Math 373 - Algebraic Structures

Based on lectures by Boris Bukh

Notes taken by Kadin Zhang

Fall 2023

Contents

1 Group Basics

1.1 Definitions and examples

A group by definition is a set of elements associated with some binary operation on these elements satisfying some properties. But a more insightful way to conceptualize elements within a group is as transformations that intrinsically compose.

The prototypical examples are the additive group of real numbers and the multiplicative group of positive real numbers. Under the additive group, real numbers are translations of the number line. We can compose any two translations together to form another translation represented by the sum of their numbers. Under the multiplicative group, real numbers are dialations on the number line centered about 0, represented by where 1 ends up on the original number line. Here, the composition of two stretches is represented by the product of their numbers. The reason we don't include 0 will become clear from the formal definition.

Definition (Group): A *group* is a pair $(G, \circ)$ consisting of a set of elements G and a binary operation $\circ : G \times G \to G$ satisfying the following properties:

(i) G has an identity element 1 such that $1 \circ g = g$ for all $g \in G$.

(ii) $\circ$ is associative, i.e. $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$.

(iii) Each item $g \in G$ has an inverse $g^{-1} \in G$ such that $g \circ g^{-1} = g^{-1} \circ g = 1$.

Note that $(\mathbb{R}, \cdot)$ is not a group since 0 has no inverse. Also, notice that communativity is not a condition; we call groups satisfying communativity *abelian* and otherwise *non-abelian*.

Example: The complex numbers form an additive group $(\mathbb{C}, +)$, where numbers are translations on the complex plane, as well as a multiplicative group $(\mathbb{C} \setminus \{0\}, \times)$, where numbers are dialations centered on 0 represented by the destination of 1. Thus we can view multiplication by a complex number by a rotation by the argument and a stretch by the magnitude.

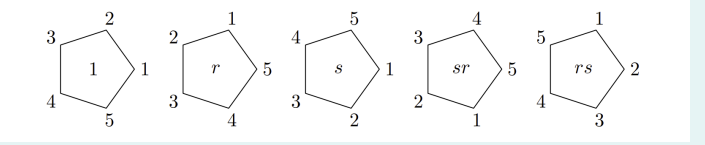
Example: The *cyclic group of order* n, denoted $\mathbb{Z}/n\mathbb{Z}$, is the group of residues modulo n under addition. The *nonzero residues modulo* p, where p is prime, is a group under multiplication which we denote $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example: The *symmetric group* S_n is the group of permutations of $\{1, \ldots, n\}$ under composition where we view each permutation as a function from $\{1, \ldots, n\}$ to itself.

Example: The *dihedral group of order* $2n$, denoted D_{2n}, is the group of rotational and reflection symmetries of a regular n-gon $A_1, \ldots, A_n$ taken as actions, consisting of the $2n$ elements

$$\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\},$$

where r is a rotation by $\frac{2\pi}{n}$ and s is a reflection about OA_1, where O is the center, and we read right to left as in function composition.



Example: Let $(G, \star), (H, *)$ be groups. We define the *product group* $(G \times H, \cdot)$ by the operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2).$$

Theorem: Suppose G is a group. Then,

(i) G contains a unique identity.

(ii) If $x \in G$, then x has a unique inverse x^{-1}.

(iii) Left multiplication is a bijection.

Proof. (iii) Suppose $gx_1 = gx_2$ for $x_1, x_2 \in G$. We left multiply both sides by g^{-1} to obtain $x_1 = x_2$. And for any $y \in G$, $gx = y$ has solution $x = g^{-1}y$. □

Definition (Subgroup): Let $G = (G, \star)$ be a group. A group $H = (H, \star)$ is a *subgroup* of G if H is a subset of G.

Example (Subgroups of $\mathbb{Z}$): Every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, where $n\mathbb{Z} \coloneqq \{nm : m \in \mathbb{Z}\}$.

Proof. Let H be a subgroup of $\mathbb{Z}$. So $0 \in H$. If H contains nothing else, $H = 0\mathbb{Z}$. Otherwise, let x be the other element in H with smallest absolute value $n = |x|$. It is clear that $n\mathbb{Z} \subseteq H$. For the other direction, suppose that $y \in H$, $y \neq nm$ for some $m \in \mathbb{Z}$. But then $y = qn + r$, where $0 < r < n \in H$, a contradiction to n being the smallest. □

Example (Trivial subgroups): All groups have both $\{1_G\}$ and G as subgroups.

Example (Dihedral group is subgroup of general linear group): Define the *general linear group* as

$$GL_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0 \right\}$$

endowed with the usual matrix multiplication. Then the dihedral group D_{2n} is a subgroup, where we let for $\theta = \frac{2\pi}{n}$,

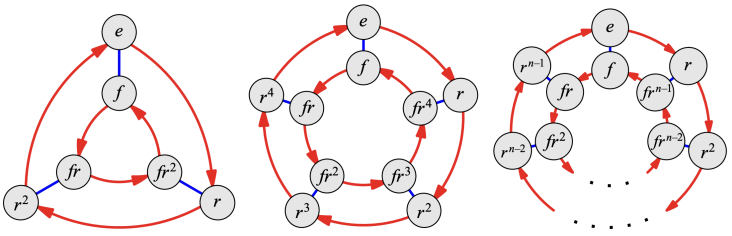
$$r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Example (Rotations are subgroup of dihedral group):

$$\{e, r, r^2, \ldots, r^{n-1}\}$$

is a subgroup of D_{2n}.

1.2 Cayley diagrams



1.3 Cyclic group

Definition (Cyclic group): A group G is *cyclic* if there exists $g \in G$ (called the *generator*) such that

$$G = \{g^n : n \in \mathbb{Z}\}.$$

Example:

(a) $1, -1$ are generators for $\mathbb{Z}$.

(b) Nonzero elements are generators for $\mathbb{Z}/p\mathbb{Z}$.

Definition (Cyclic subgroup generated by an element): Let x be an element of group G. We define the cyclic subgroup generated by x as

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\},$$

or if G is abelian and we use notation $+$,

$$\langle x \rangle = \{\dots, -2x, -x, 1, x, 2x, \dots\}.$$

The identity comes from g^0, associativity comes from the original group, and $(g^n)^{-1} = g^{-n}$.

1.4 Symmetric group

Definition (Symmetric group): Let X be a set. The *symmetric group on* X is the set of all bijections $X \to X$ with composition as the operation. We denote the symmetric group on $[n]$ with S_n.

Definition (Cycle): A cycle in a symmetric group on elements $(a_1, \dots, a_n)$ is a permuation of the form,

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_k \mapsto a_1,$$

where $k \leq n$ and the remaining $x \in X$ are mapped to themselves.

Example (Composing cycles):

$$(a_1, a_2, \dots, a_k)^2 = \begin{cases} (a_1, a_3, \dots, a_k, 2, \dots, a_{k-1}), & \text{if } k \text{ is odd;} \\ (a_1, a_3, \dots, a_{k-1})(a_2, a_4, \dots, a_k), & \text{otherwise.} \end{cases}$$

If an element i is ommitted from this notation we assume $s(i) = i$.

Proposition 1: If π, σ are two disjoint cycles (they permute disjoint sets), then they commute.

Proof. Easy. □

Theorem: Every permutation in S_n is a product of disjoint cycles.

Proof. We induct on n. $n = 1$ is trivial. Now suppose the theorem holds for $n - 1$. Suppose $s \in S_n$. If $s(n) = n$, we may invoke the $n - 1$ case easily. If $s(n) = k$ for $k \neq n$, consider the permutation

$$t = (n, k) \circ s,$$

such that $t(n) = n$. Now t can be viewed as a permutation in S_{n-1}, so we apply the induction hypothesis to obtain disjoint cycles

$$t = c_1 c_2 \dots c_r.$$

Now, we may write s again as

$$s = (n, k)c_1 \dots c_r.$$

If k is not included in t (i.e. (n, k) is a disjoint cycle in s), we're done. Otherwise, assume by communativity of disjoint cycles that $c_1 = (k, a_1, \dots, a_m)$. Then

$$s = (n, k, a_1, \dots, a_m)c_2 \dots c_r.$$

□

Definition (Order of element): Let $g \in G$. The *order* of g is $|\langle g \rangle|$.

1.5 Homomorphisms and isomorphisms

Prototypical example: linear maps $\mathbb{R}^n \to \mathbb{R}^m$.

Definition (Homomorphism): A function $f : G \to H$ is a *homomorphism* if for all $x, y \in G$,

$$f(xy) = f(x)f(y).$$

Definition (Isomorphism): A homomorphism is further called an *isomorphism* if it is a bijection.

Example (Homomorphisms):

(a) Modding out:
$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}; x \mapsto x \mod n.$$

(b) Determinant:
$$\det : GL_2(\mathbb{R}) \to (\mathbb{R} \setminus \{0\}, \cdot).$$

(c) Exponentiation:
$$\exp : (\mathbb{R}, +) \to (\mathbb{R}_+, \cdot).$$

(d) Linear maps $\mathbb{R}^n \to \mathbb{R}^m$.

(e) Trivial homomorphism $\phi(G) = 1_H$.

Example (Isomorphisms):

(a) Cyclic groups G, H of the same order are isomorphic. Let $G = \langle g \rangle, H = \langle h \rangle$. If $|G| = |H| = n < \infty$, then define the isomorphism by the map $g^i \mapsto h^i$.

Theorem (Basic properties of homomorphisms): Let $\varphi : G \to H$ be a homomorphism, then

(a) $\varphi(1_G) = 1_H$.

(b) $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Proof.

(a) $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. Left multiply by $\varphi(1_G)^{-1}$.

(b) $\varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = 1_H$.

□

Theorem (Basic properties of isomorphisms): If $\varphi : G \to H$ is an isomorphism, then $\varphi^{-1} : H \to G$ is an isomorphism.

Proof. Let $x, y \in H$. Then

$$\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y) \iff \varphi(\varphi^{-1}(xy)) = \varphi(\varphi^{-1}(x)\varphi^{-1}(y)) \iff xy = xy.$$

□

Example (Heisenberg group): Consider the group of matrices

$$H(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{R} \right\},$$

under usual matrix multiplication. We can confirm that the group is closed under multiplication, we have an identity I_3, and these matrices are invertible.

There is a homomorphism $\phi : H(\mathbb{R}) \to \mathbb{R}^2$ by $A \to (x, y)$, since

$$\phi(A_1 A_2) = \phi \begin{pmatrix} 1 & x_1 + x_2 & z_1 + z_2 + x_1 y_2 \\ 0 & 1 & y_1 + y_2 \\ 0 & 0 & 1 \end{pmatrix} = \phi(A_1)\phi(A_2).$$

Definition (Conjugation): Let G be a group and $h \in G$. The *conjugate* of an element $g \in G$ by h is

$$hgh^{-1}.$$

Theorem (Conjugate map is isomorphism): The map $\varphi_h : G \to G$ defined by

$$g \mapsto hgh^{-1}$$

is an isomorphism.

Proof.

(a) $\varphi_h(xy) = hxyh^{-1} = (hxh^{-1})(hyh^{-1}) = \varphi_h(x)\varphi_h(y)$.

(b) φ_h is a bijection since we can define φ_h^{-1} through $g \mapsto h^{-1}gh$.

□

Remark: More generally,

$$(\varphi_h\varphi_k)(g) = (hk)g(hk)^{-1} = \varphi_{hk}(g).$$

Example (Conjugate maps):

(a) If G is abelian, φ_h is the identity map.

(b) If $G = GL_2(\mathbb{R})$, $B^{-1}AB$ maps transformations to different bases.

(c) If $G = S_n$,

$$\pi \coloneqq \sigma(a_1, \ldots, a_t)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_t)),$$

since $\pi(\sigma(a_1)) = \sigma(a_2)$, etc.

Proposition 2 (Symmetric groups of same order isomorphic): If $|A| = |B|$ we can define a bijection $f : B \to A$, then define $\phi : S_A \to S_B$ by

$$\sigma \mapsto (x \mapsto \sigma(f(x))).$$

1.6 Cosets

Definition (Coset): Suppose $H \leq G$, and $g \in G$. Then

$$gH \coloneqq \{gh : h \in H\},$$

and this is called the *left coset* of H containing g.

Example (Cosets):

(a) Let $G = \mathbb{Z}$, $H = n\mathbb{Z}$. The cosets of H are the equivalence classes modulo n.

(b) Let $G = D_{2n}$, $H = \{1, r, \ldots, r^{n-1}\}$. The cosets of H are H and $fH = \{f, fr, \ldots, fr^{n-1}\}$.

(c) Let $G = \mathbb{R} \times \mathbb{R}$. Consider $H = \{0\} \times \mathbb{R}$. The cosets of H are the vertical lines.

Proposition 3: Let $H \leq G$. Then the left cosets of H form a partition of G.

Proof. Let $g_1, g_2 \in G$. Suppose $g_1H \cap g_2H \neq \varnothing$. We would like to show $g_1H = g_2H$. So let $x \in g_1H \cap g_2H$, meaning there exists h_1, h_2 such that $g_1h_1 = g_2h_2 \implies g_1 = g_2h_2h_1^{-1}$.

Let $g_1h \in g_1H$. Then

$$g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \in g_2H.$$

The other containment is similar. □

Proposition 4:

(a) Let $H \leq G$. Then $g_1H = g_2H$ if and only if $g_1^{-1}g_2 \in H$.

(b) The number of left and right cosets are equal.

Proof.

(a) Note that left multiplication by a member of a group is a bijection. So we have a chain of if and only ifs:

$$g_1H = g_2H \iff H = g_1^{-1}g_2H \iff g_1^{-1}g_2 \in H.$$

(b) We can define the bijection between left and right cosets

$$g_1H \mapsto (g_1H)^{-1} \coloneqq \{(g_1h)^{-1} : h \in H\} = Hg_1^{-1},$$

using the fact that $\{h^{-1} : h \in H\} = H$.

□

Theorem (Lagrange's Theorem): If G is a finite group and $H \leq G$, then $|H| \mid |G|$.

Proof. It suffices to show that for all $g \in G$, $|gH| = |H|$. Consider the map ϕ defined by $h \mapsto gh$. This is a bijection since we have inverse $x \mapsto g^{-1}x$. □

Definition (Index of H in G): $[G : H]$ denotes the number of left cosets of H in G.

Corollary: If $g \in G$, then $|g| \mid |G|$, since $|g| = |\langle g \rangle|$.

