> 总结一些老师上课提到的重点，以及可能要考的题。标★的章节或知识点是要重点看的。
>
> **大部分内容是由16级的赵剑辉学长所写**，在此深表感谢。
>
> 知识点会有不全的地方（建议还是看一下书），有什么问题欢迎大家指出。

第一章 基本概念

1.6 等价关系与集合的分类

概念

- 等价关系：集合M的一个关系R满足以下三个条件，这个关系是M的一个等价关系，a, b等价记作：$a \sim b$。成立
    1. $\forall\ a \in M$, 有 $a\mathrm{R}a$；（自反性）
    2. 如果 $a\mathrm{R}b$，有$b\mathrm{R}a$；（对称性）
    3. 如果 $a\mathrm{R}b$, $b\mathrm{R}c$，有$a\mathrm{R}c$；（传递性）

课后习题

2，3题

第二章 群

重点内容： 群的基本概念，判断规定了运算的代数系统是否为群?

2.1 群的定义和初步性质

概念

- **群**:

1. 运算封闭，$\forall a, b \in G, a \circ b \in G$；
    2. 结合律，$\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$；
    3. 单位元，$\forall a \in G, a \circ b = a, b \in G$，则b称为单位元，记为$e$；
    4. 逆元，$\forall a \in G, \exists b \in G, a \circ b = e$，则b为a的逆元，记为$a^{-1}$。

- 半群：满足运算封闭与结合律；

- 幺半群：满足运算封闭和结合律，并且有单位元（幺元）。
- **交换群(Abel)**：满足群的定义，群中元素的运算满足交换律：$\forall a,b\in G, a\circ b=b\circ a.$

习题

例题：1，2

课后题：1，2，4，5，6

> 6、证明：若群G中任意元素满足$x^2=e$，则G为交换群。
>
> proof:
>
> 由$x^2=e$，$x\circ x=e$，得$x^{-1}=x$;
>
> $\forall a,b\in G, a\circ b\in M$,
>
> 则$a\circ b=(a\circ b)^{-1}=b^{-1}\circ a^{-1}=b\circ a$,
>
> 故G为交换群。

★ 2.2 群中元素的阶

概念

- 元素的**阶**：
  设a为群G的一个元素，使$a^n=e$成立的最小正整数n为a的阶，记为$|a|$。

定理

1. 有限群中每个元素的阶均有限；
2. ★ $|a|=n$，则 $a^m=n \iff n\mid m$;
3. $|a|=n$，则 $|a^k|=\dfrac{n}{(k,\,n)}$;
4. $|a|=m, |b|=n, ab=ba, (m,\,n)=1 \Longrightarrow |ab|=mn=|a|\cdot|b|$;
5. G为交换群，群中所有元素有最大阶m，则G中每个元素的阶都是m的因数，即G中每个元素都满足$x^m=e.$

习题

课后题：1，2，3，4

> 1、以第一小题为例，证明：$a,\, a^{-1},\, cac^{-1}$的阶相同。
>
> Proof:
>
> 设$|a|=m, |a^{-1}|=n$，则$(a^{-1})^m=e^{-1}=e\Longrightarrow n\mid m$,
> $a^n=\left[(a^{-1})^{-1}\right]^n=e^{-1}=e\Longrightarrow m\mid n$，于是$m=n.$
>
> 其他类似可证。

2.3 子群

概念

1. 子群：群G的一个非空子集H本身关于群G的乘法也做成一个群，则H称为G的一个子群，记为$H \leqslant G$。
2. 平凡子群：$\{e\}$和G;
3. 非平凡子群（真子群）：除平凡子群以外的**子群**，记为$H < G$。

