3
3
2
$\{e\}$
$\langle s\rangle$
$\langle rs\rangle$
$\langle r^2 s\rangle$
$\langle r\rangle$
$\langle r, s\rangle$
2
2
2
3
3
3
3
2

Theorem: (The Fundamental Theorem of Galois Theory) Let k be a field and E/k a finite Galois extension.

a) If F is a field such that $k \subseteq F \subseteq E$, then E/F is a Galois extension, and $[E : F] = |\mathrm{Gal}(E/F)|$. In fact, $F = E^{\mathrm{Gal}(E/F)}$.

b) If $H \leq \mathrm{Gal}(E/k)$, then $H = \mathrm{Gal}(E/E^H)$.

c) There is an inclusion-reversing bijection between the subfields of E over k and the subgroups of $\mathrm{Gal}(E/k)$, given by

$$\begin{tikzcd} F \arrow[r, mapsto, "\psi"] & \mathrm{Gal}(E/F) \end{tikzcd}$$

$$\begin{tikzcd} E^H & H \arrow[l, mapsto, "\phi"'] \end{tikzcd}$$

where $\psi\phi = \phi\psi = id$.

Proof:

a) Since E/k is a finite and separable extension, it has a primitive element z by the Primitive Element Theorem. Thus $E = k(z)$. Since z is separable over k, it is also separable over F, and obviously E/F is still the splitting field for z. Thus E/F is a separable splitting field, so it is Galois.

Now let $H = \mathrm{Gal}(E/F)$ and let $p(x) = \prod_{\sigma \in H} (x - \sigma(z))$. Then $p \in E^H[x]$, and since H is transitive on the roots of p (since it is a Galois group), so all the roots of p are conjugate. Thus p must be irreducible in $E^H[x]$, since if even two linear factors in E multiplied to a quadratic factor in E^H, then there would be an element of H that permuted just those two roots. But this would be the identity on E^H, so H would no longer be faithful. ↯

Thus $p = m_{z/E^H}$, the minimal polynomial for z over E^H, and so $[E : E^H] = \deg p$. By definition, $\deg p = |H|$. Now since E/F is separable, $[E : F] = |\mathrm{Gal}(E/F)| = |H| = \deg p = [E : E^H]$. Moreover, since everything in $H = \mathrm{Gal}(E/F)$ fixes F by definition, so $F \subseteq E^H$. By multiplicativity of degree, $[E : F] = [E : E^H][E^H : F]$, but $[E : F] = [E : E^H]$, so $[E^H : F] = 1$. Thus $F = E^H = E^{\mathrm{Gal}(E/F)}$.

b) Let $H \leq \mathrm{Gal}(E/k)$. Then $H \leq \mathrm{Gal}(E/E^H)$ by definition — anything in H fixes everything fixed by H. Now let $E = k(z)$ from the previous proof, and let $p = \prod_{\sigma \in H} (x - \sigma(z))$ once again. As previously shown, p is irreducible over $E^H[x]$, and so $[E : E^H] = |H|$. Since E/E^H is separable, $[E : E^H] = |\mathrm{Gal}(E/E^H)|$, so $|H| = |\mathrm{Gal}(E/E^H)|$. Since E/k is finite, so is E/E^H, so $H = \mathrm{Gal}(E/E^H)$.

c) Let F be a field such that $k \subseteq F \subseteq E$. Then $\phi\psi(F) = \phi(\mathrm{Gal}(E/F)) = E^{\mathrm{Gal}(E/F)}$, and by part 1, this equals F. Now let $H \leq \mathrm{Gal}(E/k)$. Then $\psi\phi(H) = \psi(E^H) = \mathrm{Gal}(E/E^H)$, and by part 2, this equals H. Thus ϕ and ψ are inverses.

To show that the maps are inclusion-reversing, let F and K be fields such that $k \subseteq F \subseteq K \subseteq E$. Then $\psi(K) = \mathrm{Gal}(E/K) \leq \psi(F) = \mathrm{Gal}(E/F)$, since any automorphism fixing K must also fix F. Now let H and I be groups such that $H \leq I \leq \mathrm{Gal}(E/k)$. Then $\phi(I) = E^I \subseteq \phi(H) = E^H$, since anything fixed by all of I must also be fixed by everything in H — if not, then there would be an automorphism in H that was not in I, but $H \leq I$. Thus ϕ and ψ are inclusion-reversing.

Example: Let $f(x) = (x^2 - 2)(x^3 - 3)$. Then The splitting field for f is $E = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$, so $[E : \mathbb{Q}] = 4$, and $\mathrm{Gal}(E/\mathbb{Q}) = C_2 \times C_2$. If $\sigma, \tau \in \mathrm{Gal}(E/k)$ are such that $\sigma\left(\sqrt{3}\right) = -\sqrt{3}$ and $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$, then we have:

$$\begin{tikzcd}
& E \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}\left(\sqrt{2}\right) \arrow[dr, dash] & \mathbb{Q}\left(\sqrt{6}\right) \arrow[d, dash] & \mathbb{Q}\left(\sqrt{3}\right) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \langle e \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \sigma\tau \rangle \arrow[d, dash] & \langle \tau \rangle \arrow[dl, dash] \\
& C_2 \times C_2 &
\end{tikzcd}$$

To find $\mathrm{Gal}\left(f/\mathbb{Q}\left(\sqrt{2}\right)\right)$, we know $\mathbb{Q}\left(\sqrt{2}\right) = E^{\langle\sigma\rangle}$, so $\mathrm{Gal}\left(f/\mathbb{Q}\left(\sqrt{2}\right)\right) = \langle\sigma\rangle$.

