《代数结构》核心要点总结（最终排版）

一、群 (Group)

定义 1. 群. 一个非空集合 G 和其上的一个二元运算 $*$ 构成一个**群** $(G,*)$，若满足：

(i) **封闭性**: $\forall a,b\in G, a*b\in G$.

(ii) **结合律**: $\forall a,b,c\in G, (a*b)*c=a*(b*c)$.

(iii) **单位元** e: $\exists e\in G, \forall a\in G, a*e=e*a=a$.

(iv) **逆元** a^{-1}: $\forall a\in G, \exists a^{-1}\in G, a*a^{-1}=a^{-1}*a=e$.

若还满足**交换律** $a*b=b*a$，则称为**阿贝尔群**。

例子 1. 群的例子.

- **整数加法群** $(\mathbb{Z},+)$: 单位元是 0，逆元是 $-a$。
- **剩余类加法群** $(\mathbb{Z}_n,+_n)$: n 个元素 $\{[0],\dots,[n-1]\}$。
- **单位群** $(U_n,\times_n)$: 元素为 $\{k\mid 1\le k<n, \gcd(k,n)=1\}$，共 $\phi(n)$ 个元素。

定义 2. 群元素的阶. 设 $g\in G$，使得 $g^k=e$ 的最小正整数 k 称为 g 的**阶**，记作 $\mathrm{ord}(g)$。

性质 1. 阶的性质. 设 $\mathrm{ord}(g)=k$。

- **逆元**: $\mathrm{ord}(g^{-1})=k$.
- **幂的阶**: $\mathrm{ord}(g^m)=\frac{k}{\gcd(k,m)}$.
- **乘积的阶**: 若 g,h 可交换且 $\gcd(\mathrm{ord}(g),\mathrm{ord}(h))=1$，则 $\mathrm{ord}(gh)=\mathrm{ord}(g)\mathrm{ord}(h)$.
- **基本性质**: $g^n=e \iff k\mid n$.

定义 3. 子群与正规子群.

- **子群判定**: $H\subseteq G$ 是子群 $(H\le G) \iff \forall a,b\in H, ab^{-1}\in H$。对有限集 H，只需验证封闭性。
- **生成子群**: $\langle g\rangle=\{g^k\mid k\in\mathbb{Z}\}$。
- **陪集**: 左陪集 $gH=\{gh|h\in H\}$。所有左陪集构成对 G 的划分。
- **正规子群**: $H\trianglelefteq G \iff \forall g\in G, gH=Hg$.

注记/技巧 1. 正规子群判定技巧. $H\trianglelefteq G \iff \forall g\in G, gHg^{-1}=H$. 若 $[G:H]=2$ (指数为 2 的子群)，则 H 必为正规子群。

定理 1 (拉格朗日定理)**.** 若 H 是有限群 G 的子群，则 $|H|$ 整除 $|G|$。指数 $[G:H]=\frac{|G|}{|H|}$.

定义 4. 商群. 若 $H\trianglelefteq G$，则陪集集合 $G/H=\{gH\mid g\in G\}$ 在运算 $(aH)(bH)=(ab)H$ 下构成一个群。$|G/H|=[G:H]$。

定义 5. 循环群. 若 $\exists g\in G$ 使得 $G=\langle g\rangle$，则称 G 是**循环群**。

- $|G|=n \implies G\cong(\mathbb{Z}_n,+_n)$。
- $|G|=\infty \implies G\cong(\mathbb{Z},+)$。
- m 阶循环群的生成元个数为 $\phi(m)$。

注记/技巧 2. 循环群的子群结构. 阶为 n 的循环群 G 的任何子群都是循环群。对于 n 的每个正因子 d，都存在唯一一个阶为 d 的子群。子群个数等于 n 的正因子个数 $\tau(n)$。

定义 6. 群同态. 映射 $f:G\to H$ 称为**群同态**，如果 $\forall a,b\in G, f(a*b)=f(a)\circ f(b)$。若 f 是双射，则为**同构** $(G\cong H)$。

性质 2. 同态保持的性质. 设 $f:G\to H$ 是群同态。

- $f(e_G)=e_H$ (单位元)。
- $f(g^{-1})=(f(g))^{-1}$ (逆元)。
- $\mathrm{ord}(f(g))\mid\mathrm{ord}(g)$ (阶是因子)。
- 若 $S\le G$, 则 $f(S)\le H$ (子群)。
- 若 $N\trianglelefteq G$, 且 f 是满射, 则 $f(N)\trianglelefteq H$ (正规子群)。

定理 2 (群同态基本定理)**.** 设 $f:G\to H$ 是群满同态，则 $G/\ker(f)\cong H$，其中核 $\ker(f)=\{g\in G\mid f(g)=e_H\}$ 是 G 的正规子群。

注记/技巧 3. 循环群间同态. 对于 $f:\mathbb{Z}_m\to\mathbb{Z}_n$，同态个数为 $\gcd(m,n)$。

定义 7. 群间运算.