★子群的判定定理（也可以拆成两部分）：

群G的非空子集做成子群的充要条件是：

$$a,\ b \in H \implies ab^{-1} \in H.$$

习题

课后题：7

> 7、证明：任何子群都不能是两个真子群的并。
>
> 反证：设群$G = A_1 \cup A_2$，其中A_1, A_2为G的真子群。
>
> 则$\exists a \in G \backslash A_1, b \in G \backslash A_2$，
>
> 又$a \circ b \in G$，则$a \circ b \in A_1$或者$a \circ b \in A_2$，
>
> 若$a \circ b \in A_1$，由$b \in A_1$可得$a \in A_1$与假设矛盾。
>
> 若$a \circ b \in A_2$，同理;
>
> 故假设不成立，原命题成立。

2.4 循环群

概念

- 循环群：如果群G可以由一个元素a生成，即$G =< a >$，则称G为由a生成的一个**循环群**，称a为G的一个**生成元**。

定理

- n阶循环群对n的每个正因数k，有且仅有一个k阶子群，这个子群是$\langle a^{\frac{n}{k}} \rangle$;

习题

课后题：4、

2.5 变换群

概念

变换：集合M到其自身的映射，以$T(M)$记M全体变换所成集合。

置换：集合M到其自身的双射变换，以$S(M)$记M全体置换所成集合。

Cayley定理：任何群同一个双射变换群同构。

推论：任何n阶有限群都与n元对称群$\mathcal{S}_n$的一个子群同构。

定理

定理2：设G是集合M的一个变换群，则

$$G\text{是双射变换群} \iff G\text{含有}M\text{的单（满）射变换}$$

推论：设G是集合M的一个变换群，则

$$G\text{是双射变换群} \iff G\text{包含恒等变换}$$

习题

例题：2

> 2、设M={1,2,3,4}，证明：M的以下两个变换
>
> $$\alpha=\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix}\quad\beta=\begin{pmatrix}1&2&3&4\\1&1&4&3\end{pmatrix}$$
>
> 做成M的一个非双射变换群。
>
> Proof：令G={α,β}，计算有
>
> | | α | β |
> |---|---|---|
> | α | $\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix}=\alpha$ | $\begin{pmatrix}1&2&3&4\\1&1&4&3\end{pmatrix}=\beta$ |
> | β | $\begin{pmatrix}1&2&3&4\\1&1&4&3\end{pmatrix}=\beta$ | $\begin{pmatrix}1&2&3&4\\1&1&3&4\end{pmatrix}=\alpha$ |
>
> 故G中关于变换的乘法封闭；
>
> 由计算结果显然α为单位元，α,β的逆元均为自身，
>
> 故G为M的一个非双射变换群。
>
> ★扩充：
>
> 对于{α,β,ε}不构成M的一个群，利用定理2显然。

课后题：1、2、3、4、5、

★ 2.6 置换群

概念

- n元置换群：n元对称群的任意一个子群；
- n元对称群（$\mathcal{S}_n$，全体双射变换），阶为$n!$；
- n元交错群（$\mathcal{A}_n$交错群，全体偶置换），阶为$\dfrac{n!}{2}$；

- $k-$轮换$\begin{cases}\text{对换：} 2-\text{轮换}\\ \text{不相连轮换：无公共数码的轮换}\end{cases}$；

定理

- 每个置换都可以表示为对换之积；
- $(i_1 i_2 \ldots i_k) = (i_1 i_k)(i_1 i_{k-1}) \ldots (i_1 i_2)$；
- ★ $k-$轮换的阶为k，不相连轮换乘积的阶为各因子阶的最小公倍数。
- 定理5：

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

习题

例题：3、5、

> (24)的阶为2，(24)(153)的阶为6;
>
> 相连轮换乘积的阶如(123)(345):
>
> 先用(345)作用，再用(123)
>
> $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$
>
> 得：(12345)，故(123)(345)的阶为5。