Example: Let $f(x) = x^5 - 1$. Then $\mathrm{Gal}(f/\mathbb{Q}) = \langle\sigma\rangle$, where $\sigma(\zeta_5) = \zeta_5^2$. Then we have:

$$\begin{tikzcd}
\mathbb{Q}(\zeta_5) \arrow[d, dash] & \langle e \rangle \arrow[d, dash] \\
\mathbb{Q}\left(\zeta_5 + \zeta_5^4\right) \arrow[d, dash] & \left\langle \sigma^2 \right\rangle \arrow[d, dash] \\
\mathbb{Q} & \langle \sigma \rangle
\end{tikzcd}$$

We get $\zeta_5 + \zeta_5^4$ by applying σ^2 repeatedly to a primitive element until we get the element back again, and then adding all of the results.

Comment: If E/k is Galois and $k \subseteq F \subseteq E$, then E/F is Galois, but F/k may not be: for example, if $k = \mathbb{Q}$, $E = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$, and $F = \mathbb{Q}\left(\sqrt[3]{2}\right)$, then $\mathrm{Gal}(F/k) = \{e\}$, so $[F : k] = 3 \neq |\mathrm{Gal}(F/k)|$. Thus F is not separable, so it is not Galois.

Definition: Let G be a group and $H \leq G$ a subgroup. The **normalizer** of H in G is $N_G(H) = \{a \in G \mid aH = Ha\}$.

Theorem: (The Normal Subgroup Theorem) Let k be a field and E/k a finite Galois extension. Let $G = \mathrm{Gal}(E/k)$, let F be a field such that $k \subseteq F \subseteq E$, and let $H = \mathrm{Gal}(E/F)$. Then $\mathrm{Gal}(F/k) \simeq N_G(H)/H$, and F/k is Galois if and only if $H \lhd G$.

Proof: By the extension lemma, any k-automorphism of F extends to a k-automorphism of E, and by the uniqueness of splitting fields, this extended automorphism is some $\sigma \in \mathrm{Gal}(E/k)$. Thus every element of $\mathrm{Gal}(F/k)$ is some element of $\mathrm{Gal}(E/k)$ that is restricted to F.

Since $H = \mathrm{Gal}(E/F)$ fixes F, $\sigma H \sigma^{-1}$ fixes $\sigma(F)$. Thus $\mathrm{Gal}(E/\sigma(F)) = \sigma H \sigma^{-1}$, so $F = \sigma(F)$ if and only if $H = \sigma H \sigma^{-1}$. But $H = \sigma H \sigma^{-1}$ if and only if $\sigma \in N_G(H) \leq G$. Thus for $\sigma \in N_G(H)$, $\sigma(F) = F$. By definition, these σ are in $\mathrm{Gal}(F/k)$ — notice that the σ do not *fix* F, but rather permute it — so we have a homomorphism from $N_G(H) \longrightarrow \mathrm{Gal}(F/k)$ given by restriction to F. The homomorphism is surjective by the extension lemma, and the kernel is $\{\sigma \in N_G(H) \mid \sigma|_F = id\}$. But this is $\mathrm{Gal}(E/F)$ by definition, so by the first isomorphism theorem, $N_G(H)/H \simeq \mathrm{Gal}(F/k)$.

Now we show that F/k is Galois if and only if $H \lhd G$.

($\Rightarrow$) Suppose F/k is Galois. Then $|\mathrm{Gal}(F/k)| = [F : k]$, so $\frac{|N_G(H)|}{|H|} = \frac{|G|}{|H|}$. Thus $|N_G(H)| = |G|$, and since G is finite, $N_G(H) = G$. Thus $H \lhd G$.

($\Leftarrow$) Suppose $H \lhd G$. Then $\mathrm{Gal}(F/k) \simeq G/H$, so $|\mathrm{Gal}(F/k)| = \frac{|G|}{|H|}$, since G is finite. But E/k is Galois, so $|G| = |\mathrm{Gal}(E/k)| = [E : k]$, and E/F is Galois by the fundamental theorem, so $|H| = |\mathrm{Gal}(E/F)| = [E : F]$. Thus $|G| = |H|[F : k]$, so $[F : k] = \frac{|G|}{|H|} = |\mathrm{Gal}(F/k)|$. Thus F/k is Galois.

Corollary: If $H \lhd G$, then $\mathrm{Gal}(F/k) \simeq \dfrac{\mathrm{Gal}(E/k)}{\mathrm{Gal}(E/F)}$.

Example: Find the splitting field of $x^{13} - 1$ over $\mathbb{F}_3$, show that E is also the splitting field of $x^3 - x^2 + x + 1$, and express $x^{13} - 1$ as a product of linear factors in $E[x]$.

