Symmetric Groups

★ Any cycle in S_n can be written as a product of r transpositions. $(-1)^r$ is sign (works for any permutation that can be written as product of transp.).

★ Given a permutation σ_1 and σ_2, to find π such that $\pi\sigma_1\pi^{-1} = \sigma_2$ line up cycles of the same length. Ex: $\sigma_1 = (12)(345)$ and $\sigma_2 = (123)(45)$

$$\pi\sigma_1\pi^{-1} = \pi(12)(345)\pi^{-1} = \pi(12)\pi^{-1}\pi(345)\pi^{-1}$$
$$= (\pi(1)\ \pi(2))(\pi(3)\ \pi(4)\ \pi(5))$$
$$\ \ \ \ \downarrow\ \ \ \ \ \ \downarrow\ \ \ \ \ \ \ \downarrow\ \ \ \ \ \ \downarrow\ \ \ \ \ \ \downarrow$$
$$\ \ \ \ 4\ \ \ \ \ \ 5\ \ \ \ \ \ \ 1\ \ \ \ \ \ 2\ \ \ \ \ \ 3$$

$$\pi = (14253) \text{ and } \pi^{-1} = (13524)$$

★ All cycles of the same length are conjugate

permutations conjugate $\Leftrightarrow$ they have same disjoint cycle structure.

Dihedral Groups

★ D_n is generated by r, s with $r^n = 1$, $s^2 = 1$, $srs^{-1} = r^{-1}$, and $|D_n| = 2n$.

r^k = rotation, $r^k s$ = reflection

★ $\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbb{Z}/n) = \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/n)^\times, b \in \mathbb{Z}/n\right\}$

★ $N \trianglelefteq D_n \Rightarrow D_n/N = D_k$ for some k.

Conjugacy Classes:

- n is odd:
  - $\{1\}$
  - $(n-1)/2$ classes of size 2: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm (n-1)/2}\}$
  - all reflections: $\{r^i s : 0 \le i \le n-1\}$
- n is even:
  - 2 classes of size ~~{1}~~: $\{1\}, \{r^{n/2}\}$
  - $\frac{n}{2} - 1$ classes of size 2: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(\frac{n}{2}-1)}\}$
  - all reflections are in 2 classes: $\{r^{2i}s : 0 \le i \le \frac{n}{2} - 1\}$
    $\{r^{2i+1}s : 0 \le i \le \frac{n}{2} - 1\}$

Semidirect Products

- If $p<q$ and $q \not\equiv$ mod p, then all groups $|G|=pq$ are cyclic.
- $G \cong H \rtimes_{\varphi} K$ with $\varphi_k(h) = khk^{-1}$ if:
  - $G = HK$
  - $H \cap K = \{1\}$
  - $H \trianglelefteq G$.
- If $p<q$ and $q \equiv 1 \bmod p$, then two groups $|G|=pq$: one cyclic, one nonabelian.

Finite Abelian Groups

- If G is a finite abelian group, then $G \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2} \times \dots \times \mathbb{Z}/p_n^{k_n}\mathbb{Z}$ where $p_i^{k_i} \mid |G|$
- If G is a finitely generated abelian group, then $G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ where $\mathbb{Z}^r = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{r \text{ times}}$, and $r, n_i \in \mathbb{Z}$ $(i \in \{1, \dots, k\})$ such that $r \geq 0$, $n_i \geq 2$ and $n_{i+1} \mid n_i$ $(i \in \{1, \dots, k\})$.

Conjugacy Classes

- $g, h \in G$ conjugate when $g = xhx^{-1}$ for some $x \in G$.
- Conjugacy class of g: $\{xgx^{-1} : x \in G\}$ (all elements conjugate to g).
- All elements in a conjugacy class have the same order.
  $|\{xgx^{-1} : x \in G\}| = [G : Z(G)]$
- Class equation: $|G| = |Z(G)| + \sum_k \frac{|G|}{|Z(g_k)|}$.

Cauchy's Theorem

- Let G be a finite group and p be a prime factor of $|G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of order p.