Corollary: If G is a group, with $|G| = p$ for some prime p, then G is cyclic.

Proof. Pick $g \in G \setminus \{1_G\}$. Then $|g| \mid |G| = p$. But then $|g| = 1$ or $|g| = p$. Since g is not the identity, it must be that $|g| = p$. □

Example ($(\mathbb{Z}/n\mathbb{Z})^*$): Consists of $a \in \{0, 1, \ldots, n-1\}$ such that $\gcd(a, n) = 1$ with operation

$$ab = (ab) \mod n.$$

This is a group, since

(a) Associativity of multiplication modulo n.

(b) Identity 1.

(c) Existence of multiplicative inverses by Euclidean algorithm: suppose $\gcd(a, n) = 1$, then there exists c, d such that

$$ca + dn = 1 \implies ca \equiv 1 \pmod{n}.$$

Theorem (Euclidean algorithm): Let $m, n \in \mathbb{Z}$. There exists $c, d \in \mathbb{Z}$ such that

$$cm + dn = \gcd(m, n).$$

Proof. WLOG $m, n \geq 0$. We induct on $m + n$. Base case is easy. Now suppose $n \leq m$. We write

$$m = qn + r,$$

where $r < n$. Then, by inductive hypothesis,

$$\gcd(m, n) = \gcd(r, n) = cr + dn.$$

Plugging back in $r = m - qn$,

$$\gcd(m, n) = c(m - qn) + dn = cm + (d - cq)n.$$

□

Theorem (Fermat's Little Theorem):

$$a^p \equiv a \pmod{p}.$$

Proof. By Lagrange, $|a| \mid |(\mathbb{Z}/n\mathbb{Z})^*|$, thus

$$|a| \mid p - 1 \implies a^{p-1} \equiv 1 \pmod{p} \implies a^p \equiv a \pmod{p}.$$

Since this works for $a = 0$, and for equivalences $\mod p$, this is true for all $a \in \mathbb{Z}$. □

1.7 Subgroups generated by subsets

Suppose we wanted to show $\{1, r^2, f, fr^2\} \trianglelefteq D_8$. If we call the LHS B, we normally need to show that conjugation of all elements in B stays in B. But it turns out that it suffices to show $rBr^{-1} \subseteq B$ and $fbf^{-1} \subseteq B$.

Definition (Subgroup generated by subset): Let G be a group, $S \subseteq G$ a subset. Then the subgroup generated by S in G, dentoed $\langle S \rangle$, is the smallest subgroup of G containing S:

$$\langle S \rangle = \bigcap_{H \leq G : S \subseteq H} H.$$

Note that this is well-defined since the intersection of subgroups is a subgroup (easy to verify closure, identity, inverse).

Definition ($\overline{S}$): Let $S \subseteq G$. Then,

$$\overline{S} = \{\text{finite products of elements in } S \text{ and their inverses}\}.$$

Proposition 5: $\overline{S} = \langle S \rangle$.

Proof. Clearly the inverses of elements in S are included in $\langle S \rangle$, so finite products of elements and their inverses must also be in $\langle S \rangle$.

For the other containment we show $\overline{S}$ is a subgroup containing S, which shows it contains $\langle S \rangle$. This is easy: the product of two finite products is a finite product, the inverse of a finite product is a finite product, the identity is a (trivial) finite product, and each element of S is a finite product. □

1.8 Normal subgroups and quotients

Definition (Normal subgroup): A subgroup N of G is *normal* if for all $g \in G$,

$$gN = Ng.$$

Equivalently, for all $g \in G$,

$$N = g^{-1}Ng.$$

We motivate this definition by the desire for the cosets of H to be a group.

Proposition 6 (Generating condition for normal subgroup): Let $a_1, \ldots, a_k$ generate G and $H \leq G$. Then $H \trianglelefteq G$ if

$$a_i H a_i^{-1} = H$$

for all $i = 1, \ldots, k$.

Proof. Let $g \in G$. Then $g = x_1 \ldots x_n$ where $x_i \in \{a_j, a_j^{-1} : j = 1, \ldots, k\}$. So

$$gHg^{-1} = x_1 \ldots x_n H x_n^{-1} \ldots x_1 = H,$$

after we show $a_i^{-1} H a_i = H$. Indeed, this is true since multiplication is a bijection. □

Proposition 7 (Containment condition for normal subgroup): Let $N \leq G$. If for all $g \in G$,

$$gNg^{-1} \subseteq N,$$

then N is normal in G.

Proof. Fix g. We apply hypothesis to g^{-1}:

$$g^{-1}N(g^{-1})^{-1} \subseteq N \implies g^{-1}Ng \subseteq N.$$

Since left multiplication and right multiplication are bijections,

$$N \subseteq gNg^{-1}.$$

Thus $gNg^{-1} = N$ for all g and N is normal as required. □

Definition (Quotient group): Suppose N is a normal subgroup of G. The *quotient* of G by N, denoted G/N, is

$$G/N = \{gN : g \in G\}$$

with the operation

$$(g_1N) \cdot_{G/N} (g_2N) = \{xy : x \in g_1N, y \in g_2N\} =: (g_1N)(g_2N).$$

Equivalently, the RHS is $\{(g_1n_1)(g_2n_2) : n_1, n_2 \in N\}$, so we obtain

$$g_1Ng_2N = g_1(Ng_2)N = g_1(g_2N)N = (g_1g_2)N.$$

Proposition 8: If $H \leq G$ and $[G : H] = 2$ with $|G| < \infty$, H is normal in G.

Proof. Since the index is 2, the cosets are H and $G \setminus H$. If $g \in H$, $gH = H = Hg$. If $g \notin H$,

$$gH = H \setminus G = Hg.$$

□

Example (Normal subgroups):

(a) $n\mathbb{Z}$ is normal in $\mathbb{Z}$, since $\mathbb{Z}$ is abelian. The elements in $\mathbb{Z}/n\mathbb{Z}$ are $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}$.

(b) $H = \{1, r, r^2, \ldots, r^{n-1}\}$ is normal in D_{2n}, since $\{r, f\}$ generate D_{2n} and clearly $rHr^{-1} = H$ and $fHf^{-1} = H$.

(c) Suppose K, L are groups. Let $G = K \times L$, and $H = \{1\} \times L$. H is normal in $K \times L$.

Example (Normality of subgroups isn't transitive): Consider $A \coloneqq \{1, f\} \leq B \coloneqq \{1, r^2, f, fr^2\} \leq D_8$. A is normal in B by previous proposition since $[B : A] = 2$. B is normal in D_8 by the same logic. However A is not normal in D_8!

Definition (Kernel): If $\varphi : G \to H$ is a homomorphism, then the *kernel* of φ is

$$\ker \varphi = \{g \in G : \varphi(g) = 1\}.$$

Proposition 9 (Kernel is normal subgroup): Let $\varphi : G \to H$ be a homomorphism. $\ker \varphi$ is a normal subgroup of G.

Proof. First, $\ker \varphi$ is a subgroup, since

(a) $1 \in \ker \varphi$, since $\varphi(1) = 1$.

(b) $\varphi(g_1) = 1, \varphi(g_2) = 1 \implies \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 1$.

(c) If $g \in \ker \varphi$, then $\varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(g^{-1}) = 1$, so $g^{-1} \in \ker \varphi$.

Let $g \in G$. Define $K = \ker \varphi$. Let $k \in K$.

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(1) = 1.$$

Thus $gkg^{-1} \in K$, and K is a normal subgroup of G by above proposition. □

Example (Special linear group): Consider $\det : GL_2(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$. Then, define the *special linear group* as

$$SL_2(\mathbb{R}) \coloneqq \ker \det = \{M : \det M = 1\}.$$

Proposition 10: Suppose $\phi : G \to H$ is a homomorphism and $\ker \phi = 1$ ($\{1\}$). Then $\phi(G)$ is isomorphic to G, i.e. $\phi(G) \cong G$.

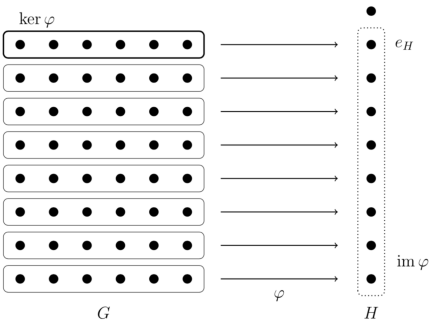
Proof. We show ϕ is isomorphism between G and $\phi(G)$. ϕ is always surjective. Suppose $\ker \phi = 1$. Choose $g_1, g_2 \in G$.

$$\phi(g_1) = \phi(g_2) \implies \phi(g_1)\phi(g_2^{-1}) = 1 \implies \phi(g_1 g_2^{-1}) = 1.$$

Then, $g_1 g_2^{-1} = 1 \implies g_1 = g_2$. □

Example: Let $T : \mathbb{R}^n \to \mathbb{R}^m$ be linear. Then if $\ker T = N(T) = \{0\}$, the image of T is a n-dimensional subspace of $\mathbb{R}^m$.

Intuitively, cosets of the kernel partition the group into sets mapping into the same element in the codomain:



Theorem (First isomorphism theorem): Let $\phi : G \to H$ be a homomorphism. Then

$$\phi(G) \cong G/\ker \phi.$$

Proof. Define $N = \ker \phi$. We want a map $f : G/N \to \phi(G)$. Following the diagram, we choose

$$gN \mapsto \phi(g).$$

We need to check this is invariant on coset representative, i.e. if $g_1 N = g_2 N$, then

$$\phi(g_1) = \phi(g_2).$$

If $g_1 N = g_2 N$, then $N = g_1^{-1} g_2 N \implies g_1^{-1} g_2 \in N$. So $\phi(g_1^{-1} g_2) = 1 \implies \phi(g_1) = \phi(g_2)$ as required.

First we show f is surjective. Let $h \in \phi(G)$. Then $h = \phi(g)$ for some $g \in G$. So $gN \in G \setminus N$ maps to $\phi(g)$. For injectivity assume $f(g_1 N) = f(g_2 N)$. Then,

$$\phi(g_1) = \phi(g_2) \implies \phi(g_1 g_2^{-1}) = 1 \implies g_1^{-1} g_2 \in N.$$

Thus $g_1 N = g_2 N$. □

Definition (Natural projection): Let $N \trianglelefteq G$. Then the map from G to G/N is called the *natural projection*.

Example: Let π be the natural projection from G to G/N. Then, $\ker \pi = N$.

2 Group action

2.1 Definitions and examples

Definition (Group action): Let G be a group and X be a set. Then an *action* of G on X is of the form $\cdot : G \times X \to X$, such that

(a) For every $g \in G$, $x \mapsto g \cdot x$ is a bijection.

(b) If $g_1, g_2 \in G$, $x \in X$,
$$g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x.$$

Example (Group actions):

(a) $G = D_{2n}$ (transformations on n-gon). Let X be the vertices of the n-gon. Then G acts on X by
$$g \cdot x = g(x),$$
i.e. where does vertex end up after transformation?

(b) S_X acts on X by
$$\pi \cdot x = \pi(x).$$

(c) $GL_2(\mathbb{R})$ acts on $\mathbb{R}^2$ by
$$M \cdot v = Mv.$$

(d) $G = S_Y$ and $X = \mathcal{P}(Y)$. S_Y acts on $\mathcal{P}(Y)$ by image:
$$\sigma \cdot Z = \sigma(Z).$$

(e) S_Y acts on $\binom{Y}{k} \coloneqq \{Z : Z \subseteq Y : |Z| = k\}$ by the same as above.

(f) Trivial action for any G, X by
$$g \cdot x = x.$$

Theorem (Group actions as homomorphisms): We can define an action of G on the group X through
$$g \cdot x = (\phi(g))(x),$$
where ϕ is a homomorphism $G \to S_X$.

Proof. We satisfy (a) since permutations are bijections. For (b),

$$\begin{aligned} g_1 \cdot (g_2 \cdot x) &= g_1 \cdot (\phi(g_2)(x)) \\ &= \phi(g_1)(\phi(g_2)(x)) \\ &= (\phi(g_1)\phi(g_2))(x) \\ &= (\phi(g_1 g_2))(x) \\ &= (g_1 \cdot g_2) \cdot x \end{aligned}$$

Conversely, given an action $\cdot : G \times X \to X$, define $\phi : G \to S_X$ by

$$g \mapsto (x \mapsto g \cdot x).$$

□

Definition (Kernel of group action): The kernel of a group action is the kernel of the homomorphism representation, i.e. elements g where $x \mapsto g \cdot x$ is the identity.

Theorem (Cayley's Theorem): Every group is isomorphic to a subgroup of a symmetric group.

Proof. Consider the following action of G on itself by left multiplication, i.e.

$$g \cdot h = gh.$$

Let $\phi : G \to S_G$ be the corresponding homomorphism. Consider $\ker \phi$, the elements mapping to the identity permutation, in other words g such that $g \cdot x = gx = x$ for all x. This can only be the identity 1_G, meaning the kernel is trivial. By the first isomorphism theorem,

$$\phi(G) \cong G/\{1_G\} = G.$$

Thus G is isomorphic to a subgroup of S_G, $\phi(G)$. □

Corollary: Let G finite group of order n, p be the smallest prime dividing n. If $|G : H| = p$, then H is normal.

Proof. Let $|G : H| = p$. Let X be the left cosets of H, and let G act on X by left multiplication. Let $\phi : G \to S_X$ denote this action. Then,

$$|\operatorname{im} \phi| \leq p!.$$

But since $|\operatorname{im} \phi|$ divides n and p is the smallest prime dividing n, $|\operatorname{im} \phi| \leq p$. So by first isomorphism,

$$|\ker \phi| \geq \frac{n}{p} \implies \ker \phi = H \trianglelefteq G.$$

□

Example (Actions of groups on themselves):

(a) Left multiplication $g \cdot h = gh$.

