Math 113

Ernest L

May 10, 2024

1 Details and definitions to remember

- Endomorphism: A <u>homomorphism</u> from a group to itself.
- Automorphism: An <u>isomorphism</u> from a group to itself.
- An ideal is characterized by the absorbing property: $a \in I, r \in R \implies ra \in I$
- Normal subgroup: $gH = Hg$ for all $g \in G$
- Think of ideals, normal subgroups as kernels of homomorphisms.
  - We can use these to take quotient groups
  - The first isomorphism theorem says: $G/\ker\Phi \cong \textbf{image}(\Phi : G \to H)$
- An integral domain occurs iff $ab = 0 \implies a = 0$ (no zero factors) or $b = 0$ which occurss iff $ca = cb \implies a = b$ (cancellation) (these are equivalent conditions)
- Correspondence theorem: $N \triangleleft G$, $N \subseteq K \subseteq G$ then $K/N \triangleleft G/N$ and $(G/N)/(K/N) \cong G/K$
- prime ideal: $ab \in I \implies a \in I$ or $b \in I$
- The quotient ring: R/I is an integral domain if and only if I is a prime ideal.
  - Proven by setting a product equal to 0 for integral domains
- The quotient ring: R/I is a field if and only if I is a maximal ideal.
  - Proven by using the fact that I is maximal ideal $\iff \forall P$ such that $I \subseteq P \subseteq R$, either $P = I$ or $P = R$
- Maximal ideals come from irreducible polynomials or prime numbers
- Burnsides Lemma: If G acts on a set X, then the number of orbits is given by: $\frac{1}{|G|}\sum_{g\in G}|X^g|$, where X^g is the set of elements fixed by g.
- Lagrange's theorem: If H is a subgroup of G, then $|H|$ divides $|G|$
  - proven by constructing bijection between cosets, all cosets equal and partition
  - Corrallary: For a normal subgroup H, the number of cosets is $|G|/|H|$

2 Some results

- Every ideal of a Euclidean domain is principal:
  - A Euclidean domain is an integral domain ring with an associated "order" function N. such that $N(0) = 0$. where every element can be divided with a unique quotient and remainder. Formally, for integral domain I, for all $a \in I$ and $b \in I \backslash 0$, there exists $q, r \in I$ such that $a = bq + r$ and $N(r) < N(b)$. We define N as a function that represents the size.
  - A principal ideal is one generated by a single element
  - If the ideal is just the zero element, then it is trivially principal
  - Proof: Let $b \in I$ be nonzero with $N(b)$ minimal. Now, observe that we can express $a \in I$ as $a = bq + r$, such that $N(r) < N(b)$. The only way to not contradict the fact that $N(b)$ is minimal is to have $N(r) = 0$, but then this implies that $a = bq$ which is what it means to be a principal domain.