课后题：3（结果分别为4，6，3，6）、4

> 4、$\tau = (327)(26)(14)$, $\sigma = (134)(57)$，求$\sigma\tau\sigma^{-1}$, $\sigma^{-1}\tau\sigma$;
>
> 解：$\sigma^{-1} = (57)(431)$
>
> $$\begin{aligned} \sigma\tau\sigma^{-1} &= (\sigma(3)\sigma(2)\sigma(7))(\sigma(2)\sigma(6))(\sigma(1)\sigma(4)) \\ &= (425)(26)(31) = (13)(2654), \\ \sigma^{-1}\tau\sigma &= \sigma^{-1}\tau(\sigma^{-1})^{-1} \\ &= (\sigma^{-1}(3)\sigma^{-1}(2)\sigma^{-1}(7))(\sigma^{-1}(2)\sigma^{-1}(6))(\sigma^{-1}(1)\sigma^{-1}(4)) \\ &= (125)(26)(43) = (1265)(34). \end{aligned}$$

2.7 陪集、指数和Lagrange定理

概念

陪集：H是群G的一个子群，$a \in G$，则称$aH = \{ax|x \in H\}$为G关于H的左陪集，$Ha = \{xa|x \in H\}$为G关于H的右陪集。常用性质$aH = bH \leftrightarrow a^{-1}b \in H(b^{-1}a \in H)$.

指数：群G关于子群H互异的左(或右)陪集的个数，即为(G:H).

定理

Lagrange定理：设H是**有限群**G的一个子群，则

$$|G| = |H|(G:H), (G:H) = \frac{|G|}{|H|}.$$

习题

课后题：2、4、5

> 2、证明：
>
> 由于$H\bigcap K\leqslant H,\ H\bigcap K\leqslant K$，所以$|H\bigcap K|\Big|m,\ |H\bigcap K|\Big|n$，所以$|H\bigcap K|\Big|(m,\ n)$，而$(m,\ n)=1$,所以$|H\bigcap K|=1\Longrightarrow H\bigcap K=\{e\}.$

> 5、反证。

第三章 正规子群与群的同态与同构

3.1 群同态与同构的简单性质

概念

- 同态映射：映射$\varphi:G\rightarrow\overline{G}$满足$\varphi(ab)=\varphi(a)\varphi(b),\ \forall\, a,\, b\in G$;
- 同构映射：上述映射为双射情形时，φ为同构映射。

习题

★例题3

（在同构意义下，6阶群只有两个：6阶循环群和三元对称群$\mathcal{S}_3$）

课后题1、3

> 1、设H是群G的一个子群，$a\in G$.证明:
>
> $$aHa^{-1}\leqslant G$$
>
> Proof：$\forall h_1,h_2\in H$，有$ah_1a^{-1}(ah_2a^{-1})^{-1}=ah_1a^{-1}ah_2^{-1}a^{-1}=a(h_1h_2^{-1})a^{-1}$,
>
> 由于H为G的一个子群，故$h_1h_2^{-1}\in H$,
>
> 则有$a(h_1h_2^{-1})a^{-1}\in aHa^{-1}$，即$aHa^{-1}\leqslant G.$

3.2 正规子群和商群

概念

正规子群：N是群G的一个子群，有:

$$\forall a\in G,aN=Na,N=aNa^{-1},$$

则称N为G的正规子群。

商群：群G的正规子群N的全体陪集对于陪集的乘法做成一个群，记为$G/N.$

- 素数阶群必为循环群(Lagrange定理)
- 若N的指数为2，则N为正规子群(非专门考证明，可直接使用)

Hamilton群：每个子群都是正规子群的**非交换群。**

单群：阶大于1且只有平凡正规子群的群。

习题

例题：4、四元数群G是最小的Hamilton群

(每个子群都是正规子群的非交换群)

- 四元数群$\{1,i,j,k,-1,-i,-j,-k\}$:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