(b) Right multiplication $g \cdot h = hg$ is not a group action, since typically

$$h(g_1 g_2) \neq (hg_2)g_1.$$

Instead, define $g \cdot h = hg^{-1}$, then

$$h(g_1 g_2)^{-1} = (hg_2^{-1})g_1^{-1}.$$

(c) Conjugation,

$$g \cdot h = ghg^{-1}.$$

2.2 Orbits

Definition (Orbit): Suppose G acts on X. Then the orbit of $x \in X$ is

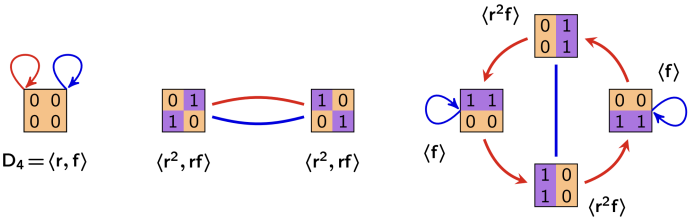
$$G \cdot x = \{g \cdot x : g \in G\}.$$

Consider $G = \mathbb{R}$, $X = \mathbb{R}^2$. Let $t \cdot v$ be the rotation of v by t. Then the orbits of vectors are rings.

Suppose our set X is the set of 7 binary squares

$$S = \left\{ \begin{smallmatrix} 0&0\\0&0 \end{smallmatrix}, \begin{smallmatrix} 0&1\\1&0 \end{smallmatrix}, \begin{smallmatrix} 1&0\\0&1 \end{smallmatrix}, \begin{smallmatrix} 1&1\\0&0 \end{smallmatrix}, \begin{smallmatrix} 0&1\\0&1 \end{smallmatrix}, \begin{smallmatrix} 0&0\\1&1 \end{smallmatrix}, \begin{smallmatrix} 1&0\\1&0 \end{smallmatrix} \right\}$$

Here is how D_4 acts on X. Note that each connected component is an orbit. The stabilizers of each binary square are labeled.



Proposition 11 (Orbits partition): Suppose $(G \cdot x) \cap (G \cdot y) \neq \varnothing$. Then

$$g_1 \cdot x = z = g_2 \cdot y,$$

for some $z \in X, g_1, g_2 \in G$. Then

$$x = (g_1^{-1} g_2) \cdot y.$$

So for any $g \in G$, $g \cdot x$ will be in $G \cdot y$. Similarly we can show the other containment, and then $G \cdot y = G \cdot x$.

Corollary: Let $H \leq G$. The left cosets of H in G form a partition.

Proof. Define the action of H on G by

$$h \cdot g = gh^{-1}.$$

Then the orbit of $g \in G$ by H is

$$H \cdot g = \{h \cdot g : h \in H\} = \{gh^{-1} : h \in H\} = gH.$$

□

Example: Let S_n act on itself by conjugation:

$$\pi \cdot \sigma = \pi\sigma\pi^{-1}.$$

Then, if σ is a t-cycle $(a_1, \ldots, a_t)$, the orbit of σ by S_n is

$$G \cdot \sigma = \{\pi(a_1, \ldots, a_t)\pi^{-1} : \pi \in S_n\} = \{(\pi(a_1), \ldots, \pi(a_t)) : \pi \in S_n\},$$

which is all t-cycles in S_n. Moreover, if σ is the composition of cycles, $\sigma = (a_1, a_2)(a_3, a_4)$, then

$$\pi\sigma\pi^{-1} = \pi(a_1, a_2)\pi^{-1}\pi(a_3, a_4)\pi^{-1} = (\pi(a_1), \pi(a_2))(\pi(a_3), \pi(a_4)).$$

Definition (Stabilizer): Let $x \in X$. The stabilizer of x under action G is

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

Theorem (Orbit stabilizer theorem):

(a) $G_x \leq G$.

(b) $|G \cdot x| = |G : G_x|$.

Proof.

(a) Let $g_1, g_2 \in G_x$. $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = g_1 \cdot x = x$, so $g_1g_2 \in G_x$. $\phi(e) = \mathrm{id}_X$, so $e \in G_x$. Then if $g \in G_x$, $e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot x = x$, so $g^{-1} \in G_x$. Thus $G_x \leq G$.

(b) We establish a bijection between $G \cdot x$ and $\{gG_x : g \in G\}$. Define f by $g \cdot x \mapsto gG_x$ so that f^{-1} maps $gG_x \mapsto g \cdot x$. We show $g_1 \cdot x = g_2 \cdot x$ if and only if $g_1G_x = g_2G_x$ showing they are both injections.

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\iff x = g_1^{-1} \cdot (g_2 \cdot x) && \text{(Left action)} \\ &\iff x = (g_1^{-1}g_2) \cdot x \\ &\iff g_1^{-1}g_2 \in G_x \\ &\iff g_1G_x = g_2G_x. \end{aligned}$$

□

Example (Orbit stabilizer prototypical example): Consider the group of symmetries of a cube acting on the faces. Fix a face. Four symmetries (rotations of the face) leave the face alone. The face can go to all six possible faces. So the size of the stabilizer of the face times the size of its orbit is 24, the size of the group.

2.3 Alternating Group

Definition (Transposition): A *transposition* in a symmetric group is a 2-cycle.

Proposition 12 (Cycles are products of transpositions): Note that each cycle

$$(a_1, \ldots, a_n)$$

can be written as

$$(a_1, a_2)(a_2, a_3) \ldots (a_{n-1}, a_n).$$

Furthermore we can actually write them as adjacent transpositions $(k, k+1)$ since by conjugation

$$(k, k+2) = (k+1, k+2)(k, k+1)(k+1, k+2),$$

and we can show this is true for all $k + \ell$ inductively. This is a cool idea as if we can show some property of a permutation is invariant on adjacent swaps, it is invariant across all permutations (USAMO 2017).

Corollary (Permutations are products of transpositions): Each permutation is a product of disjoint cycles, and each cycle is a product of transpositions.

Definition (Sign of permutation): We denote the sign of a permutation $\pi \in S_n$, $\operatorname{sgn} : S_n \to \{1, -1\}$ by

$$\operatorname{sgn} \pi = \begin{cases} 1, & \text{if } \pi \text{ is made up of even number of transpositions;} \\ -1, & \text{otherwise.} \end{cases}$$

Proposition 13 (Sign is well-defined): Consider the easily verified action of S_n on $\mathbb{R}[x_1, \ldots, x_n]$ by

$$\pi \cdot f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}).$$

Consider the polynomial

$$\Delta = \prod_{1 \le i < j \le n} (x_j - x_i),$$

then its easy to see that $\pi \cdot \Delta = \operatorname{sgn} \pi \Delta$, which shows sgn is well defined.

Proposition 14 (Sign is homomorphism): Suppose $\pi_1, \pi_2 \in S_n$. We easily verify homomorphism by casing on signs of π_1, π_2:

(a) $\operatorname{sgn}(\pi_1) = \operatorname{sgn}(\pi_2) = 1 \implies \operatorname{sgn}(\pi_1 \circ \pi_2) = 1.$

(b) $\operatorname{sgn}(\pi_1) \neq \operatorname{sgn}(\pi_2) \implies \operatorname{sgn}(\pi_1 \circ \pi_2) = -1.$

(c) $\operatorname{sgn}(\pi_1) = \operatorname{sgn}(\pi_2) = -1 \implies \operatorname{sgn}(\pi_1 \circ \pi_2) = 1$.

Definition (Alternating group): The *alternating group* of n is the subset of permutations of S_n with even number of transpositions, i.e. $\ker \operatorname{sgn}$. It's easy to verify this is indeed a subgroup of S_n.

Definition (Simple group): A *simple group* is a group whose only normal subgroups are the trivial subgroup and itself.

Theorem (Classification of finite simple groups): Every finite simple group is one of

(a) $\mathbb{Z}/p\mathbb{Z}$ for prime p.

(b) A_n for $n \geq 5$.

(c) 3 more families, 26 more specific groups.

We will prove (b).

Proposition 15: Let $T = \{\sigma \in S_n : \sigma \text{ is 3-cycle}\}$. Then $\langle T \rangle = A_n$.

Proof. Since we can write each 3-cycle as a product of two transpositions, $\langle T \rangle \subseteq A_n$. On the other hand, given an even number of transpositions, we take them side by side and combine them into 3-cycles.

(a) If $(a, b)(c, d)$ disjoint, then replace with

$$(a, b, c)(c, d, b).$$

(b) If $(a, b)(a, b)$, get rid of both.

(c) If $(a, b)(b, c)$, replace with

$$(a, b, c).$$

□

Proposition 16: Suppose a normal subgroup N of A_n, $n \geq 5$, contains a 3-cycle. Then $N = A_n$.

Proof. Suppose N contains (a, b, c). We show it contains all 3-cycles, thus by previous proposition $N = A_n$. Let (a', b', c') be an arbitrary 3-cycle in A_n. We obtain it via conjugation $(\sigma(a), \sigma(b), \sigma(c))$ which is allowed since N is normal.

Define σ as a permutation satisfying $\sigma(a) = a', \sigma(b) = b', \sigma(c) = c'$. If $\sigma \in A_n$, we are done. Otherwise, since $n \geq 5$, there exist two elements c, d not in the original cycle. Compose the cycle (c, d) onto σ, and it is now in A_n. □

Theorem: A_n is a simple group for $n \geq 5$.

Proof. Let N be a nontrivial normal group of A_n. We show it contains a 3-cycle, thus it must be A_n. We case on its non-identity element σ in disjoint product form:

(a) σ has a cycle with length at least 4.

$\sigma = \pi(a_1, \ldots, a_r)$ with $r \geq 4$. Then

$$\sigma^{-1}(\pi(a_1, a_2, a_3)(a_1, \ldots, a_r)(a_1, a_2, a_3)^{-1}) = (a_3, a_r, a_1).$$

(b) I actually don't care

□

We use the simplicity of A_n to prove a unmotivated result about the index of subgroups of symmetric groups.

Proposition 17 (We can restrict normal subgroups): If $N \trianglelefteq G, H \leq G$, then $N \cap H \trianglelefteq H$.

Proof. Let $x \in N \cap H$ and $h \in H$. WTS $hxh^{-1} \in N \cap H$. We know it is in H by closure. It is in N by normality of N. □

Proposition 18 (Kernel of symmetric group acting on sets): Let $\pi : S_n \to S_X$ be a homomorphism of S_n acting on some set X. If $|\ker \pi| \geq 3$, then it contains an even non-identity permutation.

Proof. Since $|\ker \pi| \geq 3$, it contains two non identity elements σ_1, σ_2. If one is even, we're done. Otherwise, their product is even. □

Proposition 19 (Index of subgroups of symmetric group): Let $H \leq S_n$. Then $|S_n : H| \leq 2$ or $|S_n : H| \geq n$.

Proof. Suppose $|S_n : H| < n$. We show it is at most 2. Let S_n act on $X = \{gH : g \in S_n\}$ by left multiplication. Let $\pi : S_n \to X$ be the corresponding homomorphism. Let $N = \ker \pi$. First note that $N \leq H$:

$$\sigma \in \ker \pi \implies \sigma H = \sigma \implies \sigma \in H.$$

We show $A_n \leq N$ using simplicity of A_n and previous propositions. Since $A_n \leq S_n$,

$$N \trianglelefteq S_n \implies N \cap A_n \trianglelefteq A_n.$$

So to show $A_n \leq N \leq H$, it suffices to show $|N| \geq 3$. Indeed, by first isomorphism theorem,

$$|\operatorname{im} S_n| \leq |S_X| \leq (n-1)! \implies |\ker \pi| \geq n.$$

□

3 Subgroups

3.1 Normalizers, centralizer, center

Definition (Normalizer of subset): Let $A \subseteq G$. Define the *normalizer* of A in G as

$$N_G(A) = \{g \in G : gAg^{-1} = A\}.$$

A subset $H \subseteq G$ *normalizes* A if for all $h \in H$, $hAh^{-1} = A$, or $H \leq N_G(A)$.

Definition (Centralizer of subset): Let $A \subseteq G$. The *centralizer* of A in G is the subgroup of $N_G(A)$ defined as

$$C_G(A) = \{g \in G : gag^{-1} = a \text{ for all } a \in A\}.$$

Definition (Center of group): Define the *center* "zentrum" of a group G as

$$Z(G) = \{g \in G : gh = hg, \forall h \in G\}.$$

Note that $Z(G) = C_G(G)$, so $Z(G) \leq G$. Also note that any subgroup of $Z(G)$ is normal in G since elements in the center commute with all elements in G.

Example:

(a) When G is abelian, $Z(G) = C_G(A) = N_G(A)$ for all subsets $A \subseteq G$.

(b) Let $G = D_8$. Let $A = \{1, r, r^2, r^3\}$. $C_G(A) = A$ and $N_G(A) = G$.

Example: Let G act on $\mathcal{P}(G)$ by conjugation, i.e.

$$g \cdot A = gAg^{-1}.$$

The stabilizer of a set A is $N_G(A)$.

Let $N_G(A)$ act on A by conjugation:

$$g \cdot a = gag^{-1}.$$

Then the kernel of this action is $C_G(A)$.

Finally, $Z(G)$ is the kernel of the action of G on itself by conjugation.

4 Sylow's theorems

4.1 p-groups

As motivation we would like to know when its true that a group G has a subgroup of a given order dividing $|G|$. Unfortunately this isn't always true:

Example (Converse of Lagrange's theorem isn't true): If $d \mid |G|$ and $|G| < \infty$, it isn't necessarily true there's a subgroup with order d. However if d is prime, then we can find an element of order d.

However we can show the converse of Lagrange is true for groups with orders that are powers of primes.

Definition (Finite p-group): For a prime p, a *finite p-group* is a group whose order is p^n for some $n \geq 1$.

Proposition 20 (p-group has nontrivial center):

Proof. Consider the action of G on itself by conjugation, $g \cdot h = ghg^{-1}$. Let $h \in G$ and consider its orbit by G. By orbit stabilizer,

$$|G \cdot h| = |G : G_h| = |G : N_G(h)|,$$

so $|G \cdot h|$ is a power of p. Moreover, it is 1 if and only if $N_G(h) = G$, i.e. $h \in Z(G)$. So we can partition G into orbits with more than one element, $O_1, \ldots, O_k$, and $Z(G)$:

$$G = O_1 \cup \cdots \cup O_k \cup Z(G).$$

Thus since $p \mid |G|$ and $p \mid |O_i|$, $p \mid |Z(G)|$. □

Theorem (Converse of Lagrange for p-groups): If $|G| = p^n$, then G contains a subgroup of order p^m for all $m = 0, \ldots, n$.