Group Actions

- Action of G on a set X: $g \cdot x$ is such that:
  $e \cdot x = x \ \forall x \in X$ where e is identity in G
  $g_1 \cdot (g_2 \cdot x) = g_1 g_2 \cdot x \ \forall g_1, g_2 \in G \ \forall x \in X$.
- Can be thought of as homomorphisms: $\varphi : G \to \mathrm{Sym}(X)$
- $\mathrm{Orb}_x = \{g \cdot x : g \in G\} \subset X$ and $\mathrm{Stab}_x = \{g \in G : g \cdot x = x\} \subset G$
  "orbit" "stabilizer"
- Orbit-Stabilizer formula: $|\mathrm{orb}_x| = [G : \mathrm{Stab}_x]$
- Different orbits are disjoint and form a partition of X.
- For each $x \in X$, Stab_x is a subgroup of G and $\mathrm{Stab}_{gx} = g\,\mathrm{Stab}_x\,g^{-1} \ \forall g \in G$.
- $\mathrm{Fix}_g(x) = \{x \in X : gx = x\}$ "elements fixed by g"
- Fixed point congruence: Let G be a finite p-group.
  $|X| \equiv |\{\text{Fixed points}\}| \mod p$
- Nontrivial p-groups have nontrivial center.
- Every subgroup of a p-group with index p is normal.

Sylow Theorems

- A subgroup whose order is the highest power of a prime p dividing $|G|$ is a p-Sylow subgroup of G.
- Sylow I: A finite group G has a p-Sylow subgroup for every prime p and each p-subgroup of G lies inside a p-Sylow subgroup of G.
- Sylow II: For each prime p, p-Sylow subgroups of G are conjugate.
- Sylow III: For each p, let n_p be the number of p-Sylow subgroups of G.
  If $|G| = p^k m$ with $p \nmid m$, then $n_p \equiv 1 \mod p$ and $n_p \mid m$.
- Sylow III*: $n_p = [G : N(P)]$ where P is a p-Sylow subgroup and $N(P)$ is its normalizer.
- To prove the Sylow theorems, use fixed point congruence and group actions.
- $n_p = 1 \Rightarrow$ a p-Sylow subgroup is normal.
- If $p \neq q$ and p, q prime and $n_p = n_q = 1$, then the elements of the p-Sylow subgroup commute with the elements of the q-Sylow subgroup.

Ideals

* An ideal of a ring is an additive subgroup $I \subset R$ such that $RI \subset I$ and $IR \subset I$.
* The only ideals in a field are (0) and (1).
* Ideals of R are kernels of ring homomorphisms (analogus to first isom thm)
* An ideal $I \subset R$ is prime if the quotient ring R/I is an integral domain. We call I a maximal ideal if R/I is a field.
* An ideal $I \subset R$ is prime $\Leftrightarrow$ $I \neq R$ and $\forall a, b \in R$ we have $ab \in I \Rightarrow a \in I$ or $b \in I$.
* An ideal $I \subset R$ is maximal $\Leftrightarrow$ $I \neq R$ and if an ideal J of R is such that $I \subset J \subset R$, then $J = I$ or $J = R$.
* If R is a PID, then all nonzero prime ideals are maximal.
* Every nonzero commutative ring has a maximal ideal.

Properties of Rings

* Characteristic: Smallest positive $n \in \mathbb{Z}$ such that $1^n = 0$ in a ring R. If no such $n \in \mathbb{Z}$ exists, the characteristic is said to be 0.
* Nilpotent: $a^m = 0$ for some $m \geq 1$.
* $\{\text{Nilpotents in } R\} = \bigcap_{\substack{\text{prime ideals} \\ P \subset R}} P$
* Isomorphic rings must have same number of nilpotent elements.
* If $f: R \to \tilde{R}$ is a surjective ring homomorphism, then $f(R)$ is a subring of R and there is an isomorphism $\tilde{f}: R/\ker(f) \to \tilde{R}$ by $\tilde{f}(a \bmod \ker(f)) = f(a)$.
* For an ideal $I \subset R$ and subring $R' \subset R$, $R' + I$ is a subring. I is an ideal in $R' + I$ and $(R' + I)/I \cong R'/(R' \cap I)$.
* The ideals in R/I are uniquely J/I for ideals J with $I \subset J \subset R$ and $(R/I)/(J/I) \cong R/J$.
* Zorn's lemma: Let S be a partially ordered set. If every totally ordered subset of S has an upper bound in S, then S contains a maximal element.
* Field $\Rightarrow$ Euclidean domain $\underset{\text{minimality of norms}}{\Rightarrow}$ PID $\underset{\text{contradiction for existence, direct for uniqueness}}{\Rightarrow}$ UFD $\Rightarrow$ Integral domain

