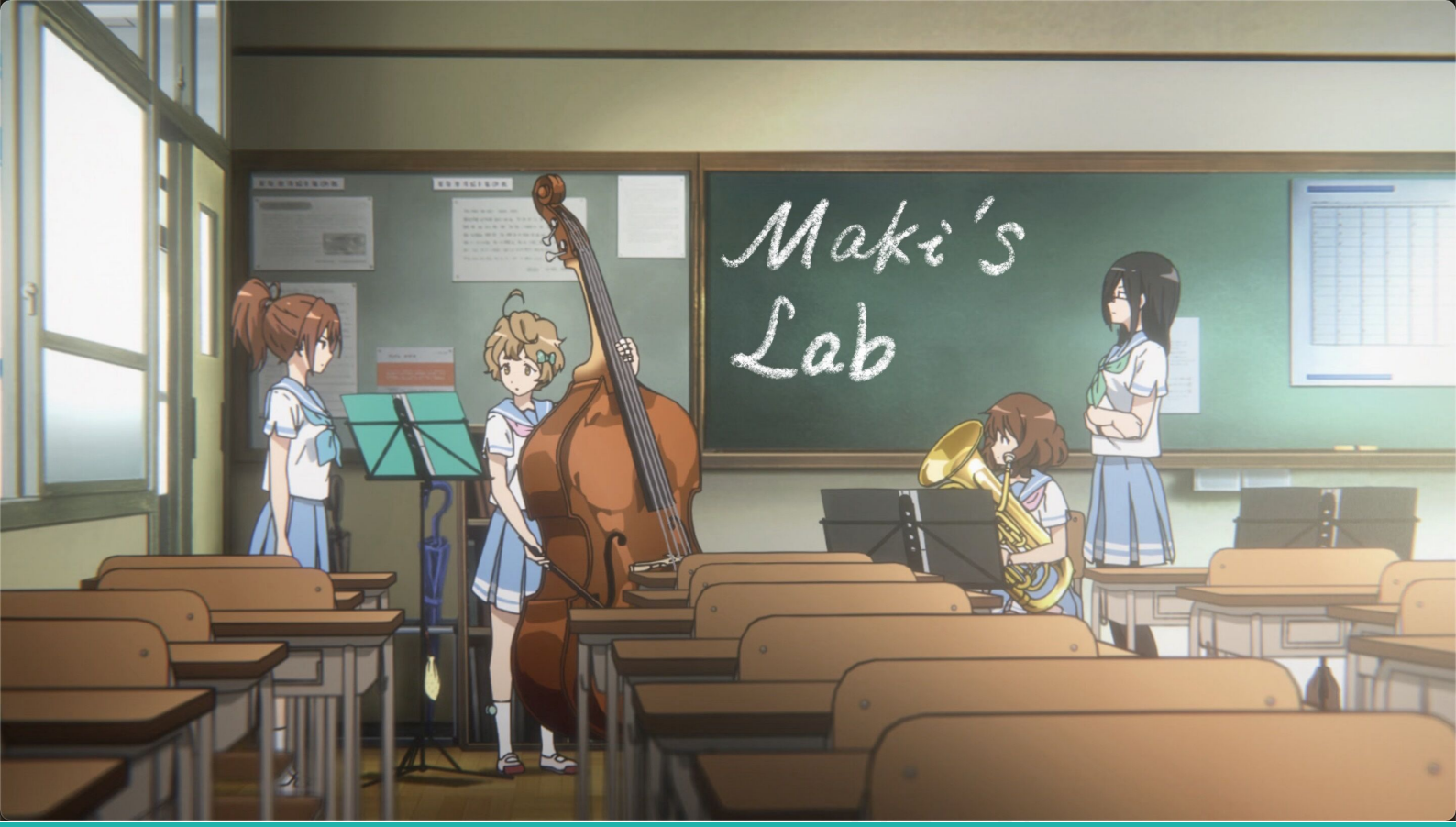
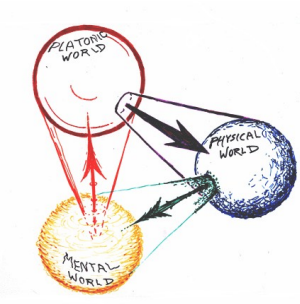