Proof. We induct on m. If $m = 0$, then G has the trivial subgroup. Suppose $m > 0$. We use nontrivality of $Z(G)$ to find a normal subgroup of G of order p. Indeed, since $|Z(G)|$ is a positive power of p we can find a subgroup with order p normal in G, call it N. Let $G' = G/N$, so

$$|G'| = \frac{|G|}{|N|} = p^{m-1}.$$

By induction G' contains a subgroup H' of order p^{m-1}. Let $H = \pi^{-1}(H')$ given natural projection $\pi : G \to G/N$. This is the preimage of a subgroup in G' under homomorphism, which is a subgroup in G (easy to show). And

$$|H| = |N||H'| = p|H'| = p^m.$$

□

4.2 Sylow's theorem I

Definition (Fixed point of group action): If G acts on a set X, a *fixed point* of X is a point x satisfying

$$g \cdot x = x, \forall g \in G.$$

Definition: If $|G| = p^n m$ where p does not divide m, then a subgroup $P \subseteq G$ is called a *Sylow p-subgroup* if

$$|P| = p^n.$$

We present the Sylow theorems, which expand our theory for existence of subgroups of certain orders.

Theorem (Sylow's theorems):

(a) Every finite group contains a Sylow p-subgroup.

(b) The number of Sylow p-subgroups is congruent to 1 modulo p.

(c) Sylow p-subgroups are conjugate, i.e. for Sylow p-subgroups P, P', there exists $g \in G$ such that

$$P = gP'g^{-1}.$$

Furthermore every p-subgroup is contained in some Sylow p-subgroup.

We will later see that theorem I implies theorems II and III. We prove theorem I with the help of two lemmas.

Lemma (1): Let G be a finite group, p a prime. The following are equivalent:

(a) G has a Sylow p-subgroup.

(b) There exists an action of G on a finite set X satisfying:

  (a) $|X|$ is not divisible by p.

  (b) $\forall x \in X$, G_x is a p-group.

  (c) There is only one orbit. (action is "transitive")

Proof. Let P be a Sylow p-subgroup of G. Let X be the left cosets of P. Suppose G acts on X by left multiplication as usual.

(a) $|X| = m$, which p does not divide.

(b) Let $y \in X$. Then

$$G_y = \{h \in G : h \cdot y = y\}\{h \in G : h \cdot (g \cdot x) = g \cdot x\}$$

Suppose G acts on X as in (b). By orbit stabilizer, for any $x \in X$,

$$|G : G_x| = |G \cdot x| = |X|,$$

which is not divisible by p. Thus p does not divide

$$\frac{|G|}{|G_x|} = \frac{p^n m}{|G_x|},$$

thus since G_x is a p-group, it must be that $|G_x| = p^n$, a Sylow p-subgroup of G. □

Lemma (2): If G has a Sylow p-subgroup and $H \leq G$, then H also has a Sylow p-subgroup.

Proof. Suppose G acts on some set X as in Lemma 1b. We first show (a) and (b) hold when we restrict to the action of H on X, then restrict X to a single orbit of X under H to satisfy (c).

(a) X is the same.

(b) Let $x \in X$. Then

$$H_x = \{h \in H : h \cdot x = x\} = G_x \cap H \leq G_x.$$

Thus by Lagrange $|H_x| \mid |G_x|$, so H_x is also a p-group.

(c) Let $O_1, \ldots, O_k$ be the orbits of X under H so that $|O_1| + \cdots + |O_k| = |X|$. Since p does not divide $|X|$, there is some orbit O_1 such that p does not divide $|O_1|$. Restrict the action of H on X to the action of H on O_1, and all properties (a), (b), and (c) are satisfied.

□

Definition (field): A *field* is a triple $(F, +, \cdot)$ where

(a) F is a set, $+, \cdot$ are binary operations on F.

(b) $(F, +)$ is an abelian group.

(c) $\cdot$ is associative and communative.

(d) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

(e) For every $d \neq 0$, $d \in F$, there is an element d^{-1} such that $d^{-1}d = dd^{-1} = 1$, where 1 is the multiplicative identity.

(f) $0 \neq 1$.

In particular, $(F \setminus \{0\}, \cdot)$ is an abelian group.

The field we will use is $\mathbb{F}_p$, which is $\mathbb{Z}/p\mathbb{Z}$ with the usual modular addition and multiplication.

Theorem (Sylow's theorem I): Every finite group contains a Sylow p-subgroup.

Proof. Since by Cayley's theorem every group is isomorphic to a subgroup of some S_n, to show G has a Sylow p-subgroup it suffices show S_n has a Sylow p-subgroup for all n. We further embed S_n as a subgroup of $GL_n(\mathbb{F}_p)$ so that it suffices to show $GL_n(\mathbb{F}_p)$ has a Sylow p-subgroup:

$$G \leq S_n \leq GL_n(\mathbb{F}_p).$$

In particular, for a given permutation π, we define the injective homomorphism $\phi : S_n \to GL_n(\mathbb{F}_p)$ by

$$\phi : \pi \to A, A_{ij} = \begin{cases} 1, & \text{if } \pi(i) = j; \\ 0, & \text{otherwise.} \end{cases}.$$

Note that $\det A = \pm 1$ since we can swap rows until we get the identity matrix. □

Example (Easy cases): Let $|S_p| = 1 \cdot 2 \cdot \cdots \cdot p$. A subgroup of order p is

$$\langle (1, 2, \ldots, p) \rangle.$$

Let $|S_{2p}| = 1 \cdot 2 \cdot \cdots \cdot 2p$. A subgroup of order p^2 is

$$\langle (1, 2, \ldots, p), (p+1, p+2, \ldots, 2p) \rangle.$$

This generalizes to subgroups of order np. Now let $|S_{p^2}|$. Let $\alpha_1, \ldots \alpha_p$ be the p disjoint cycles of size p as above. These will generate a subgroup of order p^p rather than p^{p+1}. Let β be the map $x \mapsto x + p$. Then $|\langle \alpha_1, \ldots, \alpha_p, \beta \rangle| = p^{p+1}$.

Proposition 21 (Concluding Sylow I): $GL_n(\mathbb{F}_p)$ has a Sylow p-subgroup

Proof. First we find the order of $GL_n(\mathbb{F}_p)$. Note that

$$GL_n(\mathbb{F}_p) = \{(v_1, v_2, \ldots, v_n) : v_i \in \mathbb{F}_p^n \text{ linearly independent}\}.$$

Note that we have $p^n - 1$ choices for v_1. We must avoid p multiples of v_1 for our second choice. We must avoid p^2 combinations of v_1, v_2 for our third choice, etc. So v_{i+1} can be chosen in $p^n - p^i$ ways. So

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1}).$$

So we can pull out $1 + 2 + \cdots + n - 1 = \frac{n(n-1)}{2}$ factors of p, which is the size of the Sylow p-subgroup. Consider the subgroup of $GL_n(\mathbb{F}_p)$, a generalization of the Heisenberg group, as the matrices with ones on the diagonal and zeros below it. This has size $p^{\frac{n(n-1)}{2}}$, which means it's a Sylow p-subgroup. □

4.3 Product of subgroups

Definition (Product of subgroups): Let G be a group with subgroups A, B. Define the *product* of A and B as $AB = \{ab : a \in A, b \in B\}$.

Example (Product of subgroups isn't subgroup): Let $G = S_n$, $A = \{1, (1,2)\}, B = \{1, (2,3)\}$ where $AB = \{1, (1,2), (2,3), (1,2,3)\}$ which is not a subgroup.

Proposition 22 (Size of product of subgroups): Let $A, B \leq G$ with G finite. Then,

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

Proof. Write

$$AB = \bigcup_{a \in A} aB.$$

Then $|AB| = |B||A : B|$. Two cosets of B in A are equal if and only if two cosets of $A \cap B$ in A are equal:

$$aB = a'B \iff a^{-1}a' \in B \iff a^{-1}a' \in A \cap B \iff a(A \cap B) = a'(A \cap B).$$

So the number of cosets of B is the number of cosets of $A \cap B$ in A, and

$$|AB| = |B|\frac{|A|}{|A \cap B|}.$$

□

Proposition 23: If $A, B \leq G$ and B normalizes A, then $AB \leq G$.

Proof. Since B normalizes A, $bAb^{-1} = A \implies bA = Ab$ for all $b \in B$, so

$$BA = \bigcup_{b \in B} bA = \bigcup_{b \in B} Ab = AB.$$

We show $AB \leq G$:

(a) $e = ee \in AB$.

(b) Let $a_1b_1, a_2b_2 \in AB$. Then,

$$a_1b_1a_2b_2 = a_1(a_3b_3)b_2 = a_4b_4 \in AB.$$

(c) Let $ab \in AB$. Then,

$$(ab)^{-1} = b^{-1}a^{-1} \in BA = AB.$$

□

4.4 Sylow's theorems II and III

Lemma (1): Suppose $Q \leq G$ is a p-subgroup and $P \leq G$ is a Sylow p-subgroup. Suppose Q normalizes P. Then $Q \leq P$.

Proof. By proposition above, since Q normalizes P, $PQ \leq G$. Then, since $|PQ| = \frac{|P||Q|}{|P \cap Q|}$, and $P \cap Q \leq Q$ is a p-group, $|PQ|$ is a p-group. But since $P \leq PQ$ and P is Sylow, it follows that $P = PQ$, so $P \cap Q = Q$ and $Q \leq P$.

□

Theorem (Sylow II): Let G be a finite group. Let n_p be the number of Sylow p-subgroups. Then, $n_p \equiv 1 \pmod{p}$.

Proof. Let $X = \{P \leq G : P \text{ is Sylow } p\text{-subgroup}\}$. We show $|X| \equiv 1 \pmod{p}$. Let G act on X by conjugation, and restrict the acting set to a fixed Sylow p-subgroup P. Let $Q \in X$ be any Sylow p-subgroup. We consider the P-orbit of Q:

$$|P \cdot Q| = |P : N_G(Q) \cap P| = |P : \{g \in P : gQg^{-1} = Q\}|.$$

If $Q = P$, then $|P \cdot Q| = |P : P| = 1$. Otherwise, since P is a p-group and $N_G(Q) \cap P \leq P$ is a p-group, $\frac{|P|}{|N_G(Q) \cap P|}$ is a p-group. But if it were the identity group, P must normalize Q, and by lemma 1, $P \leq Q$. But since P and Q are both Sylow, this would imply they are equal, a contradiction. So p divides $|P \cdot Q|$. So

$$|X| \equiv 1 \pmod{p}.$$

Remark (using Sylow III): for any Sylow p-subgroup P, $n_p = |G : N_G(P)|$, which means that if $n = p^k m$, $n_p \mid m$. □

Theorem (Sylow III): Let G be a finite group. The Sylow p-subgroups of G are conjugate, i.e. for Sylow p-subgroups P, P', there exists $g \in G$ such that

$$P = gP'g^{-1}.$$

Furthermore every p-subgroup is contained in some Sylow p-subgroup.

Proof.

(a) For fixed Sylow P, the P-orbits of X consist of one orbit of size 1 (just P) and other orbits of size p^k with $k \geq 1$. Note that each P-orbit is contained in a unique G-orbit. Thus the G-orbits are some aggregation of the P-orbits and there will be one G-orbit with size 1 modulo p which necessarily contains P. But since P is arbitrary, all Sylow subgroups are contained in this same orbit of size 1 modulo p, so all Sylow subgroups are conjugate.

(b) Let Q be a p-group. Consider the Q-orbits of X. Since $X \equiv 1 \pmod{p}$, at least one orbit has size not divisible by p, say $Q \cdot P$. But since Q is a p-group, p divides

$$|Q \cdot P| = |Q : N_G(P) \cap Q|.$$

So it must be that $Q \cdot P = \{P\}$, i.e. $Q \leq N_G(P)$. So $Q \leq P$.

□

Theorem (Recognition theorem): Let $A, B \trianglelefteq G$ with $A \cap B = 1$. Then $AB \leq G$ and $AB \cong A \times B$.

Proof. AB is a group, as since $A \trianglelefteq G$, all of G thus B normalizes A, and we can apply ealier proposition.

Define the map $\phi : A \times B \to AB$, $(a, b) \mapsto ab$. To show ϕ is an isomorphism it suffices to show elements in A commute with elements of B, since then we can represent elements of AB as $a'^i b'^j$ for some a', b'. So let $a \in A, b \in B$.

$$ab = ba \iff aba^{-1}b^{-1} = 1.$$

Apply normality of A and B to show that $aba^{-1}b^{-1}$ must be in both A and B, thus it is 1 as required. □

Theorem: Every finite abelian group is isomorphic to product of cyclic groups.

Lemma (1): Suppose G is a finite abelian group and $P_1, \ldots, P_k$ are its Sylow subgroups. Then $G \cong P_1 \times \cdots \times P_k$.

Proof. Note that since G is abelian, its subgroups are normal so there is only one Sylow p subgroup for each prime factor. Let $|G| = p_1^{t_1} \ldots p_k^{t_k}$. Let $G_i \coloneqq P_1 \ldots P_i$. We show that for each i, $G_i \leq G$ and $G_i \cong P_1 \times \cdots \times P_i$ by induction.

The base case $i = 1$ is trivial. Suppose $i > 1$ and $G_{i-1} \cong P_1 \ldots P_{i-1}$. So $|G_{i-1}|$ and $|P_i|$ are coprime, meaning $G_{i-1} \cap P_i = 1$ (Lagrange). So by earlier proposition $G_{i-1}P_i = G_i \leq G$ and $G_i \cong P_1 \times \cdots \times P_i$. □

4.5 Automorphisms

Definition (Automorphism group): For a group G, define $\mathrm{Aut}(G)$ as the set of all automorphisms ϕ of G. This is a group under composition:

(a) Homomorphisms are preserved under composition.

(b) id is an automorphism of G.

(c) The inverse of an isomorphism is an isomorphism.

Example:

(a) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

(b) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_3$.

Definition (Acting by automorphism): A group K acts on a group H *by automorphism* if $h \mapsto h \cdot k$ is an automorphism, i.e. there is a ϕ such that

$$\phi : K \to \mathrm{Aut}(H).$$

Proposition 24 (Conjugation of normal group is automorphism): Let $H \trianglelefteq G$. Then G acting on H by conjugation is acting by automorphism, i.e. $h \mapsto ghg^{-1}$ is an automorphism. Furthermore, if $\phi : G \to \mathrm{Aut}(H)$ represents the action, its kernel is $C_G(H)$.

