Class notes

Fields

Theorem: R/I integral domain $\iff$ I prime ideal. R/I field $\iff$ I maximal ideal.

Field:

- A ring where every nonzero element has a multiplicative inverse.
- A ring whose only ideals are R and $\{0\}$
- A ring with division and commutativity

Common Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ where p is prime, $Q[\sqrt{2}]$, $\mathbb{Q}[\sqrt{D}]$ if D is not a perfect square

A set V is a vector space over a field F if it satisfies the following axioms:

1. V is abelian group under addition
2. $(a+b)\vec{v} = a\vec{v} + b\vec{v}, \quad \forall a, b \in F, \vec{v} \in V$
3. $a(\vec{v} + \vec{w}) = a\vec{v} + a\vec{w}, \quad \forall a \in F, \vec{v}, \vec{w} \in V$
4. $(ab)\vec{v} = a(b\vec{v}), \quad \forall a, b \in F, \vec{v} \in V$

Basis: $\{v_i\}$ is an independent spanning set

- Independent: $\sum_{i=1}^{n} a_i \vec{v}_i = 0 \implies a_i = 0, \forall i$
- Spanning: If every $v \in V$ is a linear combo of $\{v_i\}$

Example: $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$

Theorem: If V has a finite basis, all bases have the same number of elements $(\dim V)$

Theorem: All ideals in $F[x]$ are principal

Irreducible: $p(x) \in F[x]$ is irreducible if $p(x) = a(x)b(x) \implies a(x)$ or $b(x)$ is a constant.

Theorem: If $p(x) \in F[x]$ is irreducible, $I = p(x)F[x]$ is maximal

Theorem: $F[x]/p(x)F[x]$ is a field

Theorem: $F[x]/p(x)F[x]$ contains a root of $p(x)$

Theorem: If $F \subset K \subset L$, then

$$[L : F] = [L : K][K : F]$$

Groups

Normal: $H \trianglelefteq G$ if

$$H = aHa^{-1} \iff a^{-1}Ha = H \iff a^{-1}Ha \subset H$$

- All subgroups of an abelian group are normal
- Any group is a normal subgroup of itself

Quotient group: $G/N = \{gN : g \in G\}$ and

$$aN \cdot bN = ab \cdot N$$

Cayley's Theorem: Every group is isomorphic to a subgroup of a symmetric/permutation group

Lemma: two orbits are identical or disjoint

Abelian Cauchy: If G abelian and $p \mid G$, G has an element of order p

Cauchy Theorem: Every finite group with $p \mid |G|$ has an element of order p

Proposition: $|H| = p^n$ has a subgroup of order p^m for any $m \leq n$

Textbook Facts

Fields

Proposition: If F, K fields, $\phi : F \to K$ is a ring homomorphism, then ϕ is injective.

Extension field: $F \subset K \subset L$ $K = F(a_1, \ldots, a_n)$ is the smallest subfield of L containing $a_1, \ldots, a_n$.

Theorem: For $L/K/F$,

$$[L : F] = [L : K][K : F]$$

Polynomial degree: $\deg(f_1 f_2) = \deg(f_1) + \deg(f_2)$

Characteristic of a Ring: the integer generating the kernel of $\phi : \mathbb{Z} \to R$. If ϕ not injective, the smallest m such that $m\alpha = 0$ for all $\alpha \in R$.

Proposition: the order of a finite field of Characteristic p is some power of p.

Theorem: p prime and $d \geq 1$, $\mathbb{F}_p[x]$ contains an irreducible polynomial of degree d

Theorem: There exists a field F containing exactly p^d elements $(d \geq 1)$ and any two fields containing p^d elements are isomorphic.

Groups

If G abelian, every subgroup is normal

Every group has at least two normal subgroups: $\{e\}$ and G

Simple group: a group whose only normal subgroups are $\{e\}$ and G

Proposition: any group of prime order is simple

Proposition: $\phi : G_1 \to G_2$ is a group homomorphism, $\ker \phi \trianglelefteq G_1$

Normality:

1. $H \trianglelefteq G$ if $gHg^{-1} \subseteq H, \forall g \in G$
2. $\forall g \in G, \{gHg^{-1}\} \trianglelefteq G$
3. there is an isomorphism $H \to g^{-1}Hg$

Isomorphism theorem: If $\phi : G_1 \to G_2$ is a group homomorphism with $\ker\phi = N$, then $G_1/\ker\phi \cong \mathrm{Im}(\phi)$

Corrolary:
$$\frac{\#G}{\#\ker(\phi)} = \#\mathrm{Im}(\phi)$$

Group action: G group, X set, $\phi : G \times X \to X$ such that

1. *Identity:* $e \cdot x = x \quad \forall x \in X$
2. *Associtivity:* $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$

Remark: Defining an action G on X is equivalent to a homomorphism $\alpha : G \to S_X$ where S_X is the set of permutations on X and $\alpha(g) : X \to X$ with $g \cdot x = \alpha(g)(x)$

Orbit: $Gx = \{g \cdot x : g \in G\}$

Stabilizer: $G_x = \{g \in G : g \cdot x = x\}$

Proposition:
$$|Gx| = \frac{|G|}{|G_x|}$$

Transitive action: $Gx = X \quad \forall x \in X$

Orbit Stabilizer Counting TheoremL G, X finite $Gx_1, \ldots,\ Gx_k$ distinct orbits,
$$|X| = \sum_{i=1}^{l} |Gx_i| = \sum_{i=1}^{K} \frac{|G|}{|G_{x_i}|}$$

Theorem: $|G| = p^n$, then $Z(G) \neq \{e\}$

Conjugation action: $g \cdot x = gxg^{-1} \in X$
$$G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

Corollary: $|G| = p^2$, G is abelian

Centralizer: $Z_G(H) = \{g \in G : gh = hg \quad \forall h \in H\}$

Normalizer: $N_G(H) = \{g \in G : g^{-1}Hg = H\}$

Sylow's theorems:

- *p-Sylow subgroup:* $p^n \mid G$, $H \subseteq G$ with $|H| = p^n$
- If $p^r \mid |G|$, G has a subgroup of order p^r
- $|G| = \prod_i |H_{p_i}|$ with H_{p_i} p-Sylow subgroups of distinct p_i
- For any two distinct p-Sylow subgroups, $P_1 \cap P_2 = \{e\}$

1. $|G| = p^n \cdot k$, G has at least one p-Sylow subgroup
2. All p-Sylow subgroups are conjugate: $\exists g \in G$, $H_2 = gH_1g^{-1}$
3. n is the number of distinct p-Sylow subgroups. $p \mid |G|$, $p \mid |k|$, $n \equiv 1 \mod p$

Lemma: $N_G(H) = \{g \in G : g^{-1}Hg = H\}$. If $H \subseteq G$, H has exactly $\#G/\$N_G(H)$ conjugates in G

Lemma: $A, B \subset D$, $AB = \{ab : a \in A, b \in B\}$,
$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

Lemma:
$$|HaK| = \frac{|H|\,|K|}{|aHa^{-1} \cap K|}$$