> 1. $\leqslant 7$阶群：
>
> n=1，H={e}，显然不是Hamilton群；
>
> n=2,3,5,7，H为循环群，均为交换群，显然非Hamilton群；
>
> n=4时，H同构于四阶循环群或K_4，均为交换群，故非Hamilton群；
>
> n=6时，H同构于六阶循环群或S_3，循环群为交换群，非Hamilton群，
>
> 若同构于S_3，S_3有子群{(1),(12)}，而
>
> $$(12)(123) = (132)$$
> $$(123)(12) = (123)$$
>
> 故S_3非Hamilton群。
>
> 2. 四元数群是Hamilton群:
>
> 对于四元数群，由Lagrange定理可知，该群中元素必为1，2，4，8阶，
>
> 该群为非交换群，故群中无8阶元素；
>
> 群中4阶元素为$i,j,k,-i,-j,-k$，二阶元素为-1，单位元为1；
>
> 则四阶子群有$\langle i\rangle,\langle j\rangle,\langle k\rangle$，二阶子群为<-1>，无其它非平凡子群，
>
> 又四阶子群的指数为2，故必为正规子群；
>
> 对于二阶子群H_2 ={1,-1}，对于四元数群中的任意元素a，有
> $a*1=a=1*a, a*(-1)=-a=(-1)a$，故$H_2$为正规子群。
>
> 综上，四元数群为最小的Hamilton群。

课后题：1、2、4

> 2、证明：若群G的n阶子群有且只有一个，则此子群必为G的正规子群。
>
> （若使用**3.1节课后题1**结论需要证明）
>
> Proof：设N为G的n阶子群，则由3.1节结论知$aNa^{-1}\leqslant G$,

> 且$\forall b_1, b_2 \in N, ab_1a^{-1} \neq ab_2a^{-1}$，
>
> 故$|N| = |aNa^{-1}| = n$
>
> 又n阶子群有且只有一个，
>
> 故aNa^{-1}与N为同一个群，$N = aNa^{-1}$
>
> 则有$aN = Na$，所以N为G的正规子群。

> 4、设H,K是群G的两个正规子群，且两者的交为{e}。证明：H与K中元素相乘时可换。
>
> Proof：由H,K为群G的两个正规子群，有
>
> $$H = k^{-1}Hk, k \in K \subseteq G \\ K = hKh^{-1}, h \in H \subseteq G$$
>
> 则$\forall k \in K, h \in H$，讨论$k^{-1}hkh^{-1}$：
>
> 显然,$k^{-1}hk \in H, h^{-1} \in H \to k^{-1}hkh^{-1} \in H,$
>
> $hkh^{-1} \in K, k^{-1} \in K \to k^{-1}hkh^{-1} \in K,$
>
> 又$K \cap H = \{e\},$
>
> 故$k^{-1}hkh^{-1} = e$,则有$hk = kh$，即H与K中元素相乘时可换。

3.3 群同态基本定理

群同态基本定理：设φ为群G到群$\overline{G}$的一个同态满射，$N = \operatorname{Ker}\varphi \trianglelefteq G$，则：

$$G/N \cong \overline{G}.$$

习题

课后题：1、2、4、5

> 2、证明：单群的同态像是单群或者单位元群。
>
> Proof：由于单群的正规子群只有{e}和其本身，又$\operatorname{Ker}\varphi$为正规子群：
>
> 若$\operatorname{Ker}\varphi$=$\{e\}$，由群同态基本定理有：$G \cong G/\operatorname{Ker}\varphi \cong \overline{G}$，即同态像同构于它自身，故为单群；
>
> 若$\operatorname{Ker}\varphi$=G，由群同态基本定理由：$\{e\} \cong G/\operatorname{Ker}\varphi \cong \overline{G}$，即同态像同构于单位元群。

3.4 群的同构定理

习题

课后题：1、2

第四章 环与域

4.1 环的定义

概念

环：非空集合R有两个代数运算，一个为加法，另一个为乘法，满足如下三个条件：

1. 对加法构成一个**加群**；
2. 乘法满足**结合律**；
3. 乘法对加法满足**左右分配律**：

$$a(b+c)=ab+ac \quad \text{左分配律}$$
$$(a+b)c=ac+bc \quad \text{右分配律}$$

交换环：满足环的定义+乘法交换律

习题

课后题：1（不是，因为不满足分配律）、2、3、4、

> 4、环R中任一元素a满足$a^2=a$，证明：R为交换环，而且其中任何元素a都满足
>
> $$a+a=0$$
>
> Proof:
>
> $\forall a\in R, a+a\in R, (a+a)^2=a+a$
>
> $(a+a)^2=a^2+a^2+a^2+a^2=a+a+a+a=a+a,$
>
> 则$a+a=0\rightarrow a=-a,$
>
> $\forall a,b\in R, (a+b)^2=a^2+b^2+ab+ba=a+b+ab+ba=a+b,$
>
> 则$ab+ba=0\rightarrow ab=-ba=ba,$
>
> 故R为交换群。