Proof. Conjugation is an isomorphism by previous proposition, and it maps $H \to H$ since H is normal, so it is an automorphism. Let $\phi : G \to \mathrm{Aut}(H)$ represent the action of G on H by conjugation. Then,

$$\ker \phi = \{g \in G : ghg^{-1} = h \text{ for all } h \in H\} = C_G(H).$$

□

4.6 Semidirect product

Definition (Semidirect product): Suppose H, K are groups, and K act on H by automorphism represented by $\phi : K \to \mathrm{Aut}(H)$. The semidirect product of H and K with respect to ϕ is the set $H \times K$ with operation

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

We denote this group $H \rtimes K$.

This is a group.

(a) Operation is associative: fuck no

(b) Identity: (e_h, e_k).

(c) Inverse: let $(h, k) \in H \rtimes K$. Then $(k^{-1} \cdot h^{-1}, k^{-1})$ is its inverse:

$$(k^{-1} \cdot h^{-1}, k^{-1})(h, k) = (k^{-1} \cdot h^{-1} k^{-1} \cdot h, k^{-1} k) = (e_h, e_k).$$

$$(h, k)(k^{-1} \cdot h^{-1}, k^{-1}) = (hk \cdot (k^{-1} \cdot h^{-1}), kk^{-1}) = (e_h, e_k).$$

□

The intuition behind semidirect products is sometimes we have $H \trianglelefteq G, K \leq G$, $H \cap K = 1$, so $HK \leq G$ with $|HK| = G$. In fact we can define a bijection between HK and $H \times K$. However this isn't necessarily an isomorphism!

Example (Semidirect product example: pq group): Let $|G| = pq$ for $p < q$. Let n_p be the number of Sylow p-subgroups and n_q be the number of Sylow q-subgroups. By Sylow II,

$$n_q \equiv 1 \pmod{q}, n_q \mid p.$$

Since $p < q$, $n_q = 1$. Let Q be the unique Sylow q-subgroup and it follows by Sylow subgroups being conjugate that $Q \trianglelefteq G$.

Let $|G| = pq$, $P, Q \leq G$ with $|P| = p$, $|Q| = q$, and Q normal (this is always true if $p < q$). Then, since $|P \cap Q| = 1$,

$$|QP| = \frac{|Q||P|}{|Q \cap P|} = pq.$$

So $QP = G$. Furthermore, $QP \cong Q \rtimes P$, where P acts on Q by $p \cdot q = pqp^{-1}$, with isomorphism $\phi : (p, q) \to pq$.

Conversely, if Q is a group of order q and P is a group of order p, $\phi : Q \to \mathrm{Aut}(P)$, $|P \rtimes Q| = pq$.

Example (Semidirect product):

(a) If H, K are groups and $\phi : K \to \mathrm{Aut}(H)$ is trivial $k \mapsto \mathrm{id}$, then $H \rtimes K = H \times K$.

(b) Let $H = \mathbb{Z}/n\mathbb{Z}, K = \mathbb{Z}/2\mathbb{Z}$ with $\phi : K \to \mathrm{Aut}(H)$. We know $\phi(0) = \mathrm{id}$. If $\phi(1)$ is $h \mapsto -h$, then

$$H \rtimes K \cong D_{2n}, (h, k) \mapsto r^h f^k.$$

This is called the *generalized dihedral group.*

(c) $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \{x \in \mathbb{Z}/n\mathbb{Z} : \gcd(x, n) = 1\}$ with isomorphism by $x \mapsto (t \mapsto xt)$.

Example (Euclidean rigid motion): Let $H = \mathbb{R}^n$, $K = O(n) \subseteq GL_n(\mathbb{R})$ the set of orthogonal matrices. $O(n)$ acts on $\mathbb{R}^n$ by automorphism by

$$M \cdot v = Mv.$$

5 Rings

5.1 Definitions and examples

Definition (Ring): A ring is a triplet $(R, +, \times)$ where R is a set, $+, \times$ are binary operations on R satisfying:

(a) $(R, +)$ is an abelian group (identity denoted 0).

(b) $\times$ is associative.

(c) Distributivity: $a \times (b + c) = a \times b + a \times c$, $(a + b) \times c = a \times c + b \times c$.

Note the absence of requirement of multiplicative identity (this allows $\mathbb{Z}/2\mathbb{Z}$ to be a ring).

Example (Rings):

(a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

(b) $\mathbb{Z}/n\mathbb{Z}$.

(c) Noncommunative example: If R is a ring, $M_n(R)$ the set of $n \times n$ matrices with entries in R with standard matrix addition and multiplication is a ring.

Definition (Center of ring): The *center* of a ring R is given by

$$Z(R) = \{a \in R : ab = ba \text{ for all } b \in R\}.$$

Proposition 25 (Basic properties): Let $a, b \in R$.

(a) $0 \times a = a \times 0 = 0$.

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

(c) $(-a)(-b) = ab$.

(d) If R has 1, it is unique and $-a = (-1)a$.

Proof. For (a), $0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a$, then subtract $0 \times a$ from both sides. The rest follow by distributive property. □

Definition (Zero divisor): An element $a \in R \setminus \{0\}$ is a *zero divisor* if there exists $b \in R \setminus \{0\}$ such that $ab = 0$ or $ba = 0$.

Example (Zero divisors):

(a) In $M_2(\mathbb{R})$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a zero divisor.

(b) In $\mathbb{Z}/n\mathbb{Z}$ for $n = ab$, a and b are zero divisors.

Definition (Unit): Suppose R has a multiplicative identity 1. Then u is a unit ("divisor of 1") if there exists $v \in R$ such that $uv = vu = 1$.

Note that 0 cannot be a unit by above proposition.

Definition (Field): A *field* is a communative ring with 1 in which each nonzero element is a unit.

Definition (Subring): A subring is a subset of a ring that is also a ring under the same operations.

Example (Subrings):

(a) $n\mathbb{Z}$ is subring of $\mathbb{Z}$.

(b) $\mathbb{Z}$ is subring of $\mathbb{Q}$ is subring of $\mathbb{R}$.

Example (Quadratic field): Let $D \in \mathbb{Q}$, then define $\mathbb{Q}(\sqrt{D}) = \{a+b\sqrt{D} : a, b \in \mathbb{Q}\}$ under usual addition and multiplication. This is a subring of $\mathbb{R}$, as we have closure under addition and associativity, distributivity are inherited.

It is a field, since the ring is communative, 1 is the multiplicative identity, and all elements are units.

5.2 Polynomial rings

Definition (Polynomial ring): Let R be a communative ring with 1. Then the ring of polynomials over R (informally) consists of expressions of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

for $n \in \mathbb{N}$, with addition and multiplication as we would expect. We denote it $R[x]$. More formally, a polynomial over R is a function $f : \mathbb{Z} \to \mathbb{R}$ such that $f(i) = 0$ if $i < 0$ and $f(i) = 0$ for all sufficiently large i. Then,

(a) $(f + g)(i) = f(i) + g(i)$.

(b) $(fg)(i) = \sum_{i+j=k} f(i)g(j)$.

Definition (Ring of power series): The ring of power series over R, $R[[x]]$ is defined the same way but without needing the condition that $f(i) = 0$ for sufficiently large i.

Definition (Ring of Laurent series): Functions $f : \mathbb{Z} \to \mathbb{R}$ such that $f(i) = 0$ for all sufficiently negative i, i.e.

$$f(x) = a_{-2}x^{-2} + a_{-1}x^{-1} + a_0 + a_1 x + \dots$$

Definition (Polynomials of 2 variables): Define $R[x, y] = R[x][y] = R[y][x]$, where $(R[x])[y]$ denotes polynomials in y where coefficients are polynomials in x.

Definition (Ring homomorphism, isomorphism): A function $\phi : R \to S$ between rings R, S is a *ring homomorphism* if for all $x, y \in R$,

(a) $\phi(x + y) = \phi(x) + \phi(y)$.

(b) $\phi(xy) = \phi(x)\phi(y)$.

A ring isomorphism is a bijective ring homomorphism.

Example:

(a) $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ modding out by n.

(b) $\mathrm{id} : R \to R$.

(c) $\phi : R \to S$ by $r \mapsto 0$.

(d) Evaluation homomorphism: suppose R is a communative ring with 1, $a \in R$ is fixed. $\phi : R[x] \to R$ evaluates the polynomial at a.

Definition (Polynomial function): The polynomial function associated with $f \in R[x]$ is the obvious $a \mapsto f(a)$.

Example (Polynomial functions are not polynomials): Let $R = \mathbb{Z}/2\mathbb{Z}$. Let $f_1 = x, f_2 = x^2 \in R[x]$. The polynomials are distinct, however the polynomial functions are equal.

Definition (Kernel): Let $\phi : R \to S$ a ring homomorphism. Then

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

5.3 Ideal

Definition (Ideal): A subring I of R is an *ideal* if for all $r \in R, a \in I$, $ra, ar \in I$.

Proposition 26 (Kernel is ideal): Let $\phi : R \to S$ be a ring homomorphism. Then $\ker \phi$ is an ideal in R.

Proof. Let $I = \ker \phi$. Then $(I, +)$ is a normal subgroup. Let $a \in I$, $r \in R$. Then,

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \times 0 = 0.$$

□

Example (Ideals in $\mathbb{Z}$): The ideals in $\mathbb{Z}$ are $n\mathbb{Z}$.

(a) If I, J are ideals, then $I + J = \{x + y : x \in I, y \in J\}$ is an ideal in R. And
$$n\mathbb{Z} + m\mathbb{Z} = \gcd(n, m)\mathbb{Z}.$$

(b) If I, J are ideals, then $I \cap J$ is an ideal, and
$$n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(n, m)\mathbb{Z}.$$

Definition: We define the *ideal generated by a subset* $S \subseteq R$ as
$$(S) = \bigcap_{S \subseteq I} I.$$

Proposition 27: $(S) = \{r_1 a_1 r_1' + r_2 a_2 r_2' + \cdots + r_n a_n r_n' : r_i, r_i' \in R, a_i \in S\}$.

Example (Product of ideals): If I, J are ideals, then we cannot define $IJ = \{xy : x \in I, y \in J\}$, as closure isn't guaranteed. So we define
$$IJ = (\{xy : x \in I, y \in J\}).$$

Definition (Ring quotient): For a ring R and an ideal I, the quotient ring R/I consists of cosets $r + I$ for $r \in R$ with operations

(a) $(r + I) + (s + I) = (r + s) + I$.

(b) $(r + I)(s + I) = rs + I$.

Note that the multiplication is not $\{xy : x \in r + I, y \in s + I\}$ since if $I = 3\mathbb{Z}$, $(0 + 3\mathbb{Z})(0 + 3\mathbb{Z}) = 0 + 3\mathbb{Z}$, but the naive product is $9\mathbb{Z}$.

Proposition 28 (R/I is a ring): Let

Example (Ring quotients):

(a) $\mathbb{Z}/n\mathbb{Z}$.

(b) Say I is in a ring R. Then $M_n(I) \subseteq M_n(R)$ is an ideal.

Definition (Maximal ideal): An ideal I in a ring R is *maximal* if there is no ideal J such that $I \subset J \subset R$.

Example (Maximal ideals in $\mathbb{Z}$ are $p\mathbb{Z}$): In $\mathbb{Z}$, $m\mathbb{Z} = (m), n\mathbb{Z} = (n)$, so $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid m$. So the maximal ideals in $\mathbb{Z}$ are (p).

Proposition 29: If R is communative with 1, and M is an ideal in R, Then

$$M \text{ is maximal } \iff R/M \text{ is a field.}$$

Proof. Suppose M is maximal. R/M has multiplicative identity $1+M$, since $(1+M)(a+M) = a+M$. Suppose $a+M \in R/M$ is nonzero, i.e. $a \notin M$. Since M is a maximal ideal, $(a, M) = R$. So $1 \in (a, M)$, i.e. for $b, c_i \in R$, $m_i \in M$, $n \in \mathbb{N}$,

$$1 = ba + \sum_{i=1}^{n} c_i m_i.$$

Now, $(a+M)(b+M) = (1+c)+M$ for some $c \in M$, so it equals $1+M$.

Now suppose R/M is a field. Let L be an ideal properly containing M. So there is $a \in L, a \notin M$. So $a+M \neq 0$ and for some $b \in R$,

$$(a+M)(b+M) = 1+M.$$

So $1-ab \in M$. Since $ab \in L$ as L is an ideal, it follows that $(1-ab)+ab = 1 \in L$, which means $L = R$.

□

Definition ($\mathbb{F}_p$): Since $p\mathbb{Z}$ is maximal in $\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ is a field. We call this $\mathbb{F}_p$.

Example: Let $R = \mathbb{R}[x]$, $M = (x^2+1)$. Then, by previous proposition (we show later (x^2+1) is maximal since x^2+1 is irreducible and $\mathbb{R}[x]$ is a PID),

$$Q = \frac{\mathbb{R}[x]}{(x^2+1)}$$

is a field. Each element of the quotient is of the form $f + (x^2+1)$ where f is a polynomial of degree less than 2. Also, if f_1, f_2 have degree < 2, and $f_1 + (x^2+1) = f_2 + (x^2+1)$, then clearly $f_1 = f_2$. Furthermore,

$$\{a + (x^2+1) \in Q : a \in \mathbb{R}\}$$

is a subring of Q isomorphic to $\mathbb{R}$.

Example (Complex numbers): Q as above has an element such that $r^2 = -1$, namely x. Denote this i, then

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}.$$

5.4 Euclidean domains

Definition (Integral domain): An *integral domain* is a communative ring with 1 and no zero divisors.

The virtue here is that we can cancel things: for r, s, s', if $rs = rs'$, then $r(s-s') = 0$ and so $s - s' = 0$ (r is not a zero divisor). Note that all fields are integral domains.

Proposition 30 (Finite integral domains are fields):

Proof. By cancellation law $x \mapsto ax$ is injective. □

Definition (Euclidean domain): An integral domain R is an *Euclidean domain* if there is $N : R \to \mathbb{Z}_{\geq 0}$ such that $N(a) = 0$ if and only if $r = 0$ and for every $a \in R$, nonzero $d \in R$,

$$a = qd + r,$$

for some $q \in R$ and $r \in R$ such that $N(r) < N(d)$. This function N is called the "norm on a Euclidean domain".

Example (Euclidean domains):

(a) Fields, like $\mathbb{Q}, \mathbb{R}$. Division is defined, so we never need remainders and can set $N(x) = 0$ if $x = 0$, 1 otherwise.