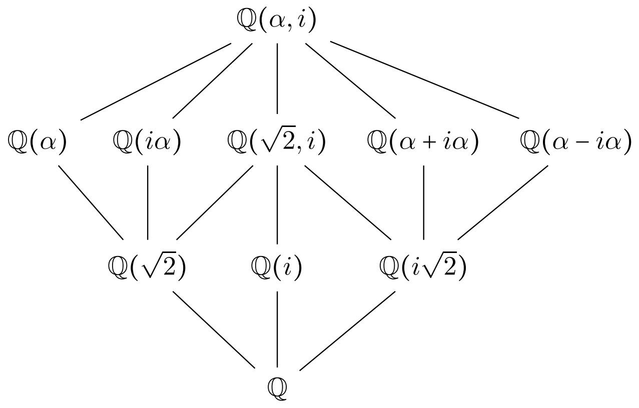
Let E be the splitting field. Any root of $x^13 - 1$ has order 1 or 13 in $E^\times$, and the first finite field with elements of order 13 in its group of units is $\mathbb{F}_{27} = \mathbb{F}_{(2)(13)+1}$. Thus $E = \mathbb{F}_{27}$.

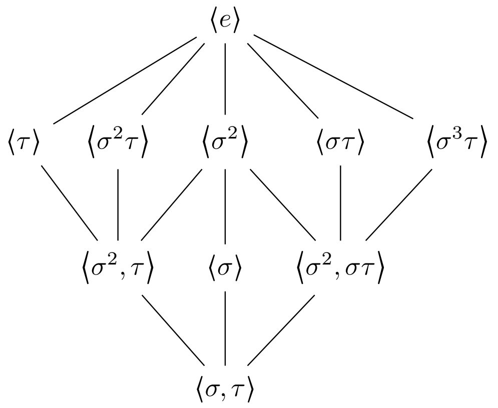
To show that the splitting field of $x^3 - x^2 + x + 1$ over $\mathbb{F}_3$ is also E, first notice that $x^3 - x^2 + x + 1$ is irreducible over $\mathbb{F}_3$ — neither 0, 1, or 2 make the polynomial vanish. Thus $x^3 - x^2 + x + 1$ splits completely in $\mathbb{F}_3/(x^3 - x^2 + x + 1) \simeq \mathbb{F}_{27}$. If a is a root of $x^3 - x^2 + x + 1$, then $a^{27} - a = 0$, since $x^3 - x^2 + x + 1 \;\big|\; x^{27} - x$. Thus E is the splitting field for $x^3 - x^2 + x + 1$.

Finally, let z be a generator of $E^\times$, which we have previously shown is cyclic. Then $|z| = 16$, so $\left|z^2\right| = 13$, and therefore $x^{13} - 1 = \prod_{i=1}^{13} \left(x - z^{2i}\right)$.

Example: Find the Galois subextensions of $x^4 - 2$ over $\mathbb{Q}$.

Let $\alpha = \sqrt[4]{2}$, $\sigma = (1234)$, and $\tau = (24)$. Then we have




$\langle e \rangle$
$\langle \tau \rangle$
$\langle \sigma^2\tau \rangle$
$\langle \sigma^2 \rangle$
$\langle \sigma\tau \rangle$
$\langle \sigma^3\tau \rangle$
$\langle \sigma^2, \tau \rangle$
$\langle \sigma \rangle$
$\langle \sigma^2, \sigma\tau \rangle$
$\langle \sigma, \tau \rangle$

Now the normal subgroups of $\langle \sigma, \tau \rangle$ are $\langle e \rangle$, $\langle \sigma^2 \rangle$, $\langle \sigma^2, \tau \rangle$, $\langle \sigma \rangle$, $\langle \sigma^2, \sigma\tau \rangle$, and $\langle \sigma, \tau \rangle$, so the Galois subextensions of $\mathbb{Q}(\alpha, i)/\mathbb{Q}$ are $\mathbb{Q}(\alpha, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$, and $\mathbb{Q}/\mathbb{Q}$.

XIV — Cyclotomic Extensions

Definition: Let k be a field. A Galois extension E/k is **abelian** is $\mathrm{Gal}(E/k)$ is abelian.

Definition: Let k be a field. A Galois extension E/k is **cyclic** is $\mathrm{Gal}(E/k)$ is cyclic.

Proposition: Let $n \in \mathbb{N}$ and let $\Phi_n(x)$ be the nth cycloctomic polynomial. Then $\Phi_n(x) = m_{\zeta_n/\mathbb{Q}}$.

Definition: Let $n \in \mathbb{N}$. The nth cyclotomic extension is $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Comment: By the Gauss lemmas, $\Phi_n(x) \in \mathbb{Z}[x]$, and obviously $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois and abelian.

Proposition: Let $n \in \mathbb{N}$. Then $\deg \Phi_n \leq \varphi(n)$, where φ is the Euler phi function.

Proof: Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then σ is an automorphism of $\mathbb{Q}(\zeta_n)$, and it fixes $\mathbb{Q}$, so it is also a group automorphism of $\mathbb{Q}(\zeta_n)^\times$. Thus $|\sigma(\zeta_n)| = |\zeta_n| = n$, so all of the roots of Φ_n are primitive nth roots of unity. There are exactly $\varphi(n)$ of these, so $\deg \Phi_n \leq \varphi(n)$.

Theorem: Let $n \in \mathbb{N}$. Then $\deg \Phi_n = \varphi(n)$.