4.2 环的零因子和特征

概念

- 左右零因子、正则元；
- 整环：阶大于1、有单位元且无**零因子**($\exists ab=0,a,b\neq 0$)的交换环；
- 环的特征：环R的元素对加法有最大阶n，n为R的特征；

习题

课后题：1、2

4.3 除环和域

概念

除环：阶大于1、有单位元且每一个非零元都有逆元的环。

域：可换除环。

习题

例题：2、

课后题：4、

> 4、域F的阶为4，证明：1) char F=2； 2) F中非0及1的两个元素均满足方程$x^2=x+1$。
>
> Proof:
>
> 1) $|F|=4$，char $F\Big||F|$ ，于是char F$\in\{1,2,4\}$. 又因为F是域，域的特征为素数，所以char F=2.
>
> 2) 由1)，char F=2，设F中非0及1的元素为a、b（$a\neq b,\ a,b\neq 0$且$a,b\neq 1$），即$F=\{0,1,a,b\}$，
>
> 下证$b=a+1$，
>
> $$\begin{cases}如果a+1=0，则有a=-1，而-1=1，所以a+1\neq 0\\ 如果a+1=1，则有a=0，与a\neq 0矛盾，所以a+1\neq 1\\ 如果a+1=a，则有1=0，矛盾\end{cases}$$
>
> 综上，$b=a+1$，于是有
>
> $$(a+1)^2=a^2+2a+1=a^2+1$$
>
> 下面验证四个元素是否满足条件：
>
> $$\begin{cases}若a^2=0，矛盾\\ 若a^2=1，有(a+1)^2=a^2+1=1+1=2=0，则a=1，矛盾\\ 若a^2=a+1，则(a+1)^2=(a+1)+1，成立\\ 若a^2=a，则a(a-1)=0，矛盾\end{cases}$$
>
> 证毕。

4.4 模n剩余类环

模n的剩余类环Z_n

- Z_n中元素$\overline{m}$如果与n互素，则为可逆元，否则为零因子。
- Z_n有且只有$T(n)$个子环。

习题

例题：3、4、

课后题：1、2、3、5、6、7、

> 1、★ Z_{10}**的各种计算：**
>
> - 零因子：$2*5=\overline{0}$，$4*5=\overline{0}$，$6*5=\overline{0},8*5=\overline{0}$，故零因子为$\overline{2},\overline{4},\overline{5},\overline{6},\overline{8}$.

> - 可逆元(单位):$\overline{1},\overline{3},\overline{7},\overline{9}$,
> - 特征(char R，对于加法的最大阶)：10.
> - 子群、子环、理想:T(10)=4
>   1. $\{\overline{0}\}$;　特征：0
>   2. Z_{10};　特征：10
>   3. $\{\overline{0},\overline{5}\}$;　特征：2
>   4. $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8}\}$;　特征：5

> 5、证明：有理数域的自同构只有恒等自同构。
>
> Proof：设φ为Q到其自身的同构映射，
>
> 显然$\varphi(0)=0$，
>
> 又$\varphi(1)=\varphi(1\circ 1)=\varphi(1)\varphi(1)=\varphi(1)*1$
>
> 则$\varphi(1)(\varphi(1)-1)=0$，又Q为域，
>
> 故$\varphi(1)=1.$
>
> 则$\varphi(m)=\varphi(m\circ 1)=m\varphi(1)=m,m\in Z$
>
> $\forall n\in Z\backslash\{0\},\varphi(\frac{1}{n}\circ n)=\varphi(n)\varphi(\frac{1}{n})=n\varphi(\frac{1}{n})=1$
>
> 则$\varphi(\frac{1}{n})=\frac{1}{n}$
>
> 故$\forall a\in Q,a=\frac{m}{n}$,
>
> 则$\varphi(a)=\varphi(\frac{m}{n})=\varphi(m)\varphi(\frac{1}{n})=m*\frac{1}{n}=a$
>
> 故$\varphi(a)=a$，则有理数域的自同构只有恒等自同构。