(b) $\mathbb{Z}$ with $N(r) = |r|$.

(c) If F is a field, then $R = F[x]$ is a Euclidean domain with $N(f)$ as 0 if $f = 0$ and $\deg f + 1$ otherwise.

Proposition 31 (Euclidean domains are PID): If R is an Euclidean domain, and I is an ideal in R, then there exists $r \in R$ such that $I = (r)$.

Proof. If $I = 0$, then $I = (0)$. Otherwise, consider

$$m = \min\{N(s) : s \in I \setminus \{0\}\}.$$

Let r be an element of $I \setminus \{0\}$ with $N(r) = m$. We claim $I = (r)$. Let $a \in I$, then by definition of Euclidean algorithm,

$$a = qr + r'$$

where $N(r') < N(r)$. So $r' = 0$ by minimality, and $a = qr \in (r)$. On the other hand $(r) \subseteq I$ trivially since $r \in I$. □

Definition (Principal ideal): An ideal of the form (r) is called a *principal* ideal.

Definition (Principal ideal domain): An integral domain all of whose ideals are principal is called a *principal ideal domain.*

5.5 Gaussian Integers

Definition (Gaussian integers): $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is subring of $\mathbb{C}$.

Example (Norm on quadratic extensions of $\mathbb{Q}$): Let $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ for D not square. Define the (easily verified) automorphism $\tau : a + b\sqrt{D} \mapsto a - b\sqrt{D}$. Define the norm

$$N(r) = r \cdot \tau(r); N(a + b\sqrt{D}) = a^2 - b^2 D.$$

Note that $N(rr') = N(r)N(r')$ since τ is an automorphism.

Proposition 32: $\mathbb{Z}[i]$ is an Euclidean domain.

Proof. Using the above norm on $\mathbb{Z}[i]$, define

$$N(a+bi) = a^2 + b^2.$$

We show this is a norm on a Euclidean domain:

(a) $N(a+bi) = 0$ iff $a+bi = 0$.

(b) If $a+bi \in \mathbb{Z}[i], c+di \in \mathbb{Z}[i] \setminus 0$, then thinking of $\mathbb{Z}[i]$ as a subring of $\mathbb{Q}[i]$,

$$\frac{a+bi}{c+di} = \frac{(ac+db)+(bc-ad)i}{c^2+d^2}.$$

Define the quotient in $a+bi = q(c+di)+r$ by the closest integer to the integer and imaginary parts, and do the algebra.

□

5.6 Prime ideals and elements

Definition (Generating ring from subset): For a ring S and a subring R, and a set $A \subseteq S$, define $R[A]$ as the ring generated by $R \cup A$.The notion is simlar for fields.

Definition (Prime ideal): An ideal P in a ring R is *prime* if $P \neq 0$, P is proper, and

$$ab \in P \implies a \in P \text{ or } b \in P.$$

Definition (Prime element): An element $p \in R$ is a *prime element* if (p) is a prime ideal.

Definition (Irreducible element): Let R be a ring with 1. An element r is *irreducible* if $r = ab$ implies a or b is a unit.

Proposition 33 (Prime elements are irreducible in integral domain): Let R be an integral domain. If $r \in R$ is prime, then r is irreducible.

Proof. Say $r = ab$. Since r is prime, $ab \in (r)$. So one of a, b is in (r) (?). If $a \in (r)$, then $a = kr$ for some $k \in R$. Then,

$$r = (kr)b = rkb.$$

Since r is not zero or a zero divisor, we can cancel, and so $1 = kb$ and b is a unit. □

Example (Irreducible but not prime): Let $R = \mathbb{Z}[\sqrt{-5}]$. 3 is irreducible: if $3 = ab$ for $a, b \in \mathbb{Z}[\sqrt{-5}]$, then $N(3) = N(ab) = N(a)N(b) = 9$. If $N(a) = 1$, then $a = \pm 1$ is a unit. Similar for $N(b) = 1$. If both $N(a) = N(b) = 3$, then $x^2 + 5y^2 = 3$, which is not possible. However, 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$:

$9 = 3 \cdot 3 \in (3)$, but $9 = (2+\sqrt{-5})(2-\sqrt{-5})$. 3 does not divide either factor, so (3) cannot be a prime ideal.

Proposition 34 (1): If R is a PID, and $r \in R$ is irreducible, then r is prime.

Proposition 35 (2): If R is a PID, $r \in R$ is irreducible, then (r) is a maximal ideal.

Proof. Suppose $(r) \subset M$, where M is an ideal. Since we are in a PID, there is $m \in R$ such that $M = (m)$. So

$$(r) \subseteq (m) = \{am : a \in R\}.$$

Thus $r = bm$ for some $b \in R$. Since r is irreducible, either b or m is a unit. If m is a unit, then $(m) = R$, and (r) is maximal since M is arbitrary. If b is a unit, then we may take its multiplicative inverse, so

$$m = rb^{-1}.$$

This implies $(m) \subseteq (r)$, so $(m) = (r)$ □

Proposition 36 (3): Maximal ideals are prime.

Proof. Suppose M is maximal, and $ab \in M$. Assume $a \notin M$. We show $b \in M$. Since M is maximal and $a \notin M$,

$$(a, M) = R \implies 1 \in (a, M) \implies 1 = ca + m,$$

for some $c \in R, m \in M$. Then,

$$b = abc + mb \in M.$$

□

Example (Prime ideal but not maximal): Consider (x) which is not maximal since otherwise $\mathbb{Z}[x]/(x) = \mathbb{Z}$ would be a field.

5.7 Unique factorization

Definition (Unique factorization domain): An integral domain R is a *unique factorization domain* (UFD) if every nonzero, nonunit r can be factored as

$$r = p_1 p_2 \dots p_n,$$

where $p_1, \dots, p_n$ are irreducibles in R, and this factorization is unique (i.e. two factorizations have the same number of terms and there is permutation $\pi \in S_n$ such that p_i and $q_{\pi(i)}$ are *associate*, meaning $p_i = u_i q_{\pi(i)}$ for some unit u_i).

Definition: A ring R satisfies an *ascending chain condition* (ACC) if whenever $I_1 \subseteq I_2 \subseteq \dots$, then there exists n_0 such that $I_n = I_{n+1}$ for all $n \geq n_0$.

Proposition 37 (PID satisfies ACC):

Proof. Let $I_1 \subseteq I_2 \subseteq \dots$, and let $I = \bigcup_n I_n$. By HW9, I is an ideal, and since we are in PID, for some $g \in I$,

$$I = (g).$$

Then there is n_0 such that $g \in I_{n_0}$, so $(g) \subseteq I_{n_0}$. This means $I = I_{n_0}$. □

Theorem: If R is a PID, then R is a UFD.

Proof. Let $B = \{r : r \text{ is not zero or unit, cannot be factored as irreducibles}\}$. Suppose $B \neq \varnothing$, let $b_1 \in B$. b_1 is clearly not irreducible, so there is factorization $b_1 = b_2 b_2'$ where neither b_2, b_2' is a unit. If neither is in B, then they both have factorizations and clearly b_1 has a factorization.

So suppose $b_2 \in B$. Note that $(b_1) \subseteq (b_2)$ since b_1 is a multiple of b_2. Since b_2' is not a unit, $(b_1) \neq (b_2)$, so

$$(b_1) \subset (b_2).$$

Continue likewise, TODO.

Now we show uniqueness. Suppose $p_q p_2 \dots p_n = q_1 q_2 \dots q_m$. We induct on maximum of n, m. Suppose $n \leq m$. Since p_n is prime, ... □

Definition (Greatest common divisor): For elements r, r' in a communative ring R, a greatest common divisor of r, r' is an element $d \in R$ such that $d \mid r$ and $d \mid r'$ and for every d' such that $d' \mid r, d' \mid r'$, $d' \mid d$.

Note that gcd is defined up to multiplication by units.

Remark: In UFD, any two elements have a gcd, and it can be computed in the usual way by considering the factorizations.

5.8 UFD polynomial rings

Theorem: If R is UFD, then $R[x]$ is UFD.

Corollary: If F is a field, then $F[x_1, \dots, x_n]$ is a UFD.

Definition (Rings of fractions): Suppose R is a communative ring, and $D \subseteq R$ such that

(a) $D \neq \varnothing$.

(b) D has no zero divisors and $0 \notin D$.

(c) D is closed under multiplication.

Define an equivalence relation on $R \times D$ by $(r, d) \sim (r', d')$ if $rd' = r'd$:

(a) Suppose $(r_1, d_1) \sim (r_2, d_2)$, $(r_2, d_2) \sim (r_3, d_3)$. So $r_1 d_2 = r_2 d_1, r_2 d_3 = r_3 d_2$. Then, ...

Define the ring of fractions denoted by $D^{-1}R$ or $R[D^{-1}]$ consisting of equivalence classes $\frac{r}{d}$ for $r \in R, d \in D$ with usual operations. This is well-defined (proof omitted).

Example:

(a) If R is an integral domain, and $D = R \setminus \{0\}$. Then $R[D^{-1}]$ is a field, since we can define $(a/d)^{-1} = d/a$.

(b) If $R = \mathbb{Z}$, then the field of fractions is $\mathbb{Q}$.

(c) If $R = 2\mathbb{Z}$, then the field of fractions is isomorphic to $\mathbb{Q}$.

(d) If $R = F[x]$, where F is a field, then the field of fractions is denoted $F(x)$.

(e) If R is a communative ring, $d \in R$ is not a zero divisor or 0, we can let $D = \{d, d^2, d^3, \dots\}$. Then, $R[D^{-1}] = \{\frac{a}{d^n} : n \in \mathbb{Z}\}$.

Definition: Let R be a UFD, $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. The *content* of f is

$$c(f) = \gcd(a_0, a_1, \dots, a_n).$$

Theorem (Gauss's lemma for primitivity): If R is a UFD and $f, g \in R[x]$ are nonzero,

$$c(fg) = c(f)c(g).$$

Proof. Observe that if $c \in R$, then $c(cf) = c \cdot c(f)$. This allows us to assume WLOG $c(f) = c(g) = 1$.

Assume towards contradiction that some irreducible $p \in R$ divides $c(fg)$. Let i_0, j_0 denote the smallest indices such that p does not divide a_i, b_i respectively. Consider

$$c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + (\sum_{i<i_0} + \sum_{j<j_0}) a_i b_j.$$

In particular p divides both sums.

TODO □

Remark: Every $f \in F[x]$ is of the form

$$\frac{f'}{d}, f' \in R[x], d \in R \setminus \{0\}.$$

Since we can let d be the product of the denominators of coefficients of f.

Definition (Content of fraction): Let $f \in F[x]$, i.e.

$$f = \frac{f'}{d},$$

$f' \in R[x]$, $d \in R, d \neq 0$. Then,

$$c(f) \coloneqq \frac{c(f')}{d}.$$

This is well defined, since $\frac{f_1}{d_1} = \frac{f_2}{d_2} \implies f_1 d_2 = f_2 d_1$, so

$$c(f_1 d_2) = c(f_2 d_1) \implies c(f_1) d_2 = c(f_2) d_1 \implies \frac{c(f_1)}{d_1} = \frac{c(f_2)}{d_2}.$$

Proposition 38: If $f, g \in F[x]$, then $c(fg) = c(f)c(g)$.

Proof. Let $f = \frac{f'}{d}, g = \frac{g'}{e}$. Then, using Gauss's lemma,

$$c\left(\frac{f'g'}{de}\right) = \frac{c(f'g')}{de} = \frac{c(f')}{d}\frac{c(g')}{e} = c(f)c(g).$$

□

Proposition 39: Let $f \in F[x]$. The following are equivalent:

(a) $f \in R[x]$.

(b) $c(f) \in R$.

Proof. If $f \in R[x]$, $c(f)$ is a gcd of things in R, which is in R. Conversely, if $c(f) \in R$, then letting $f = f'/d$ for $f' \in R$,

$$c(f) = \frac{c(f')}{d} \in R.$$

This means d divides $c(f')$ in R so $f \in R$. □

Theorem (Gauss's lemma): Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. If p is reducible in $F[x]$ then it is reducible in $R[x]$.

More precisely, if $p(x) = A(x)B(x)$ for nonconstant polynomials $A, B \in F[x]$, then for some nonzero $r, s \in F$,

$$p(x) = (rA(x))(sB(x)) =: a(x)b(x),$$

where $a, b \in R[x]$.

Proof. Multiply $p(x) = A(x)B(x)$ through by a common denominator d so that

$$dp(x) = a'(x)b'(x)$$

for $a', b' \in R[x]$. If d is a unit in R then we are essentially done. Otherwise write d as a product of irreducibles $d = p_1 \dots p_n$. Reduce the equation modulo p_1, leaving us with an integral domain (R/I is integral domain iff I is prime ideal) in which $\overline{a'(x)b'(x)} = 0$. By integral domain we can cancel p_1 into either a' or b'. Repeat this until we have canceled all irreducibles in d, and we're done. □

Remark: The converse of Gauss's lemma is only true when $c(p) = 1$, else a factorization into irreducibles in $R[x]$ may not be a factorzation into irreducibles in $F[x]$.

Example: $7x + 14$ is irreducible in $\mathbb{Q}[x]$ since 7 is a unit. But it's reducible $7(x + 2)$ in the integer polynomials.

Proposition 40: The irreducible elements of $R[x]$ (R is UFD) are

(a) Polynomials of degree 0.

(b) Polynomials $f \in R[x]$ with $\deg f \geq 1$ such that $c(f) = 1$ and f is irreducible in $F[x]$.

Theorem: R is UFD $\iff$ $R[x]$ is UFD.

Proof. Omitted. □

5.9 *Irreducibility criterion

Note that by Gauss's lemma, when determining irreducibility in a UFD polynomial ring $R[x]$ it suffices to consider factorizations in the polynomial ring of fractions $F[x]$.

Theorem (Root iff linear factor): Let F be a field and $p(x) \in F[x]$. $p(x)$ contains a root if and only if $p(x)$ contains a linear factor.

Proof. Suppose $p(a) = 0$. By division algorithm in $F[x]$

$$p(x) = q(x)(x - a) + r,$$

where r is constant. Plugging in $x = a$ we see $r = 0$ and so $p(x) = q(x)(x - a)$ as required. Conversely, linear factors always yield roots. □

Corollary: If $\deg f \leq 3$, f is reducible in $F[x]$ if and only if f has a root in F.