Proof: By the previous proposition, we need only show that $\deg \Phi_n \geq \varphi(n)$ — that is, that every primitive nth root of unity is a root of Φ_n. Now $x^n - 1 = \Phi_n(x)q(x)$ for some $q \in \mathbb{Z}[x]$, since every root of Φ_n is a root of $x^n - 1$. We first claim that if $\Phi_n(\zeta) = 0$ for some primitive nth root of unity ζ, then $\Phi_n(\zeta^p) = 0$ for all primes p with $p \nmid n$ — or, equivalently, that $q(\zeta^p) \neq 0$.

There is a map $\overline{} : \mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x]$ given by reduction mod p. Now $\overline{x^n - 1} = x^n - \overline{1}$, and $\frac{\mathrm{d}}{\mathrm{d}x}\left[x^n - \overline{1}\right] = \overline{n}x^{n-1} \neq 0$, since $p \nmid n$. Thus $x^n - \overline{1}$ has no repeated roots, and since $x^n - \overline{1} = \overline{x^n - 1} = \left(\overline{\Phi_n x}\right)\left(\overline{q(x)}\right)$, $\gcd\left(\overline{\Phi_n x}, \overline{q}\right) = 1$.

Now suppose $\Phi_n(\zeta) = 0$ and $q(\zeta^p) = 0$ for some primitive nth root of unity ζ. Then $\Phi_n(x)$ and $q(x^p)$ have a common factor, and since Φ_n is irreducible, $\Phi_n(x) | q(x^p)$. Thus $\overline{\Phi_n(x)} | \overline{q(x^p)} = \left(\overline{q(x)}\right)^p$ by the freshman's dream and the fact that $a^p = a$ for $a \in \mathbb{F}_p$. Thus $\gcd\left(\overline{\Phi_n x}, \overline{q}\right) \neq 1$. $\lightning$

Thus if $\Phi_n(\zeta) = 0$, then $q(\zeta^p) \neq 0$, and since $\zeta^n - 1 = 0$, $\Phi_n(\zeta^p) = 0$. Now let $k \in \mathbb{N}$ with $\gcd(k, n) = 1$. Then $k = p_1 \cdots p_r$ for some primes $p_1, \ldots, p_r$. Now $\Phi_n(\zeta^{p_1}) = 0$, and since $p_1 \nmid n$, ζ^{p_1} is another primitive nth root of unity, so $\Phi_n\left((\zeta^{p_1})^{p_2}\right) = 0$. Continuing in this manner, $\Phi_n\left(\zeta^k\right) = 0$. But these ζ^k with $\gcd(k, n) = 1$ are exactly the primitive nth roots of unity, and every one is a root of Φ_n. Thus $\deg \Phi_n = \varphi(n)$.

Corollary: Let $n \in \mathbb{N}$. Then $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proof: Let $d \in \mathbb{N}$. Then every dth root of unity is an nth root, so $\Phi_d | x^n - 1$. Thus $\prod_{d|n} \Phi_d(x) | x^n - 1$, and since $n = \sum_{d|n} \varphi(d)$, $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Corollary: Let ζ_n be a primitive nth root of unity, where n is a prime power. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is cyclic.

Proof: There is an obvious isomorphism between $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $C_n^\times$, where $\sigma \longmapsto i$ if $\sigma(\zeta_n) = \zeta_n^i$. As previously shown, the multiplicative group of a finite field is cyclic, and since n is a prime power, C_n is a finite field. Thus the Galois group is cyclic.

XV — Solvability by Radicals

Example: Express ζ_5 in terms of roots of rationals.

$\operatorname{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq C_4$, and a generator is $\sigma : \zeta_5 \longmapsto \zeta_5^2$. Let $K = \mathbb{Q}(\zeta_5)^{\langle \sigma^4 \rangle}$ be the subfield fixed by id and σ^4. Then a candidate for a primitive element of K is $\left(\sigma^4 + id\right)(\zeta_5) = \zeta_5 + \zeta_5^4 = \zeta_5 + \zeta_5^{-1}$. Now $m_{\zeta_5/K} = x^2 - \left(\zeta_5 + \zeta_5^{-1}\right) + \zeta_5\zeta_5^{-1} = x^2 - 2\cos\frac{2\pi}{5}x + 1$. We would therefore like to determine $\cos\frac{2\pi}{5}$ in terms of radicals. This is equivalent to wanting a polynomial with root $x + x^{-1}$, where $x^5 - 1 = 0$. One method to derive such a polynomial is to notice that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, so $\frac{\Phi_5(x)}{x^2} = x^2 + x + 1 + x^{-1} + x^{-2} = \left(x + x^{-1}\right)^2 + \left(x + x^{-1}\right) - 1$. Thus $y^2 + y - 1 \in \mathbb{Q}[x]$ is our desired polynomial. Using the quadratic formula, $2\cos\frac{2\pi}{5} = \zeta_5 + \zeta_5^{-1} = x + x^{-1} = y = \frac{1}{2}\left(-1 + \sqrt{5}\right)$. Then using the quadratic formula again,

$$\zeta_5 = \frac{\sqrt{5} - 1 + \sqrt{-10 + 2\sqrt{5}}}{4}.$$

Definition: Let k be a field and E/k an extension. An element $z \in E$ is **expressible by radicals** if $z \in k(z_1, ..., z_n)/k$ for some z_i such that for all i, $z_i^{r_i} \in k(z_1, ..., z_{i-1})$ for some $r_i \in \mathbb{N}$.