* Generalized Chinese Remainder Theorem for rings: For a commutative ring R with ideals I and J such that $I+J=R$, then $R/I\cap J \cong R/I \times R/J$ given by $(a \bmod I\cap J) \longmapsto (a \bmod I, a \bmod J)$.
* Euclidean domain: Division w/ remainder exists with $N(r)<N(b)$ or $r=0$ when $a=bq+r$. $N: R \to \mathbb{N}-\{0\}$ is Euclidean function.
* Principal ideal domain (PID): All ideals principal, in other words, have the form (m) for some $m\in R$.
* Unique factorization domain (UFD): Every $a\neq 0, \neq$ unit in R has a factorization $a=p_1p_2\cdots p_k$ where p_i are irreducible. If it is such that $p_1p_2\cdots p_k = q_1q_2\cdots q_\ell$ with p_i, q_j all irreducible, then $k=\ell$ and after relabelling $q_i = u_ip_i$ (u_i is a unit).
* A unit $a\in R^\times$ is such that $N(a)=\pm 1$. Call $a\in R$ irreducible if $a\neq 0, \neq$ unit and whenever $a=bc$ in R, b or c is a unit (the other is a unit multiple). Otherwise, call $a\in R$ reducible.
* Call $p\in R$ prime if $p\neq 0, \neq$ unit and whenever $p\mid xy$ in R, $p\mid x$ or $p\mid y$ (equivalently, (p) is a prime ideal in R).
* In all integral domains: prime $\Rightarrow$ irreducible
* In PID: prime $\Leftrightarrow$ irreducible
* In UFD: prime $\Leftrightarrow$ irreducible
* Ring of fractions: Consider all pairs (a,b) of $a,b\in A$, $b\neq 0$ and set $(a,b)\sim(c,d) \Leftrightarrow ad=bc$ in A. Next, set $K = \{\overline{(a,b)} \in A\times(A-\{0\})\}$
$= \{\overline{(a,b)} : a,b\in A, b\neq 0\}$

To make K a field: $\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)}$
$\overline{(a,b)}\cdot\overline{(c,d)} = \overline{(ac, bd)}$

Polynomial Rings

* $A[X]$ is the ring of all polynomials in X with coefficients in the comm. ring A.
* $A[X]$ integral domain $\Leftrightarrow$ A integral domain.
* If F is a field, then $F[X]$ is a Euclidean domain.
* Similarly, if A is a nonzero comm. ring, then for $f,g\in A[X]$ with g monic, there are unique $q,r\in A[X]$ such that (1) $a=bq+r$, (2) $r=0$ or $\deg(r)<\deg(g)$.
($\therefore$ $A[X]$ not Euclidean domain).

* In $\mathbb{Z}[\sqrt{d}]$ ($d \in \mathbb{Z}$, d squarefree), and $N(\alpha) = \pm p$ for a prime p, then α is irreducible in $\mathbb{Z}[\sqrt{d}]$. Moreover, if $\pi \in \mathbb{Z}[\sqrt{d}]$ is prime, then $\pi | p$ for prime p and $N(\pi) = \pm p$ or $N(\pi) = \pm p^2$.

* In $\mathbb{Z}[\sqrt{d}]$, if $\alpha \in \mathbb{Z}[\sqrt{d}]$ with $\alpha = x + y\sqrt{d}$, then $N(\alpha) = x^2 - dy^2$. Therefore, if the equation $x^2 - dy^2 = \pm z$ has no solution z, then there cannot exist an element $\beta \in \mathbb{Z}[\sqrt{d}]$ with $N(\beta) = \pm z$.

* Call a polynomial $f(x) \in \mathbb{Z}[x]$ <u>primitive</u> if gcd(coeffs of f) = 1. A primitive polynomial is irreducible in $\mathbb{Z}[x]$ $\Leftrightarrow$ irreducible in $\mathbb{Q}(x)$.

* If R is a UFD, then $R[x]$ is a UFD.