抽象代数习题讲义

作者：Hongxin Yang 南风

时间：October 19, 2025



目录

第 1 章 相关定理环境等的标识

Proof 使用方法:begin+ proof+ end

注 使用方法:begin+ remark+ end

例题 1.1 使用方法：begin+ example + end

Exercise 1.1 使用方法:begin+ exercise +end

性质 使用方法:begin+ property + end

问题 1.1 使用方法:begin + problem +end

结论 使用方法:begin+ conclusion +end

笔记 使用方法；begin + note + end

定义 1.1

使用方法:begin+ definition+ end

命题 1.1

使用方法:begin+ proposition+ end

引理 1.1

使用方法:begin+ lemma+ end

推论 1.1

使用方法:begin + corollary + end

公理 1.1

使用方法:begin+ axiom + end

公设 1.1

使用方法:begin + postulate + end

第 2 章 群论习题

Exercise 2.1

设$n\in\mathbb{N},\mathbb{Z}_n$表示集合$\{\overline{0},\overline{1},\cdots,\overline{n-1}\}$，在$\mathbb{Z}_n$中定义运算如下$\bar{a}\cdot\bar{b}=\bar{c}$，其中$c$是$ab$模$n$的余数；$\bar{a}+\bar{b}=\bar{d}$，其中$d$是$a+b$模$n$的余数

(1) 证明：$\{\mathbb{Z}_n;\cdot\}$是交换么半群，$\{\mathbb{Z}_n;+\}$是交换群

(2) 设$\mathbb{Z}_n^*=\{\bar{a}\in\mathbb{Z}_n\mid(a,n)=1\}$证明：$\left\{\mathbb{Z}_n^*;\cdot\right\}$是群

(3) 设p是素数，利用群的思想证明$Wilson$定理：$(p-1)!\equiv-1(\mathrm{mod}p)$.

(4) 证明$Euler$定理$\varphi(n)$为小于n的与n互素的正整数个数，那么$a^{\varphi(n)}\equiv1\,(\mathrm{mod}p)\quad a\in\mathbb{N}^+$且$(a,n)=1$

Proof 前面都是$check$定义的问题我们不过做解释

下面证明$Wilson$定理构造$\mathbb{Z}_p^*=\left\{\bar{1},\bar{2},\cdots\overline{p-1}\right\}$这一群此时我们注意到$\bar{1}$为么元且$\overline{p-1}$的逆元为$\overline{p-1}$

那么此时我们往证：$(p-1)!\equiv-1\,(\mathrm{mod}p)\Longleftrightarrow\bar{1}\cdot\bar{2}\cdot\cdots\cdot\overline{p-1}=\overline{p-1}\Longleftrightarrow\bar{1}\cdot\bar{2}\cdot\cdots\cdot\overline{p-2}=\bar{1}\Longleftrightarrow\bar{2}\cdot\cdots\cdot\overline{p-2}=\bar{1}$

此时我们注意到在$\mathbb{Z}_p^*=\left\{\bar{1},\bar{2},\cdots\overline{p-1}\right\}$中$\bar{2},\cdots\overline{p-2}$中每个元素的逆元都在其中即是两两配对的故显然

下面证明$Euler$定理对于任意的正整数n构造$\mathbb{Z}_n^*=\{\bar{a}\mid(a,n)=1\}$此时$\left|\mathbb{Z}_n^*\right|=\varphi(n)$

由拉格朗日定理我们即知道$(\overline{a})^{\varphi(n)}=\bar{1}$

Exercise 2.2

设S是所有数论函数（即$\mathbb{N}^*$到$\mathbb{C}$的映射）的全体.对于$f,g\in S$我们定义$Dirichlet$卷积为$f*g(n)=\sum\limits_{d|n}f(d)g\left(\dfrac{n}{d}\right)=\sum\limits_{ab=n}f(a)\,g(b)$

