Notes

Group Theory

Sylow Theorems: Write $\abs{G} = p^n m$ where $m {\notdivides} p$, S_p a sylow$\dash p$ subgroup, and n_p the number of sylow$\dash p$ subgroups.

- $\forall p^n \divides \abs{G}$, there exists a subgroup of size p^n.
    - Corollary: $\forall p \divides \abs{G}$, there exists an element of order p.
- All sylow$\dash p$ subgroups are conjugate for a given p.
    - Corollary: $n_p = 1 \implies S_p \normal G$
- $n_p \divides m$
- $n_p \equiv 1 \mod p$
- $n_p = [F : N(S_p)]$ where N is the normalizer.

Useful facts:

- $\ZZ_p, \ZZ_q \subset G \implies \ZZ_p \intersect \ZZ_q = \ZZ_{(p,q)}$, so coprime order subgroups are disjoint.
- $(p, q) = 1 \implies \ZZ_p \times \ZZ_q \cong \ZZ_{pq}$
- Characterizing direct products: $G \cong H \times K$ when
    - $G = HK = \theset{hk \suchthat h\in H, k\in K}$
    - $H\intersect K = \theset{e} \subset G$
    - $H, K \normal G$
        - Can relax to only $H\normal G$ to get a semidirect product instead

Semidirect Products:

$G = N \semidirect_\phi H$ where $$ \phi: H \to \Aut(N) \\ h \mapsto h(\wait)h^{-1} $$

Note $\Aut(\ZZ_n) \cong (\ZZ^n)\units \cong \ZZ^{\varphi(n)}$ where φ is the totient function.

Class Equation: \[\abs{G} = \abs{Z(G)} + \sum_{\substack{\text{One x_i from} \\ \text{each conjugacy class}}} [G: C_G(x_i)] \] where \(C_G(x)\) is the centralizer of \(x\), given by \(C_G(x) = \theset{g \suchthat [g, x] = e}\).

Fields: \(GF(p^n)\) is obtained as \(\displaystyle\frac{\FF_p}{\generators{f}}\) where \(f \in \FF_p[x]\) is irreducible of degree \(n\).

Eisenstein's Criterion: If \(f(x) = \sum_{i=0}^n \alpha_i x^i \in \QQ[x]\) and \(\exists p\) such that both \(p\notdivides a_n\) and \(p^2 \notdivides a_0\) but \(p \divides a_{i\neq n}\), then \(f\) is irreducible.

Linear Algebra

Finding the minimal polynomial \(m(x)\) of \(A\):

1. Find the characteristic polynomai \(\chi(x)\); this annihilates \(A\) by Cayley-Hamilton. Then \(m(x) \mid \chi(x)\), so just test the finitely many products of irreducible factors.
2. Pick any \(\vector v\) and compute \(T\vector v, T^2\vector v, \cdots T^k\vector v\) until a linear dependence is introduced. Write this as \(p(T) = 0\); then \(\chi(x) \ p(x)\).

Proof that when \(A_i\) are diagonalizable, \(\theset{A_i}\) commutes \(\iff A,B\) are simultaneously diagonalizable: induction on number of operators

- \(A_n\) is diagonalizable, so \(V = \bigoplus E_i\) a sum of eigenspaces
- Restrict all \(n-1\) operators \(A\) to \(E_n\).
    - The commuted in \(V\) so they commute here too
    - (Lemma) They were diagonalizable in \(V\), so they're diagonalizable here too
    - \(\implies\) they're simultaneously diagonalizable by I.H.
- But these eigenvectors for the \(A_i\) are all in \(E_n\), so they're eigenvectors for \(A_n\) too.
- Can do this for each eigenspace. \(\qed\)
- Full Details: here