Title

D. Zack Garza

August 27, 2019

Contents

1 Notes

1.1 Group Theory

Sylow Theorems: Write $|G| = p^n m$ where $m \not| p$, S_p a sylow-p subgroup, and n_p the number of sylow-p subgroups.

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

Useful facts:

- $\mathbb{Z}_p, \mathbb{Z}_q \subset G \implies \mathbb{Z}_p \bigcap \mathbb{Z}_q = \mathbb{Z}_{(p,q)}$, so coprime order subgroups are disjoint.
- $(p, q) = 1 \implies \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$
- Characterizing direct products: $G \cong H \times K$ when
  - $G = HK = \{hk \ni h \in H, k \in K\}$
  - $H \bigcap K = \{e\} \subset G$
  - $H, K \trianglelefteq G$
    - Can relax to only $H \trianglelefteq G$ to get a semidirect product instead

Semidirect Products:

$G = N \rtimes_\phi H$ where

$$\begin{aligned} \phi : H &\to \mathrm{Aut}(N) \\ h &\mapsto h(\,\cdot\,)h^{-1} \end{aligned}$$

Note $\text{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}^n)^\times \cong \mathbb{Z}^{\varphi(n)}$ where φ is the totient function.

Class Equation:

$$|G| = |Z(G)| + \sum_{\substack{\text{One } x_i \text{ from} \\ \text{each conjugacy class}}} [G : C_G(x_i)]$$

where $C_G(x)$ is the centralizer of x, given by $C_G(x) = \{g \ni [g,x] = e\}$.

Fields: $GF(p^n)$ is obtained as $\dfrac{\mathbb{F}_p}{\langle f \rangle}$ where $f \in \mathbb{F}_p[x]$ is irreducible of degree n.

Eisenstein's Criterion: If $f(x) = \sum_{i=0}^{n} \alpha_i x^i \in \mathbb{Q}[x]$ and $\exists p$ such that both $p \not\big| a_n$ and $p^2 \not\big| a_0$ but $p \,\Big|\, a_{i \neq n}$, then f is irreducible.

1.2 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 $\mathbf{v}$ and compute $T\mathbf{v}, T^2\mathbf{v}, \cdots T^k\mathbf{v}$ until a linear dependence is introduced. Write this as $p(T) = 0$; then $\chi(x)\ p(x)$.

Proof that when A_i are diagonalizable, $\{A_i\}$ 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. $\square$
- Full Details: here