Definition: Let k be a field. A polynomial $p \in k[x]$ is **solvable by radicals** if all of its roots are expressible by radicals.

Comment: Our first goal is to express every ζ_n by radicals with the r_i as small as possible.

Proposition: Let $n \in \mathbb{N}$ such that $n = rs$ for some $r, s \in \mathbb{N}$ with $\gcd(r, s) = 1$. Let $G = \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $H = \operatorname{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$, and $K = \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ Then $G \simeq H \times K$.

Proof: Since $\mathbb{Q}(\zeta_r) \cap \mathbb{Q}(\zeta_s) = \mathbb{Q}$, $H \cap K = \{id\}$. And since $rx + sy = 1$ for some $x, y \in \mathbb{Z}$, $\zeta_n^i = \zeta_n^{i(rx+sy)} = \zeta_s^{ix}\zeta_r^{iy}$, so $H \times K$ is an internal direct product of groups. Thus $G \simeq H \times K$.

Comment: Let p be a prime, $r \in \mathbb{N}$, and $n = p^r$. Then $\operatorname{Gal}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}) \simeq C_{p^r}^\times \simeq C_{p^r-1}$. In the proof of this fact, we showed that $C_{p^r}^\times$ contains an element of order d for every $d | p^r - 1$. Since $p^r - 1 = (p-1)\left(1 + p + p^2 + \cdots + p^{r-1}\right)$, there is an element of order $p - 1$ in $C_{p^r}^\times$. Thus there is some subfield K of $\mathbb{Q}(\zeta_{p^r})$ that is the fixed field of $C_{p-1} \leq C_{p^r}^\times$.

Theorem: Let $r \in \mathbb{N}$. Then $\operatorname{Gal}(\mathbb{Q}(\zeta_{2^{r+2}})/\mathbb{Q}) = \langle 5 \rangle \times \langle -1 \rangle \leq C_{2^{r+1}}^\times$.

Comment: The motivating example in this section required a primitive element for the intermediate extension. If we want a general method to express ζ_n by radicals, then we will need a method to find primitive elements of the subfields of $\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}$.

Definition: Let p be a prime and ζ a primitive pth root of unity. Let σ be a generator of $\operatorname{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) = C_{p-1}$, and let $\zeta_i = \sigma^i(\zeta)$ for $i = 0, 1, ..., p-2$. Then $\{\zeta_0, \zeta_1, ..., \zeta_{p-2}\} = \{\zeta, \zeta^p, ..., \zeta^{p-1}\}$. Suppose $p - 1 = ef$ for $e, f \in \mathbb{N}$. The ***e* periods of *f* terms** (e and f are quantities here, not adjectives) are

$$\begin{aligned}
\eta_0 &= \zeta_0 + \zeta_e + \zeta_{2e} + \cdots + \zeta_{(f-1)e} \\
\eta_1 &= \zeta_1 + \zeta_{e+1} + \zeta_{2e+1} + \cdots + \zeta_{(f-1)e+1} \\
&\vdots \\
\eta_{e-1} &= \zeta_{e-1} + \zeta_{2e-1} + \zeta_{3e-1} + \cdots + \zeta_{fe-1}
\end{aligned}$$

Notice that every ζ^i for $i \neq 0$ appears exactly once. Moreover, since $\{\zeta_0, \zeta_1, ..., \zeta_{p-2}\}$ is linearly independent by Kronecker's theorem, so is $\{\eta_0, ..., \eta_{e-1}\}$.

Example: Let $p = 7$. Then $\zeta = \zeta_7 = e^{\frac{2\pi i}{7}}$ and $p - 1 = 6 = 6 \cdot 1 = 3 \cdot 2 = 2 \cdot 3 = 1 \cdot 6$. Given a generator $\sigma \in C_7^\times \simeq C_6$,

The 6 periods of 1 term are ζ_0, ζ_1, ζ_2, ζ_3, ζ_4, and ζ_5.

The 3 periods of 2 terms are $\zeta_0 + \zeta_3$, $\zeta_1 + \zeta_4$, and $\zeta_2 + \zeta_5$.

The 2 periods of 3 terms are $\zeta_0 + \zeta_2 + \zeta_4$ and $\zeta_1 + \zeta_3 + \zeta_5$.

The 1 period of 6 terms is $\zeta_0 + \zeta_1 + \zeta_2 + \zeta_3 + \zeta_4 + \zeta_5$.

Comment: Every η_i is obtained by exhausting σ^e on ζ_i. Since $\sigma^j \in \operatorname{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)$, it sends roots to their conjugates, so η_i and $\sigma^j\left(\eta_i\right) = \eta_{i+j}$ are conjugate. Thus all periods of f terms are conjugate.

Definition: Let η be a field of f terms. The **field of *f*-term periods** is $K_f = \mathbb{Q}(\eta)$.

Proposition: K_f contains all f-term periods.

Proof: $K_f \subseteq \mathbb{Q}(\zeta)$, and since $\operatorname{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right) \simeq C_{p-1}$ is abelian, all of its subgroups are normal. Thus all of the subfields of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are Galois, so in particular, K_f is a splitting field. Since K_f contains one period of f terms and all of those periods are conjugate, it follows that K_f contains all f-term periods.