(1) 证明：$(S,*)$为一个交换么半群

(2) 证明：f可逆当且仅当$f(1)\neq0$

(3) 称f为积性函数，如果$(m,n)=1$时有$f(mn)=f(m)f(n)$　证明：所有非零积性函数的全体在运算$*$下构成一个$Abel$群

(4) 称f为完全积性函数，如果对任意$m,n\in\mathbb{N}^*$有$f(mn)=f(m)f(n)$．所有非零完全积性函数的全体在运算$*$下是否构成一个$Abel$群？

Proof

(1) 交换性：$\sum\limits_{ab=n}f(a)\,g(b)$通过该式子显然可以得到　其次：考察么元设么元函数为e那么此时由交换性我们只需找到$f*e=f$即可

此时$\forall n\in\mathbb{N}^+$应有$f*e(n)=f(n)=\sum\limits_{ab=n}f(a)\,e(b)=f(1)\,e(n)+\cdots+f(n)\,e(1)=f(n)$

故我们构造么元函数$e:=\begin{cases}e(1)=1\\e(2,3\cdots)=0\end{cases}$即可

下面说明结合律：

$$(f*g)*h(n)=\sum_{d|n}h(d)\,(f*g)\left(\frac{n}{d}\right)=\sum_{d|n}h(d)\left(\sum_{k|n/d}f(k)\,g\left(\frac{n}{kd}\right)\right)=\sum_{abc=n}f(a)\,g(b)\,h(c)=f*(g*h(n))$$

所以$(S,*)$为一个交换么半群

(2) 若f可逆，从而存在$g\in S$，使得$f*g=e$，从而$f(1)g(1)=e(1)=1\Longrightarrow$则$f(1)\neq0$

若$f(1)\neq0$，下面归纳构造g使得其为f的逆，注意到$f(1)g(1)=1$，从而取$g(1)=\dfrac{1}{f(1)}$

则由$f(1)g(2)+f(2)g(1)=0$从而$g(2)=-\dfrac{f(2)g(1)}{f(1)}$

假设$k\leq n$均定义$g(k)$，则由$g(n+1)f(1)+\sum\limits_{d|n+1,d>1}g\left(\dfrac{n+1}{d}\right)f(d)=0$从而由$\dfrac{n+1}{d}\leq n$

从而有归纳假设可知为确定值,从而$g(n+1)$可被确定，故归纳可构造出g使得为f的逆.

(3) 此时f为非零积性函数此时我们有$f(1)=f(1\cdot 1)=f^2(1)$我们断言$f(1)\neq 0$且$f(1)=1$
不然$\forall m\in\mathbb{Z}^+$此时$f(m)=f(1\cdot m)=0$与非零函数矛盾
在运算$*$下构成一个$Abel$群其中交换性由(1),结合律同样由(1)保证保证
其次幺元函数$e:=\begin{cases} e(1)=1 \\ e(2,3\cdots)=0 \end{cases}$ 容易验证也为非零积性函数
下面说明封闭性此时两个非零积性函数在卷积下是否仍然为非零积性函数呢
对任意$m,n\in\mathbb{N}^*$，设$m=p_1^{a_1}\cdots p_t^{a_t},n=q_1^{b_1}\cdots q_s^{b_s}$，其中$p_i,q_j$互不相等，从而有

$$\begin{aligned} f*g(mn)&=\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\cdot\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\cdot\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\\ &=\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\right)\cdot f\left(\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\right)\cdot g\left(\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\\ &=\left[\sum_{x_1=0}^{a_1}\cdots\sum_{x_t=0}^{a_t}f\left(\prod_{i=1}^{t}p_i^{x_i}\right)g\left(\prod_{i=1}^{t}p_i^{a_i-x_i}\right)\right]\cdot\left[\sum_{y_1=0}^{b_1}\cdots\sum_{y_s=0}^{b_t}f\left(\prod_{j=1}^{s}q_j^{y_j}\right)g\left(\prod_{j=1}^{s}q_j^{b_j-y_j}\right)\right]\\ &=f*g(m)\cdot f*g(n)\end{aligned}$$