Theorem (Rational root theorem): Let $p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ is a rational root in lowest terms, $r \mid a_0$ and $s \mid a_n$.

Proof.

$$a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$$

tells us that $r \mid a_0$. Multiplying through by s^n, we see $s \mid a_n$. □

Proposition 41: Let I be an ideal of integral domain R. Let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If p is reducible in $R[x]$, then p is reducible in $(R/I)[x]$.

In particular, to show a polynomial is irreducible in $\mathbb{Z}$ it suffices to show it is irreducible when we reduce coefficients modulo n.

Proof. Trivial. □

Theorem (Eisenstein's criterion): Let P be a prime ideal of integral domain R, let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. Suppose $a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$. Then f is irreducible in $R[x]$.

Proof. Suppose the conditions are met but $f(x) = a(x)b(x)$ for nonconstant polynomials a, b. Mod out by P, then

$$x^n = a(x)b(x) \pmod{P}.$$

We claim both a, b must have 0 constant terms (modulo P). Suppose a has nonzero constant term, then multiply it by the smallest nonzero term in b to get a nonzero term of degree less than n in the product. Thus $a_0 \notin P^2$ is a contradiction. □

Example:

(a) Let $f(x) = x^4 + 1$. Although we cannot apply Eisenstein directly, let $g(x) = f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$, and we can apply it using $p = 2$. Since $f(x+1)$ is irreducible clearly f is irreducible (in general, if $f(g(x))$ is irreducible then $f(x)$ is irreducible maybe?).

(b) Let $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Then,

$$f(x) = \frac{x^p - 1}{x - 1} \implies f(x+1) = \frac{(x+1)^p - 1}{x} \equiv x^{p-1} + p \pmod{p},$$

and Eisenstein with p tells us f (called cyclotomic polynomial) is irreducible.

5.10 Factorization in Gaussian integers

Let π be an irreducible in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a PID, so by proposition 35, (π) is a maximal thus prime ideal.

Proposition 42: Every irreducible in $\mathbb{Z}[i]$ is a factor of a prime number. Each prime number has 1 or 2 such factors.

Lemma: $p \in \mathbb{Z}$ factors into 2 irreducibles in $\mathbb{Z}[i]$ if and only if it is the sum of two squares.

Proof. If $p = a^2 + b^2$, then $p = (a + bi)(a - bi)$, and the irreducibles of these factors divide p. If p splits into 2 factors, then, $p = \pi\overline{\pi} = a^2 + b^2$ (earlier). □

Theorem: A prime number $p \in \mathbb{Z}$ is irreducible in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod{4}$.

Proof. If $p \equiv 3 \pmod{4}$ then p cannot be sum of squares since squares are $0, 1$ modulo 4. So p is irreducible. If p is irreducible, we use the lemma: □

Lemma: A prime number p divides a number of the form $n^2 + 1$ if and only if $p \equiv 1, 2 \pmod{4}$.

Proof. Suppose p divides a number of form $n^2 + 1$. So $n^2 \equiv -1 \pmod{p}, n^4 \equiv 1 \pmod{p}$. So $(\mathbb{Z}/p\mathbb{Z})^*$ as an element of order 4, i.e. $4 \mid p - 1$.

Conversely, suppose $4 \mid n - 1$. TODO □

Continued. Suppose $p \equiv 1 \pmod 4$. Suppose that p is irreducible in $\mathbb{Z}[i]$. By last lemma, $p \mid n^2+1 = (n+i)(n-i)$. Suppose $p \mid n+i$. Then $p = \overline{p} \mid \overline{n+i} = n-i$. So p divides both, and

$$p \mid (n+i) - (n-i) = 2i.$$

Then,

$$N(p) \mid N(2i) = 4 \implies p = 2.$$

But this contradicts p being an odd number. □

Theorem: $N \in \mathbb{Z}$ is of the form a^2+b^2 if and only if its prime factorization in $\mathbb{Z}$ is

$$N = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n},$$

where e_i is even wherever $p_i \equiv 3 \pmod 4$.

Proof. $G = \{a^2 + b^2 : a, b \in \mathbb{Z}\} = \{N(a + bi) : a, b \in \mathbb{Z}\}$ is closed under multiplication, which implies the backwards direction.

On the other hand, say $N = a^2+b^2 = (a+bi)(a-bi)$. Factor into irreducibles in $\mathbb{Z}[i]$:

$$a + bi = \pi_1 \pi_2 \dots \pi_m.$$

Then,

$$N = N(a + bi) = N(\pi_1)N(\pi_2) \dots N(\pi_m).$$

Then use classification of primes as irreducible if $p \equiv 3 \pmod 4$ to use $N(p) = p^2$. □

5.11 Chinese remainder theorem

Definition (Comaximal): Ideals I, J are *comaximal* if $I + J = R$.

For example, if $R = \mathbb{Z}$, $I = (a), J = (b)$, with $\gcd(a, b) = 1$ then $I + J = (\gcd(a, b)) = \mathbb{Z}$ by Euclidean algorithm.

Lemma (First isomorphism for rings): If $\phi : R \to S$ is a ring homomorphism then

$$\phi(R) \cong \frac{R}{\ker \phi}.$$

Theorem (Chinese remainder theorem): Suppose ideals $I_1, \dots, I_n$ are pairwise comaximal. Then

(a) $I_1 I_2 \dots I_n = I_1 \cap \dots \cap I_n$.

(b) $\frac{R}{I_1} \times \dots \times \frac{R}{I_n} \cong \frac{R}{I_1 I_2 \dots I_n}$.

Proof of CRT. Define $\phi : R \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$ by $r \mapsto (r + I_1, r + I_2, \ldots, r + I_n)$. Supposing (a) holds,

$$\ker \phi = I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \ldots I_n.$$

Then, by first isomorphism, if $\phi(R) = \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$, (b) holds.

We prove (a) and surjectivity by induction on n. $n = 1$ is trivial. For $n = 2$, suppose I, J are comaximal ideals, so $I + J = R$. Then, $1 \in I + J$, so $1 = x + y$ for some $x \in I, y \in J$ (these are the "coprime" elements). Consider

$$\phi(ax + by) = (ax + by + I, ax + by + J).$$

So

$$\phi(ax + by) \equiv b(1 - x) \pmod{I}, ax + by \equiv a(1 - y) \pmod{J}.$$

This shows $\phi(ax + by) = (b + I, a + J)$ so ϕ is surjective. Next, $I \cap J = IJ$:

(a) $IJ \subseteq I \cap J$ since $IJ \subseteq I$ and $IJ \subseteq J$.

(b) Let $r \in I \cap J$. Then,

$$r = r \cdot 1 = r(x + y) = rx + ry \in IJ.$$

Now suppose $n \geq 3$. We claim I_1 and $I_2 \ldots I_n$ are comaximal. Since I_1, I_j are comaximal, we can find $x_j \in I_1, y_j \in I_j$ such that $1 = x_j + y_j$. Write

$$1 = (x_2 + y_2)(x_3 + y_3) \ldots (x_n + y_n) \in I_2 \ldots I_n + I_1.$$

Therefore $1 \in I_2 \ldots I_n + I_1 \implies I_1 + I_2 \ldots I_n = R$ (sum of ideals is ideal). So IH and $n = 2$ case implies

$$I_1(I_2 \ldots I_n) = I_1(I_2 \cap \cdots \cap I_n) = I_1 \cap \cdots \cap I_n.$$

For surjectivity, define ψ as the surjective map for the $n-1$ case. Let $\tau : \frac{R}{I_1 \ldots I_n} \to \frac{R}{I_1} \times \frac{R}{I_2 \ldots I_n}$ (surjective by $n = 2$). Write the map $\phi : \frac{R}{I_1 \ldots I_n} \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$ as

$$\phi = (id \times \psi) \circ \tau,$$

which is the composition of surjective functions so surjective. □

Example (CRT in elementary number theory): Let n be a positive integer and $p_1^{a_1} \ldots p_k^{a_k}$ be its prime factorization. Then,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}.$$

So we have isomorphism also of their groups of units:

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^*.$$

Taking size of these groups tells us that the totient function is multiplicative across coprime numbers:

$$\varphi(n) = \varphi(p_1^{a_1}) \ldots \varphi(p_k^{a_k}).$$

Example (Lagrange interpolation): Consider $F[x]$ for a field F with ideals

$$I_1 = (x - a_1), I_2 = (x - a_2), \ldots, I_n = (x - a_n)$$

for a_i distinct. Note that these ideals are comaximal, since $I_1 + I_2$ contains $\frac{1}{a_2 - a_1}((x - a_1) - (x - a_2))$. Then,

$$\frac{F[x]}{(x - a_1)} \times \cdots \times \frac{F[x]}{(x - a_n)} \cong \frac{F[x]}{(x - a_1) \ldots (x - a_n)}.$$

So fixing a polynomial with $f(a_1) = b_1, \ldots, f(a_n) = b_n$ gives us a unique polynomial of degree $n - 1$.

5.12 Ring examples summarized

Things we care about:

(a) Ideals and prime ideals, is it PID?

(b) Integral domain.

(c) Division: is it a Euclidean domain?

(d) Factorization: is it a UFD?

Keep in mind

$$\text{Field} \implies \text{Euclidean domain} \implies \text{PID} \implies \text{UFD}.$$

Example (Integers):

(a) Ideals are $n\mathbb{Z}$, prime ideals are $p\mathbb{Z}$, so $\mathbb{Z}$ is PID.

(b) $\mathbb{Z}$ is an integral domain.

(c) $\mathbb{Z}$ is an Euclidean domain with absolute value as the norm. $\mathbb{Z}$ is UFD since it is Euclidean domain.

Example (Integer polynomials):

(a) Not PID, consider $(2, x)$.

(b) $\mathbb{Z}[x]$ is integral domain.

(c) $\mathbb{Z}[x]$ is not Euclidean domain, consider dividing x by $2x$.

(d) $\mathbb{Z}[x]$ is UFD since $\mathbb{Q}[x]$ is UFD ($\mathbb{Q}$ UFD) and factorization over rationals gives factorization over integers.

Can we do this in generality for ring R, field F?

Example (Gaussian integers):

6 Fields

6.1 Definitions and properties

Recall that a field is a ring with 1 where each element is a unit (so we can divide).

Proposition 43: The only ideals in a field F are (0) and F.

Proof. If an ideal contains a nonzero element a, it contains $aa^{-1} = 1$, which means it is F. □

Proposition 44: Ring homomorphisms between fields are either trivial or define a subfield relation.

Proof. Let $\phi : F \to L$ be a ring homomorphism between fields F, L. We have two cases: either $\ker \phi = F$, i.e. $\phi = 0$, or $\ker \phi = (0)$, which means ϕ is injective and $F \cong \phi(F)$, in which case L is an extension of F. □

Definition (Extension): If F is a subfield of K, we call K an *extension* of F. We write K/F.

Example: Let F be a field, and let $n = 1 + \cdots + 1$. If $n \neq m$ in F for any $n, m \in \mathbb{Z}$, then we have ring homomorphism

$$\phi : \mathbb{Z} \to F; n \mapsto 1 + \cdots + 1.$$

So there is a copy of $\mathbb{Z}$ in F.

On the other hand, if $n = m$ in F, then note that $n - m \in F$, so let us denote p as the minimum natural number that is 0 in F (necessarily prime). Then F contains a copy of $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (why?).

Definition (Characteristic of field): Let F be a field, define its *characteristic* as

$$char(F) = \begin{cases} p, & \text{if } \mathbb{F}_p \text{ is a subfield of } F; \\ 0, & \text{if } \mathbb{Q} \text{ is in } F. \end{cases}$$

We call $\mathbb{Q}$ and $\mathbb{F}_p$ *prime fields*.

Definition (Vector space over field): Let F be a field. A *vector space* over F is a set V with operations

(a) $+ : V \times V \to V$.

(b) $\cdot : F \times V \to V$.

such that for $\lambda, \lambda_1, \lambda_2 \in F$, $v, v_1, v_2 \in V$:

(a) $(V, +)$ is an abelian group.

(b) $(\lambda_1 \lambda_2)v = \lambda_1(\lambda_2 v)$.

(c) $1 \cdot v = v$.

(d) $(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$ and $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$.

Example:

(a) F^n is a vector space over F.

(b) $M_n(F)$ is a vector space over F.

Definition (Spanning): A set $S \subseteq V$ is *spanning* is every $v \in V$ can be written in the form $\lambda_1 s_1 + \cdots + \lambda_n s_n$ for some $\lambda_i \in F, s_i \in S$.

Definition (Linearly independent): A set $S = \{s_1, \ldots, s_n\} \subseteq V$ is *linearly independent* if

$$\lambda_1 s_1 + \cdots + \lambda_n s_n = 0 \implies \lambda_1 = \cdots = \lambda_n = 0.$$

Definition (Basis): A *basis* is a spanning and linearly independent set.

Definition (Dimension): Define $\dim_F V$ as the size of the basis. This depends on the fact that all bases have the same size (which is proved by showing the size of any spanning set is greater than the size of a linearly independent set).

Example (Dimension of vector spaces):

(a) $\dim_F F^n = n$.

(b) $\dim_F M_n(F) = n^2$.

(c) $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$ since $\{1, \sqrt{2}\}$ is spanning and linearly independent.

Definition (Degree of extension): If K/F is an extension, then K is a vector space over F. We define the *degree* of K/F as

$$|K/F| = \dim_F K.$$

Example (Extensions):

(a) $|\mathbb{Q}(\sqrt{2})/\mathbb{Q}| = 2$.

(b) $|\mathbb{C}/\mathbb{R}| = 2$.

(c) $|\mathbb{C}/\mathbb{Q}| = \infty$ (if finite, then $|\mathbb{C}| = |\mathbb{Q}^n|$ countable?).

6.2 Polynomial rings over fields

Proposition 45: Let F be a field and $f \in F[x]$ be an irreducible polynomial. Then

$$K \coloneqq \frac{F[x]}{(f)}$$

is a field that contains a copy of F and contains a root of f and has degree $\deg f$ over F.

Proof. First note that K is a field since $F[x]$ is PID so (f) is maximal.

