Main topics relevant to the second exam.

Thursday, November 20, 2014
6:45 PM

Elementary Arithmetic:

- Division algorithm.
- $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$.
- $a \mid bc$ and $\gcd(a,b) = 1 \Rightarrow a \mid c$
- Unique factorization and v_p.
- Congruences and $\mathbb{Z}_n$
- Group of units $\mathbb{Z}_n^\times$.
- Chinese Remainder Theorem
- $\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $[a]_{mn} \longmapsto ([a]_m, [a]_n)$

  is a well-defined bijection. It is also a homomorphism
- Euler φ function:
  - $\varphi(mn) = \varphi(m)\varphi(n)$ if $\gcd(m,n) = 1$.
  - $\varphi(p^k) = p^k - p^{k-1}$.

Group theory:

- Definition, uniqueness of the identity and inverse of an element.

- Subgroup criteria.
- Group generated by a set.
- Cyclic groups:

* Any subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$ where either $d=0$ or d is the smallest positive number of this subgroup.

In particular any subgroup of $\mathbb{Z}$ is cyclic.

* Let $G=\langle g\rangle$.

- $I_0 := \{n\in\mathbb{Z} \mid g^n=e\}$ is a subgroup of $\mathbb{Z}$.
- If $|G|<\infty$, then $I_0 = |G|\,\mathbb{Z}$.

* Order $o(g)$ of g.

* Important properties of order:

- $\mathbb{Z}_{o(g)} \to \langle g\rangle$, $[m]_{o(g)} \longmapsto g^m$ is well-defined bijection. It is also a homomorphism
- $o(g) = |\langle g\rangle|$.
- $g^n = g^m \iff n\equiv m \pmod{o(g)}$.
- $o(g^m) = \dfrac{o(g)}{\gcd(o(g),m)}$.

- $\left.\begin{array}{l} ab=ba \\ \gcd(o(a),o(b))=1 \end{array}\right\} \Rightarrow o(ab)=o(a)\,o(b)$

- A finite group G is cyclic

$$\Updownarrow$$

$$\exists\, g\in G\ ,\quad o(g)=|G|.$$

- Group Actions.
  - Orbits: TFAE ① $x_1\in O(x_2)$
    ② $O(x_1)\cap O(x_2)\neq\emptyset$
    ③ $O(x_1)=O(x_2)$.
  - $G\backslash X := \{O(x)\mid x\in X\}$ is a partition.
  - Lagrange Theorem $|G|=|H|\,|H\backslash G|$ if $H\leq G$ and G is a finite group.
  - Index of H in G $=[G:H]=|H\backslash G|$.
  - $H\backslash G \longrightarrow G/H \quad Hg\longmapsto g^{-1}H$ is a well-defined bijection.
  - $G \curvearrowright X\ ,\ x\in X \Rightarrow$

    ① $G_x:=\{g\in G\mid g\cdot x=x\}\leq G$.

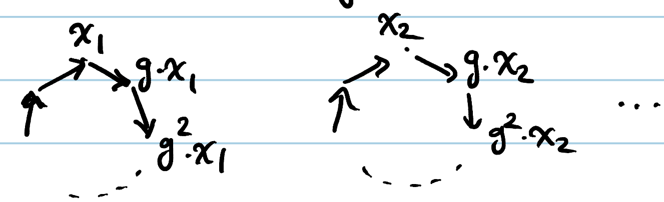
    ② $G/G_x \longrightarrow O(x)$

$$gG_x \longmapsto g\cdot x$$

is a well-defined bijection.

③ $|O(x)| = [G : G_x]$.

- How to understand the action of a finite cyclic group via Schreier cycles.



The vertices in each cycle give us an orbit of $\underline{\langle g \rangle}$. So their size divide $o(g)$.

- $H \curvearrowright G$ left multiplication: orbits are called right cosets
- $G \curvearrowright G$ by conjugation: orbits are called conjugacy classes.

• Symmetric Group:

- Any permutation can be uniquely written as a product of disjoint cycles.

- Any permutation is a product of transpositions.

- Even and odd permutation.
- $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ and A_n
- Two important equations:

$$(a_1, a_2, \cdots, a_n)\circ(a_n, a_{n+1}, \cdots, a_{n+k})$$
$$= (a_1, a_2, \cdots, a_n, a_{n+1}, \cdots, a_{n+k})$$

and $\tau \cdot (a_1, a_2, \cdots, a_n) \cdot \tau^{-1} = (\tau(a_1), \cdots, \tau(a_n))$

- $o(C_1 \cdot C_2 \cdot \cdots \cdot C_n) = \operatorname{lcm}(k_1, k_2, \cdots, k_n)$

where C_i are disjoint k_i-cycles.