* <u>Irreducibility Tests for polynomials</u>:
  1) If $f(x) \in R[x]$ is monic and $\deg(f) = 2$ or 3, then f is irreducible in $R[x]$ $\Leftrightarrow$ f has no roots in R.
  2) <u>Reduction mod p test ($\mathbb{Z}[x]$)</u>: $f(x) \in \mathbb{Z}[x]$ is monic. If there is a prime $p \in \mathbb{Z}$ such that $f(x) \bmod p \in (\mathbb{Z}/p)[x]$ is irreducible in $\mathbb{Z}/p$, then $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$.
  3) <u>Eisenstein Criterion ($\mathbb{Z}[x]$)</u>: Call a monic $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ in $\mathbb{Z}[x]$ Eisenstein at prime p if $c_i \equiv 0 \bmod p$ $\forall i \in \{0, \ldots, n-1\}$ and $c_0 \not\equiv 0 \bmod p^2$. Every Eisenstein polynomial in $\mathbb{Z}[x]$ is irred. in $\mathbb{Z}[x]$.
  4) <u>Reduction mod $\mathfrak{p}$ test (general)</u>: Let R be a domain and $\mathfrak{p}$ a nonzero prime ideal in R. If $f(x) \in R[x]$ is monic and reduction $\bar{f}(x) \in (R/\mathfrak{p})[x]$ is irreducible in $(R/\mathfrak{p})[x]$, then $f(x)$ is irreducible in $R[x]$.
  5) <u>Eisenstein criterion (general)</u>: Let R be a domain and $\mathfrak{p}$ a nonzero prime ideal in R. Call a monic poly. $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 \in R[x]$ Eisenstein at $\mathfrak{p}$ if $c_i \equiv 0 \bmod \mathfrak{p}$ ($c_i \in \mathfrak{p}$ $\forall i$) and $c_0 \not\equiv 0 \bmod \mathfrak{p}^2$. All Eisenstein polynomials in $R[x]$ are irreducible.

  [Note: $\mathfrak{p}^2 = \left\{ \sum_{i=1}^{k} a_i b_i : k \geq 1,\ a_i \in \mathfrak{p},\ b_i \in \mathfrak{p} \right\}$]

Vector Spaces

* A vector space V over a field F is an abelian group V with a scaling map $F \times V \to V$, $(c,v) \mapsto cv$, that's compatible with $+$ in V and $+, \times$ in F. Also:

$$\left.\begin{array}{l} 1)\ c(v+v') = cv + cv' \\ 2)\ (c+c')v = cv + c'v \\ 3)\ (cc')v = c(c'v) \end{array}\right\} \forall c, c' \in F \text{ and } \forall v, v' \in V.$$

* Given any finite subset $\{v_1, \dots, v_n\} \subset V$, its span is $\text{Span}(v_1, \dots, v_n) = \{c_1 v_1 + \dots + c_n v_n : c_i \in F\}$. A finite subset $\{w_1, \dots, w_m\}$ is linearly independent when $c_1 w_1 + \dots + c_m w_m = 0 \Rightarrow c_i = 0\ \forall i \in \{1, \dots, m\}$.

* If $\mathcal{B}$ and $\mathcal{C}$ are bases of V and W, then $L: V \to W$ linear, the dual $L^*: W^* \to V^*$ satisfies $[L^*]_{\mathcal{C}^*}^{\mathcal{B}^*} = ([L]_{\mathcal{B}}^{\mathcal{C}})^T$ with $\mathcal{B}^*, \mathcal{C}^*$ dual bases.

* For $\dim(V) < \infty$, we have $V \cong V^{**}$ by $v \mapsto ev_v$ (V^{**} = dual space of the dual space of V)

* $[L^{**}]_{\mathcal{B}^{**}}^{\mathcal{C}^{**}} = [L]_{\mathcal{B}}^{\mathcal{C}}$ (double dual of linear map L)

* $\text{Tr}(L) = \text{Tr}([L]_{\mathcal{B}}^{\mathcal{B}})$ and $\det(L) = \det([L]_{\mathcal{B}}^{\mathcal{B}})$.

* Trace is linear, determinant is multiplicative. Also: $\text{Tr}(AB) = \text{Tr}(BA)$, $\text{Det}(AB) = \text{Det}(A)\text{Det}(B)$.

* Inner product: $\langle , \rangle : V \times V \to \mathbb{R}$ such that $\langle , \rangle$ is bilinear, symmetric, and positive-definite.

* Given a linear map A, its adjoint A^* is such that $\langle Av, w \rangle = \langle v, A^* w \rangle$. If $A = A^*$, then A is self-adjoint.

* Spectral Theorem: For a real vector space V with $\dim(V) < \infty$ with an inner product $\langle , \rangle$ and linear map $A: V \to V$ that is self-adjoint with respect to $\langle , \rangle$, there's a basis of eigenvectors for A in V that is orthogonal:

$$V = \sum_{i=1}^{N} \mathbb{R} v_i, \text{ where } \langle v_i, v_j \rangle = 0\ \forall i \neq j \text{ and } A v_i = \lambda_i v_i \ (\lambda_i \in \mathbb{R}).$$

* A basis $\{e_1, \dots, e_n\} \subset V$ is orthonormal $\Leftrightarrow \langle e_i, e_j \rangle = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$.