4.5 环与域上的多项式环

习题

例题：1、2、

课后题：2、3、

> 2、例如：在$\mathbb{Z}_4$中，两个一次多项式$\overline{2}x$相乘，得到：$\overline{4}x=\overline{0}$，并不是2次多项式。

4.6 理想

概念

理想:

设N是环R的一个子加群，如果：

$$r\in R,a\in N\Longrightarrow ra\in N$$

则N为R的一个左理想，左吸收律；

设N是环R的一个子加群，如果：

$$r \in R, a \in N \Longrightarrow ar \in N$$

则N为R的一个右理想，右吸收律；

若N既为左理想也为右理想，则N为双边理想，简称理想，记为$N \trianglelefteq R$.

主理想$< a >$(包含元素a的最小理想)中元素的一般形式：

$$< a >= \{xa + ay + na + \sum_{i=1}^{m} x_i a y_i | x, y, x_i, y_i \in R, n \in Z, m \in N^+\}$$

1. R可交换：$< a >= \{ra + na | r \in R, n \in Z\}$;
2. R有单位元：$< a >= \{\sum_{i=1}^{m} x_i a y_i | m \in N^+\}$;
3. R既可交换也有单位元：$< a >= \{ra | r \in R\}$.

习题

例题：4、5

> 4、整数环的理想<4,6>=<2>.
>
> Proof：显然整数环既可交换也有单位元
>
> 故<2>={2n | n∈Z}，<4,6>={$4k_1 + 6k_2 | k_1, k_2 \in Z$}
>
> 又$2 = 6 - 4 \in < 4, 6 >, 4 = 2 * 2 \in < 2 >, 6 = 3 * 2 \in < 2 >$
>
> 故$< 2 > \subseteq < 4, 6 >, < 2 > \supseteq < 4, 6 >$
>
> 则$< 4, 6 > = < 2 >$。

> 整数环上的多项式环Z[x]的理想$< 2, x >$不是主理想。
>
> 反证法：
>
> 若$< 2, x >$是Z[x]的主理想，则有$< 2, x > = < g(x) >$,
>
> 又$Z[x]$既可交换也有单位元，
>
> 故有$< g(x) >= \{f(x)g(x) | f(x \in Z[x])\}$
>
> 则可令
>
> $$\begin{aligned} 2 &= t_1(x)g(x) \\ x &= t_2(x)g(x) \end{aligned}$$
>
> 上式只有当$g(x) = \pm 1$时可成立，而$< 2, x >$中不包含± 1，故假设不成立。

课后题：2、

> 2、设R为偶数环，证明：
>
> $$N = \{4r | r \in R\} \trianglelefteq R$$
>
> 问：N=$< 4 >$是否成立？N是由哪个数生成的主理想？
>
> (1）N是R的一个子加群
>
> $\forall r_1, r_2 \in R, 4r_1 - 4r_2 = 4(r_1 - r_2)$,
>
> 由于R为环，$r_1 - r_2 \in R$,
>
> 故$4r_1 - 4r_2 \in N$,

> 则N为R的一个子加群。
>
> (2) 左右吸收律（循环环不需证明）
>
> $\forall r' \in R, r \in R, r' * (4r) = 4(r'r)$(交换律)
>
> 由于R为环，$r'r \in R$，
>
> 故$r' * 4r \in N$，满足左吸收律 。
>
> 又偶数环R可交换，故满足右吸收律。
>
> 所以$N \trianglelefteq R$.
>
> 显然，$<4>$中包含4，而$4 \notin N$，故$N \neq <4>$.
>
> $N=<8>$,证明同上述例4.