- **外直积**: $G\times H=\{(g,h)\mid g\in G,h\in H\}$。
- **内直积**: 若 $H,K\trianglelefteq G, H\cap K=\{e\}, G=HK$，则 $G\cong H\times K$.

二、环 (Ring)

定义 8. 环. 集合 R 和两个运算 $(+,\cdot)$ 构成一个**环** $(R,+,\cdot)$，若:

(i) $(R,+)$ 是一个**阿贝尔群**。

(ii) **乘法结合律**成立。

(iii) **分配律**成立。

例子 2. 环的例子.

- **整数环** $(\mathbb{Z},+,\cdot)$。
- **剩余类环** $(\mathbb{Z}_n,+,\cdot)$。
- **多项式环** $F[x]$。

定义 9. 整环. 一个**无零因子**的**含幺交换环**称为**整环**。$(ab=0 \implies a=0 \text{ 或 } b=0)$

例子 3. . $\mathbb{Z}$ 是整环。$\mathbb{Z}_n$ 是整环 $\iff$ n 是素数。**高斯整环**: $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$。

定义 10. 子环与理想.

- **子环判定**: $S\subseteq R$ 是子环 $\iff$ $(S,+)$ 是子群且 S 对乘法封闭。
- **理想**: 子环 $I\subseteq R$ 是**理想**，若满足**吸收性**: $\forall r\in R, a\in I \implies ra\in I$ 且 $ar\in I$。
- **主理想**: $\langle a\rangle = RaR$。交换环中 $\langle a\rangle = Ra=\{ra \mid r\in R\}$。
- **素理想**: $ab\in P \implies a\in P$ 或 $b\in P \iff R/P$ 是整环。
- **极大理想**: 不存在理想 I 使得 $M\subset I\subset R \iff R/M$ 是域。

> **注记/技巧 4. PID 中的理想关系.** 在主理想整环 (PID) 中（如 $\mathbb{Z}$ 和 $F[x]$），所有非零的素理想都是极大理想。

定义 11. 理想间运算. 设 I,J 是环 R 的理想。

- **加**: $I+J=\{a+b \mid a\in I, b\in J\}$.
- **交**: $I\cap J$.
- **乘**: $IJ=\{\sum a_ib_i \mid a_i\in I, b_i\in J\}$. $IJ\subseteq I\cap J$。

定义 12. 环的特征.$\text{char}(R)$ 是使得 $\forall r\in R, kr=0$ 的最小正整数 k。

性质 3. . 整环的特征为 0 或一个素数。若 $\text{char}(R)=p$ (素数), 则 $(a+b)^p=a^p+b^p$。

定义 13. 环同态. $f:R\to S$ 是**环同态**，如果保持加法和乘法运算。

性质 4. 环同态保持的性质.

- $f(0_R)=0_S$ (零元)。若 f 是满射, 则 $f(1_R)=1_S$。
- 若 $R'\le R$, 则 $f(R')\le S$ (子环)。
- 若 I 是 R 的理想, 则 $f(I)$ 是 $f(R)$ 的理想。

定理 3 (环同态基本定理)**.** 设 $f:R\to S$ 是一个环满同态，则 $R/\ker(f)\cong S$。

> **注记/技巧 5. 中国剩余定理 (环论形式).** 若 I,J 是理想且 $I+J=R$，则 $R/(I\cap J)\cong R/I\times R/J$. 对于 $\mathbb{Z}$，若 $\gcd(m,n)=1$, 则 $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$。

三、域 (Field)

定义 14. 域. 一个**含幺交换环** $(F,+,\cdot)$ 称为**域**，如果每个非零元素都有**乘法逆元**。即 $(F\setminus\{0\},\cdot)$ 是一个阿贝尔群。

例子 4. 域的例子.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$。
- $\mathbb{Z}_p$ (p 为素数) 是一个有限域。
- $\text{GF}(p^n)$: 阶为 p^n 的有限域 (伽罗瓦域)。

性质 5. 域的结构性质.

- 域一定是整环。有限整环一定是域。
- 域中只有两个理想: $\{0\}$ 和 F 本身。

定义 15. 有限域.

- **阶**: 阶为 q 的有限域存在 $\iff$ $q=p^n$.
- **加法群**: $(\text{GF}(q),+)\cong(\mathbb{Z}_p)^n$。
- **乘法群**: $(\text{GF}(q)\setminus\{0\},\cdot)$ 是一个阶为 $q-1$ 的**循环群**。

> **注记/技巧 6. 有限域的构造与本原元.**
>
> - **构造**: $\text{GF}(p^n)\cong\mathbb{Z}_p[x]/\langle f(x)\rangle$，其中 $f(x)$ 是 $\mathbb{Z}_p$ 上一个 n 次的**不可约多项式**。
> - **本原元**: 有限域乘法群的生成元称为**本原元**。例如，在 $\text{GF}(2^3)\cong\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ 中，x 就是一个本原元。