Example: Again, let $p = 7$. Then $K_1 = \mathbb{Q}(\zeta_0) = \mathbb{Q}(\zeta)$, $K_2 = \mathbb{Q}(\zeta_0 + \zeta_3)$, $K_3 = \mathbb{Q}(\zeta_0 + \zeta_2 + \zeta_4)$, and $K_6 = \mathbb{Q}(\zeta_0 + \zeta_1 + \cdots + \zeta_5) = \mathbb{Q}(-1) = \mathbb{Q}$. K_2 is fixed by $\langle \sigma^3 \rangle$, K_3 is fixed by $\langle \sigma^2 \rangle$, and K_6 is fixed by $\langle \sigma \rangle$.

Theorem: Let p be prime, $p - 1 = ef$, η an f-term period, and σ a generator of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq C_{p-1}$. Then

a) $K_f/\mathbb{Q}$ is Galois.

b) $K_f = \mathbb{Q}(\zeta)^{\langle \sigma^e \rangle}$.

c) $\text{Gal}(K_f/\mathbb{Q}) \simeq \langle \sigma \rangle / \langle \sigma^e \rangle$.

d) $[K_f : \mathbb{Q}] = e$.

e) If $p - 1 = gh$ for $g, h \in \mathbb{N}$ and $f|h$, then $K_h \subseteq K_f$ and K_f/K_h is Galois with degree $\frac{e}{g} = \frac{h}{f}$ and Galois group $\langle \sigma^g \rangle / \langle \sigma^e \rangle$.

Proof:

a) As previously argued, $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq C_{p-1}$ is abelian, so all its subgroups are normal. By the normal subgroup theorem, $K_f/\mathbb{Q}$ is Galois.

b) Since K_f is fixed by σ^e but no lower power of σ, $K_f = \mathbb{Q}(\zeta)^{\langle \sigma^e \rangle}$ by the fundamental theorem.

c) Since $K_f = \mathbb{Q}(\zeta)^{\langle \sigma^e \rangle}$, $\text{Gal}(\mathbb{Q}(\zeta)/K_f) = \langle \sigma^e \rangle$ by the fundamental theorem. Since $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \langle \sigma \rangle$, $\text{Gal}(K_f/\mathbb{Q}) = \langle \sigma \rangle / \langle \sigma^e \rangle$ by the normal subgroup theorem.

d) Since $K_f/\mathbb{Q}$ is Galois, it is separable. Thus $[K_f : \mathbb{Q}] = |\text{Gal}(K_f/\mathbb{Q})| = |\langle \sigma \rangle / \langle \sigma^e \rangle| = \frac{ef}{f} = e$.

e) If $p - 1 = gh$, then $\text{Gal}(\mathbb{Q}(\zeta)/K_h) = \langle \sigma^g \rangle$. If $f|h$, then $h = kf$ for some $k \in \mathbb{Z}$, so $ef = gh = gkf$. Then $e = kg$, so $g|e$. Thus $\langle \sigma^e \rangle \leq \langle \sigma^g \rangle$, so by the fundamental theorem, $K_h \subseteq K_f$. Now $\text{Gal}(K_h/\mathbb{Q}) = \langle \sigma \rangle / \langle \sigma^g \rangle$, so $\text{Gal}(K_f/K_h)$ is the subgroup of $\langle \sigma \rangle / \langle \sigma^e \rangle = \{id, \sigma, \sigma^2, ..., \sigma^{e-1}\}$ that fixes K_h. But every automorphism of K_f that fixes K_h is an automorphism of $Q(\zeta)$ that fixes K_h, and those are $(\mathbb{Q}(\zeta)/K_h) = \langle \sigma^g \rangle$. Thus $\text{Gal}(K_f/K_h)$ consists of all the elements of $\{id, \sigma, \sigma^2, ..., \sigma^{e-1}\}$ whose power is divisible by g, and this is exactly $\langle \sigma^g \rangle / \langle \sigma^e \rangle$.

Corollary: Any period of f terms is the root of a polynomial of degree $\frac{h}{f}$ whose coefficients are $\mathbb{Q}$-linear combinations of powers of a period of h terms.

Definition: Let k be a field. The **affine *k*-plane** is $\mathbb{A}^2(k) = \{(x, y) \mid x, y \in k\}$.

Definition: Let k be a field and $S \subseteq \mathbb{A}^2(k)$ a finite subset. A line is **constructible** from S if it contains two points of S. A circle is **constructible** from S if it is centered at a point in S and contains two points of S.

Definition: Let k be a field and $S \subseteq \mathbb{A}^2(k)$ a finite subset. A point is **constructible in one step** from S if it is the intersection of distinct, constructible lines and circles in S.

Definition: Let k be a field and $S \subseteq \mathbb{A}^2(k)$ a finite subset. A point is **constructible** from S if it is constructible in finitely many steps from S.

Definition: Let k be a field and $S \subseteq \mathbb{A}^2(k)$ a finite subset. A point is **constructible** if it is constructible from $\{0, 1\}$.