4.7 商环与环同态基本定理

概念

商环：设N是环R的一个理想，则R/N对于陪集的加法与乘法作成一个环。

定理

环同态基本定理

设R和$\overline{R}$是两个环，且$R \sim \overline{R}$，则：

1. 这个同态映射的核N，是R的一个理想；
2. $R/N \cong \overline{R}$

习题

例题：1、2、

课后题：1、4、

> 1、$\varphi: R \rightarrow \overline{R}$为同态满射，$N=\operatorname{Ker} \varphi$，证明：$\varphi$同构映射 $\Longleftrightarrow \quad N=\{0\}$;
>
> Proof:
>
> “$\Longrightarrow$”：显然
>
> “$\Longleftarrow$”：设$N=\operatorname{Ker} \varphi$，且
>
> $$\varphi(a)=\varphi(b), \quad \forall a, b \in R,$$
>
> 则有$\varphi(a-b)=\varphi(a)-\varphi(b)=\overline{0}$，于是$a-b \in \operatorname{Ker} \varphi=\{0\}$，所以$a=b$，$\varphi$单射（相同像的原像相同）。 ■

其他补充题

★ ≤7阶群的结构

> - $n=1$，H={e}
> - $n=2,3,5,7$，n为素数，故H为循环群

- $n=4$:

  由Lagrange定理，H中元素只有1，2，4阶

  若$\exists h,|h|=4$，则$|H|=|h|$，则H可由该元素生成，必同构于循环群；

  若H中非单位元均为2阶，则H中元素满足$x^2=e$，则有H为Abel群，

  群H中元素应为{e,a,b,ab}，下证$ab\neq a,b,e$:

  若ab=e，则a=b，产生矛盾；

  若ab=a，则b=e，产生矛盾；

  若ab=b，则a=e，产生矛盾；

  又$(ab)^2=(ab)(ab)=a^2b^2=e$，故$|ab|=2$，所以H必同构于{e,a,b,ab}.

- $n=6$, **3.1节例3**

  由Lagrange定理，H中元素必为1，2，3，6阶

  若$\exists h,|h|=6$，则|H|=|h|，群H可由该元素生成，必同构于循环群；

  若群中除e外均为3阶元素，则在H存在3阶子群：

  $A_1=\{e,a,a^2\},A_2=\{e,b,b^2\},b\notin A_1$

  则$A_1\cap A_2=\{e\}$，故

  $$|A_1A_2|=\frac{|A_1||A_2|}{|A_1\cap A_2|}=9$$

  与$|H|=6$矛盾；

  若群中除e外均为2阶元素，则在群H中可取互异的二阶元素，有

  $\{e,a,b,ab\}\leqslant H$，与Lagrange定理相矛盾；

  因此，H中必同时含有2、3阶元：

  设$H=\{e,a,b,b^2,ab,ab^2\}$，|a|=2,|b|=3:

  作映射

  $$\begin{aligned}\varphi:&e\to(1),a\to(12),b\to(123)\\&b^2\to(132),ab\to(23),ab^2\to(13)\end{aligned}$$

  该映射为同构映射，故$H\cong S_3$。

整数环Z的所有自同态

> 设$\varphi|Z\to Z$是同态映射
>
> 则
>
> $$\begin{aligned}\varphi(1)=\varphi(1*1)=\varphi(1)\circ\varphi(1)=\varphi(1)\circ 1\Longrightarrow\varphi(1)=0\ \ or\ \ \varphi(1)=1\\\varphi(m)=\varphi(m*1)=m\varphi(1)\Longrightarrow\varphi(m)=0\ \ or\ \ \varphi(m)=m\end{aligned}$$
>
> 故整数环的所有自同态为:
>
> 1. $\varphi(m)=0,\forall m\in Z$
> 2. $\varphi(m)=m,\forall m\in Z$