Let $\phi : F \to K$ by $\phi(a) = a + (f)$. Since f is irreducible and F is a field, $\ker \phi = F \cap (f) = \varnothing$. Thus K extends F. We show $|K/F| = \deg f$ using $1, x, \ldots, x^{n-1}$ as a basis for the vector space of K over F. This is linearly independent, and if $g \in K$, the residue modulo (f) can be written in terms of the basis. Then note that

$$f(x + (f)) = f(x) + f((f)) = 0.$$

□

Example (Complex numbers): Let $F = \mathbb{R}$, $f = x^2 + 1$. Then,

$$\frac{\mathbb{R}[x]}{(x^2 + 1)}$$

is an extension of degree 2 where $x^2 + 1$ has a root (i).

We now prove that these extensions take the form of adjoining, which is where we usually see them. In other words, in the above example, we can define the root of $x^2 + 1$ as i and use representation $a + bi$ for the complex numbers.

Theorem: Let K/F be a field extension, f an irreducible polynomial in $F[x]$ but with root in K, $f(\alpha) = 0$. Then

$$\frac{F[x]}{(f)} \cong F(\alpha).$$

Proof. □

Example:

(a) Let $F = \mathbb{Q}, K = \mathbb{C}$, $f = x^3 - 2$. If f were reducible in $\mathbb{Q}[x]$, then f would be reducible in $\mathbb{Z}[x]$ by Gauss.

6.3 Algebraic extensions

Definition: Let K/F. An element $a \in K$ is *algebraic* over F if a is a root of a polynomial in $F[x]$. If a is not algebraic it is called *transcendental* over F. We call K/F *algebraic* if every element of K is algebraic over F.

Proposition 46: Let a be algebraic over F. There is a unique monic irreducible polynomial $m_a \in F[x]$ which has a as a root. Moreover a polynomial $f \in F[x]$ has α as a root if and only if m_a divides f in $F[x]$.

Proof. Consider the (scaled WLOG to monic) polynomial of minimal degree with a as a root. If there are multiple, then subtract to contradict minimiality of degree. Now suppose this unique minimal monic polynomial f isn't irreducible. So $f(x) = g(x)h(x)$ for g, h smaller degree than f. But then $f(a) = g(a)h(a) = 0$, meaning either $g(a)$ or $h(a)$ is 0 once again contradicting minimality of degree.

Now suppose $k(x)$ is a polynomial with a as a root. By Euclidean algorithm on $F[x]$,

$$k(x) = q(x)f(x) + r(x),$$

where r has smaller degree than k. But since $k(a) = q(a)f(a) + r(a)$, and k, f both have a as root, it follows that $r(a) = 0$, a contradiction. □

Proposition 47: Suppose a is algebraic over F. Then,

$$F(a) \cong F[x]/(m_a)$$

Proof. Since m_a is irreducible with root a in K, this follows by earlier theorem. □

Proposition 48: a is algebraic over F if and only if $F(a)/F$ is finite.

Proof. Suppose a is algebraic over F. The degree of $F(a)/F$ is the degree of m_a, which is finite. Suppose $F(a)/F$ is finite of degree n. Then, the elements

$$1, a, a^2, \ldots, a^n$$

are linearly dependent, i.e.

$$c_n a^n + \cdots + c_1 = 0.$$

This means the polynomial $f(x) = c_n a^n + \cdots + c_1$ has root a so a is algebraic over F. □

Proposition 49: Let $f, g \in F[x]$.

$$\deg fg = \deg f + \deg g.$$

Theorem (Tower of extensions): Suppose K/E and E/F. Then

$$[K : F] = [K : E][E : F].$$

Proof. Suppose $a_1, \ldots, a_n$ is a basis for K over E and $b_1, \ldots, b_m$ is a basis for E over F. Then,

$$\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a basis for K over F (omitted). □

Theorem: A field generated over F by a finite number of algebraic elements of degrees $n_1, \ldots, n_k$,

$$F(\alpha_1, \alpha_2, \ldots, \alpha_k)$$

is algebraic of degree $\leq n_1 \ldots n_k$.

Proof. Write

$$\begin{aligned}[F(\alpha_1, \ldots, \alpha_k) : F] &= [F(\alpha_1, \ldots, \alpha_k) : F(\alpha_2, \ldots, \alpha_k)] \ldots [F(\alpha_k) : F] \\ &\leq n_1 \ldots n_k,\end{aligned}$$

where since the minimal polynomial of α_i over F has degree n_i, and this is an admissible polynomial over $F(\alpha_{i+1}, \ldots, \alpha_k)$, the extension has degree at most n_i. □

Proposition 50: Let a, b algebraic elements in F. Then, by previous theorem,

$$ab, a + b, a/b, a - b \in F(a, b)$$

are all algebraic of degree $\leq mn$.

Definition (Algebraic numbers): Define

$$\overline{\mathbb{Q}} = \{r \in C : r \text{ is algebraic over } \mathbb{Q}\}$$

as the *field of algebraic numbers.*

Definition (Algebraically closed): A field F is *algebraically closed* if every every $f \in F[x]$ has a root in F.

Theorem (Fundamental theorem of algebra): $\mathbb{C}$ is algebraically closed.

Proof. TODO dummit □

6.4 Straightedge and compass constructions

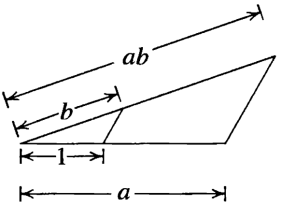
The Greeks proposed the following problems to be solved with straightedge and compass:

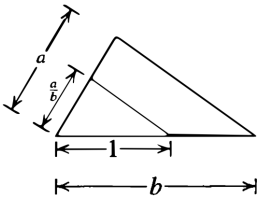
(a) Can we construct a cube with twice the volume of the first?

(b) Can we trisect an angle?

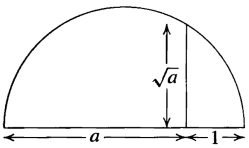
(c) Can we find a square whose area is that of a circle?

We show all to be false. Call a length constructible if we can make it with straightedge and compass starting from the unit distance. We first note that constructible elements are closed under addition, subtraction, multiplication, and division:





So given a collection of constructible elements, we can construct the subfield of $\mathbb{R}$ it generates, F. We can also take square roots of elements with



We can show that beginning with constructible coordinates from F, intersecting lines keeps coordinates in F and intersecting circles with lines or circles brings us to at most a quadratic extension of F. Since extension degrees are multiplicative:

Proposition 51: Let $\alpha \in \mathbb{R}$ be obtained from a finite number of straightedge and compass operations on F. Then

$$[F(\alpha) : F] = 2^k$$

for some $k \geq 0$.

Theorem (Greek problems are impossible):

Proof. Starting with a unit length equates to starting with field $\mathbb{Q}$.

(a) We cannot double the cube since

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

(b) If we can construct an angle θ, we can construct $\cos\theta, \sin\theta$. So we want to construct $\cos\frac{\theta}{3}$. Let $\theta = \pi/3$, then using triple angle and solving for $\frac{\theta}{3} = x$,

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3} \implies \frac{1}{2} = 4x^3 - 3x.$$

Solving for x reduces to a cubic extension which is bad by (a).

(c) We cannot square a circle since π is transcendental (proved later).

$$[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty.$$

□

Theorem: e is irrational.

Proof. Since

$$e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \ldots,$$

if we suppose $e = \frac{p}{q}$ then

$$p(q-1)! = q!e = q! + q! + \frac{q!}{2!} + \cdots + \frac{q!}{q!} + \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \ldots.$$

But the non integer portion is bounded by geometric series:

$$< \frac{1}{q},$$

a contradiction. □

Theorem (Lindemann): If $a \neq 0$ is algebraic then e^a is not.

Proof. Omitted. □

Theorem (Euler's formula): Plugging ix into e^x expansion formally,

$$e^{ix} = 1 + ix + \frac{(ix)^2}{2!} + \cdots = \cos x + i \sin x.$$

So by Lindemann, since $e^{\pi i} = -1$, we have that π is not algebraic.

6.5 Constructing n-gons

Lemma: Let $a, b \in \mathbb{R}$, $a^2 + b^2 = 1$. Then $\mathbb{Q}(a)/\mathbb{Q}$ is a degree 2^n extension iff, letting $z = a + bi$, $\mathbb{Q}(z)/\mathbb{Q}$ is a degree 2^m extension for some $m \in \mathbb{N}$.

Thus a n-gon is constructible only if defining

$$z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} = e^{i\frac{2\pi}{n}},$$

we satisfy $|\mathbb{Q}(z)/\mathbb{Q}| = 2^m$ for some m.

Proof. Suppose $|\mathbb{Q}(a)/\mathbb{Q}| = 2^n$. □

6.6 Splitting fields

Lemma: Let F be a field, f a polynomial in $F[x]$. Then there is an extension K/F such that f factors into linear factors in $K[x]$.

Proof. Let $d = \deg f$. Proceed by induction on d. When $d = 1$, we are done. Suppose it holds for d. If f factors into at least two irreducibles, we repeatedly apply the IH to the smaller degree irreducibles. Otherwise, if f is irreducible,

$$\frac{F[x]}{(f)}$$

is an extension of f containing a root of f, reducing to the former case. □

Definition (Splitting field): An extension K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if f factors completely into linear factors over $K[x]$ and f does not factor in this manner in any proper subfield of K containing F.

Definition (Cyclotomic fields): Define

$$\zeta_n \coloneqq e^{i\frac{2\pi}{n}}$$

as the first nth root of unity which generates all other roots $\zeta_n^2, \ldots, \zeta_n^n$. Then $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$ and is called the *cyclotomic field of the nth roots of unity.*

Note that in the case where p is prime, since

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1),$$

ζ_p is a root of the cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

Therefore $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$, and

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

6.7 Separability and finite fields

Recall that every field contains a prime subfield ($\mathbb{Q}$ or $\mathbb{F}_p$ for p prime). A finite field cannot have the former, so it must be that

$$|F/\mathbb{F}_p| = d < \infty$$

for some p. It follows that every finite field F satisfies $|F| = p^d$ for some positive integer d, and there is a basis $\alpha_1, \ldots, \alpha_d \in F$ such that every element in F is

$$c_1\alpha_1 + \cdots + c_1\alpha_d, c_1, \ldots, c_d \in \mathbb{F}_p.$$

Definition (Derivative): Let F be a field. The derivative of a polynomial in $F[x]$ is defined as

$$(x^n)' = nx^{n-1},$$

extended linearly.

Proposition 52:

(a) $(f+g)' = f' + g'$.

(b) $(cf)' = cf'$.

(c) $(fg)' = f'g + fg'$.

Lemma: Let F be a field and $f \in F[x]$ splits into linear factors. Then the following are equivalent:

(a) f has a repeated root.

(b) $\gcd(f, f')$ is not a unit.

Proof. Suppose f has a repeated root. Then

$$f = (x-a)^2 g \implies f' = 2(x-a)g + (x-a)^2 g'.$$

So both f, f' are divisible by $x - a$.

Conversely, there is a $x - a$ which divides both f and f':

$$f = (x-a)g, f' = (x-a)h.$$

Take derivative $f' = g + (x-a)g'$, so $(x-a) \mid g \implies (x-a) \mid f$. □

Remark: Let $f, g \in F[x]$, K/F. Then $\gcd(f, g)$ is the same both when computed in $F[x]$ and in $K[x]$.

Proof. The Euclidean algorithm computes gcd and uses only field operations. So, if all coefficients left are in F, then all intermediate results are in F. □

Definition (Separable polynomial): A polynomial f is separable over a field F if f has no repeated roots. By above, it suffices to check $\gcd(f, f') = 1$.

Example: Consider $x^n - 1$ with derivative nx^{n-1}. Then, over any field with characteristic not dividing n, the derivative only has one root 0 which is not shared with $x^n - 1$. So $x^n - 1$ is separable and there are n unique roots of unity.

Definition (Frobenius endomorphism): Let F be a field of characteristic p. The *Forbenius endomorphism* is the map $x \mapsto x^p$, an injective homomorphism $F \to F$:

$$(ab)^p = a^p b^p, (a+b)^p \equiv a^p + b^p \pmod{p}.$$

Theorem (Construction of finite fields): Let p be a prime, d a positive integer. Then there exists a unique field with p^d elements.

Proof. Define

$$f = x^{p^d} - x \in \mathbb{F}_p[x].$$

Let $K/\mathbb{F}_p$ in which f splits into p^d linear factors. Let L be the roots of f in K. $|L| = p^d$ since $f' = -1 \implies \gcd(f, f') = 1$. That L is a subfield follows directly from using the Frobenius endomorphism.

Now suppose we have any field F of p^d elements. Consider the abelian group $F^* = F \setminus \{0\}$. By Lagrange, for any element $a \in F$,

$$a^{p^d - 1} = 1 \implies a^{p^d} = a.$$

Thus F^* contains $p^d - 1$ distinct roots of $x^{p^d} - x$, and it follows that F is the splitting field of $x^{p^d} - x$ since in any proper subfield we lose a root. Since splitting fields of a polynomial are the same up to isomorphism (not shown), we are done. □

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

Proof. Suppose $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Then for some t, $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = t$, so

$$p^n = (p^m)^t \implies m \mid n.$$

Conversely, if $n = md$, then

$$p^n - 1 = (p^m - 1)(p^{m(d-1)} + p^{m(d-2)} + \cdots + 1).$$

Thus if a is a root of $x^{p^m} - x$ then

$$a^{p^m} = a \implies a^{p^m - 1} = 1 \implies a^{p^{n-1}} = 1,$$

so a is a root of $x^{p^n} - x$. Thus

$$(x^{p^m} - x) \mid (x^{p^n} - x).$$

It follows that the splitting field for $x^{p^m} - x$ is a subfield of the splitting field for $x^{p^n} - x$, meaning $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ as required. □

Theorem: In $\mathbb{F}_p$ there are irreducible elements of every degree.

Proof. Let F be a field with $|F| = p^d$ and define S as the elements of F not contained in any proper subfield $E \subseteq F$.

$$|S| \geq p^d - \sum_{e \mid d, e \neq d} p^e \geq p^d - (p^{d-1} + p^{d-2} + \cdots + p) = p^d - \frac{p^d - 1}{p - 1} + 1 > 0.$$

So there is an element $a \in F$ not contained in any proper subfield. In particular, $\mathbb{F}_p(a)$ cannot be any proper subfield of F so it is F. Then,

$$[\mathbb{F}_p(a) : \mathbb{F}_p] = d,$$

which means the minimal polynomial of a over $\mathbb{F}_p$ has degree d. Since this holds for arbitrary d we can construct irreducible elements of any degree. □