Lemma: Let k be a field. Then any point constructible in one step from $\mathbb{A}^2(k)$ is contained in $\mathbb{A}^2\left(k\left(\sqrt{d}\right)\right)$ for some $d \in k$.

Proof: The intersection of two distinct lines constructible in one step from $\mathbb{A}^2(k)$ is given by substituting one linear equation into another, which always produces another element of k. The intersection of a line and a circle is given by substituting a linear equation into a quadratic one, which requires at most one square root. The intersection of two distinct circles contains at most two points, so it is equivalent to intersecting one of the circles with the perpendicular bisector of the line joining the two centers of the circles — and this line is constructible, since both centers are.

Theorem: ζ_n is constructible if and only if $\varphi(n) = 2^r$ for some $r \in \mathbb{N}$.

Proof: $(\Rightarrow)$ If ζ_n is constructible, then ζ_n is contained in a tower of quadratic extensions, so $\varphi(n) = |\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right)| = \left[\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right] = 2^r$ for some $r \in \mathbb{N}$.

$(\Leftarrow)$ If $\varphi(n) = 2^r$, then $|\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right)| = 2^r$. But $\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right)$ is abelian, so it has subgroups of every order dividing 2^r. In particular, there is a tower of quadratic extensions containing ζ_n. Thus ζ_n is constructible.

Corollary: It is impossible to square a circle.

Proof: Given a circle with radius 1, its area is π, so we must construct a square with side length $\sqrt{\pi}$. But $[\mathbb{Q}\left(\sqrt{\pi}\right) : \mathbb{Q}] = [\mathbb{Q}\left(\sqrt{\pi}\right) : \mathbb{Q}(\pi)][\mathbb{Q}(\pi) : \mathbb{Q}]$, and since π is not algebraic, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is infinite, and therefore not a finite power of 2.

Corollary: It is impossible to double a cube.

Proof: Given a cube with side length 1, we must construct another with side length $\sqrt[3]{2}$. But $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3 \neq 2^r$ for any $r \in \mathbb{N}$.

Corollary: It is impossible to trisect every angle.

Proof: $\frac{\pi}{3}$, for instance: the trisected angle is $\frac{\pi}{9}$, so we need to construct ζ_{18}, but $[\mathbb{Q}(\zeta_{18}) : \mathbb{Q}] = \varphi(18) = (2-1)\left(3^2-3\right) = 6 \neq 2^r$.

Corollary: It is impossible to construct every regular polygon.

Proof: This requires constructing ζ_n for every n, but this is only possible when $\varphi(n) = 2^r$. Interestingly, the only known primes p for which $\varphi(p) = 2^r$ (so $p = 2^r + 1$) are 3, 5, 17, 257, and 65537 at the time of writing. Therefore, the only n-gons known to be constructible are those for which n is the product of powers of these five numbers.

Theorem: Let $E/\mathbb{Q}$ be a Galois extension and let $G = \mathrm{Gal}(E/\mathbb{Q})$. Then G is abelian if and only if $E \subseteq \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$. In particular, if $\mu = \{z \in \mathbb{C}^* \mid |z| \text{ is finite}\} = \left\{e^{\frac{2\pi ik}{n}} \mid k, n \in \mathbb{N}\right\}$, then every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\mu)$.

Corollary: If $z \in \mathbb{C}$ has an abelian Galois group over $\mathbb{Q}$, then z is expressible by radicals, since every $\zeta_n = \sqrt[n]{1}$.

Comment: The converse of this corollary is false — not every element expressible by radicals over $\mathbb{Q}$ has an abelian Galois group. $\sqrt[3]{2}$, for example, has Galois group D_3 over $\mathbb{Q}$.

Proposition: Let k be a field of characteristic 0 and $p(x) = x^n - a \in k[x]$ a separable polynomial. Then $\mathrm{Gal}(p/k)$ is a solvable group.

Proof: Let E be the splitting field for p. If k already contains every nth root of unity, then $E = k\left(\sqrt[n]{a}\right)$. If $\sigma, \tau \in E$, then $\sigma\left(\sqrt[n]{a}\right) = \zeta_n^i \sqrt[n]{a}$ and $\tau\left(\sqrt[n]{a}\right) = \zeta_n^j \sqrt[n]{a}$ for some $i, j \in \mathbb{N}$. Then $\sigma\tau = \tau\sigma$ since they both fix ζ_n, so $\mathrm{Gal}(p/k)$ is abelian, and therefore solvable.

If k does not contain all of the nth roots of unity, then $E = k\left(\zeta_n, \sqrt[n]{a}\right)$. Let $F = k(\zeta_n)$. Then $\mathrm{Gal}(F/k)$ is abelian. Now F/k is Galois, so by the Normal Subgroup theorem, $\mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/k)$, and since $\mathrm{Gal}(F/k) \simeq \frac{\mathrm{Gal}(E/k)}{\mathrm{Gal}(E/F)}$ and $\mathrm{Gal}(F/k)$ is abelian, $\frac{\mathrm{Gal}(E/k)}{\mathrm{Gal}(E/F)}$ is abelian, and therefore solvable. By the previous paragraph's argument, $\mathrm{Gal}(E/F)$ is solvable. By a proposition from group theory, if $N \lhd G$ and both N and G/N are solvable, then G is too. Thus $\mathrm{Gal}(E/k)$ is solvable.

Theorem: (Galois's Theorem) Let k be a perfect field and $p \in k[x]$ a separable polynomial. If p is solvable by radicals, then $\mathrm{Gal}(p/k)$ is a solvable group.

Proof: Let E be the splitting field for p. Since p is solvable by radicals, $E \subseteq k(z_1, ..., z_n)$, where each $z_i^{r_i} \in k(z_1, ..., z_{i-1})$ for some $r_i \in \mathbb{N}$. Let $a_i = z_i^{r_i}$. Then we have a tower of field extensions:

$$\begin{tikzcd}
K \arrow[d, dash] \\
K_{n-1} \arrow[d, dash] \\
K_{n-2} \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_2 \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
k
\end{tikzcd}$$

Here, each $K_i = K_{i-1}(z_i)$, $K = K_n$, and $k = K_0$. Then each $a_i \in K_{i-1}$. The problem here is that K/k may not be a splitting field, and therefore not Galois, and we will need a Galois extension to complete the proof. Therefore, we will find a larger radical extension L/k that contains K and is Galois.

Let L_1 be the splitting field of $x^{r_1} - a_1$ over k. Then $z_1 \in L_1$, among other things. Now let L_2 be the splitting field of

$$(x^{r_1} - a_1)\left(\prod_{\sigma \in \mathrm{Gal}(L_1/k)} (x^{r_2} - \sigma(a_2))\right).$$

Continuing in this manner, let L_j be the splitting field of

$$(x^{r_1} - a_1)\left(\prod_{\sigma \in \mathrm{Gal}(L_1/k)} (x^{r_2} - \sigma(a_2))\right) \cdots \left(\prod_{\sigma \in \mathrm{Gal}(L_{j-1}/k)} (x^{r_j} - \sigma(a_j))\right),$$

and let $L = L_n$. Now each $L_j \subseteq L_{j+1}$. Since k is perfect, any irreducible polynomial is separable. Thus L/k is separable, since L is a splitting field, and so L/k is Galois.

Let

$$f_j = \left(\prod_{\sigma \in \mathrm{Gal}(L_{j-1}/k)} (x^{r_j} - \sigma(a_j))\right).$$

Now the factors of f_j are permuted by $\mathrm{Gal}(L_{j-1}/k)$, so f_j itself is fixed by everything in $\mathrm{Gal}(L_{j-1}/k)$. Thus $f_j \in k[x]$.

We now claim that $\mathrm{Gal}(L/k)$ is a solvable group. To show this, we will decompose each L_j/L_{j-1} into a tower of smaller extensions that are easier to work with. Let $j \in \{1, ..., n\}$ and let $\mathrm{Gal}(L_j/k) = \{id, \sigma_2, ..., \sigma_r\}$. Now let M_1 be the splitting field of $x^{r_j} - a_j$ over L_{j-1}, M_2 the splitting field of $(x^{r_j} - a_j)(x^{r_j} - \sigma_2(a_j))$, and so on, until M_r is the splitting field of f_j over L_{j-1} (that is, $M_r = L_j$). Then each M_l/M_{l-1} is Galois, since M_l is the splitting field of $x^{r_j} - \sigma_l(a_j)$ over M_{l-1}. But since $a_j \in L_{j-1}$, $\sigma_l(a_j) \in L_{j-1}$ for all l by the extension lemma. Thus $\mathrm{Gal}(M_l/M_{l-1})$ is solvable by the previous proposition. Since this holds for all l, $\mathrm{Gal}(M_{l-1}/M_{l-2})$ is also solvable.

Thus $\mathrm{Gal}\left(M_l/M_{l-2}\right) \simeq \dfrac{\mathrm{Gal}\left(M_l/M_{l-1}\right)}{\mathrm{Gal}\left(M_{l-1}/M_{l-2}\right)}$ is solvable. Continuing in this manner, $\mathrm{Gal}\left(M_r/M_0\right) = \mathrm{Gal}\left(L_j/L_{j-1}\right)$ is solvable. This is true for all j, so $\mathrm{Gal}\left(L_n/L_0\right) = \mathrm{Gal}\left(L/k\right)$ is solvable. Now $E \subseteq L$, so $\mathrm{Gal}(E/k) \leq \mathrm{Gal}(L/k)$. Thus $\mathrm{Gal}(E/k)$ is solvable.

Comment: The converse of this theorem is also true, but it requires cohomology.

Corollary: There are polynomials in $\mathbb{Q}[x]$ that are not solvable by radicals.

Proof: Let $p(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. We will show that p cannot be solved by radicals.

First, p is irreducible by Eisenstein's criterion. Let E be the splitting field of p and $G = \mathrm{Gal}(E/\mathbb{Q})$. Then E is Galois, since $\mathbb{Q}$ is perfect, so $[E : \mathbb{Q}] = |G|$. Since the roots of p have order 5, $5 \;\big|\; |G|$. By the intermediate value theorem, three roots of p are real and two are complex. The action of conjugation gives $(12) \in G$, and by Cauchy's theorem, G contains a 5-cycle. Thus $G = S_5$, but $S_5' = A_5$, since S_5' can only contain even elements and is normal in S_5, and $A_5' = A_5$, since A_5 is simple and nonabelian. Thus $x^5 - 4x + 2$ is not solvable by radicals.