故可知$f*g$也为积性函数
下面说明逆元性：f为一非零积性函数此时要找到另一个非零积性函数g使得$fg=e$
此时仿照(2)的计算我们有$g(1)=1\quad f(1)g(2)+f(2)g(1)=0\Longrightarrow g(2)=-f(2)\cdots\cdots\Longrightarrow g(m)=\sum_{ab=m且b\neq m}f(a)g(b)$
上述给出了f的逆元函数g的算法(且特别的$g(p)=-f(p)$其中p为一素数)
且不难验证g的前面几项是满足积性函数条件的我们下面利用归纳法来证明g的积性函数性质
假设小于等于$k-1$之时满足积性条件：$g(ab)=g(a)g(b)$如果$(a,b)=1$这当$ab\leqslant k-1$成立
那么针对$g(k)$其中k为素数显然成立积性条件另一方面但k为合数时不妨证明$g(mn)=g(k)=g(m)g(n)$且$(m,n)=1$
设$m=p_1^{t_1}\cdots p_s^{t_s}$且$n=q_1^{l_1}\cdots q_k^{l_k}$做质因数分解此时且$p_1\sim p_s$与$q_1\sim q_k$互不相同
那么$g(mn)=g\left(p_1^{t_1}\cdots p_s^{t_s}q_1^{l_1}\cdots q_k^{l_k}\right)=g(m)g(n)$
故所有非零积性函数的全体在运算$*$下构成一个$Abel$群

(4) 设$f(n)=n$该非零完全积性函数但此时幺元函数$e:=\begin{cases} e(1)=1 \\ e(2,3\cdots)=0 \end{cases}$
但考虑f的逆元函数g通过计算前面四项发现$g(1)=1\quad g(2)=-f(2)=-2\quad g(3)=-f(3)=-3$
$f(4)+f(2)g(2)+g(4)=0\Longrightarrow g(4)=-4-(-4)=0$但是$g(4)\neq g(2)\cdot g(2)$矛盾
故不构成一个$Abel$群

Exercise 2.3

已知群$(\mathbb{Z},+)$　证明：设$m\in\mathbb{N}$,那么$m\mathbb{Z}=\{mn|\ n\in\mathbb{Z}\}$是$(\mathbb{Z},+)$的子群,除此之外群$(\mathbb{Z},+)$的子群都形如$m\mathbb{Z}$

Proof 容易验证整数加法群的幺元为0,不难知道$\forall k_1m$与$k_2m\in m\mathbb{Z}$那么$k_1m+k_2m=(k_1+k_2)m\in m\mathbb{Z}$
且$k_1m+(-k_2m)=(k_1-k_2)m\in m\mathbb{Z}$故由子群的判别定理知道即可
接下来证明整数加法群的子群结构此时：
设H为一子群,首先显然若H为$\{0\}$即幺元构成的单元素群显然也是符合结构特征的
故不妨设$H<\mathbb{Z},H$不是$\{0\}$,此时则有$0\neq m\in H\subseteq\mathbb{Z}$,那么不妨设$m>0$且不妨设$m$为$H$中绝对值最小的数
从而由归纳法不难证明$mn\in H$对任意$n\in\mathbb{Z}$,从而$m\mathbb{Z}\subseteq H$

又若存在$n \in H$且$m \nmid n$, 则考虑$d = \gcd(m, n)$, 则由*Bezout*定理, 存在$a, b \in \mathbb{Z}$, 使得$d = am + bn \in H$, 而$0 < d < m$
这与m的最小性矛盾！从而$H = m\mathbb{Z}$，即证.

✍ **Exercise 2.4** 在有限群里, 阶数大于2的元素个数一定是偶数。
更进一步表述 : $Group\ G\ , k\ is\ a\ integer > 2; amount\ of\ a\ that\ order\ (a) = k\ must\ be\ even\ number$

Proof 由本节的习题8可知, 元素a与a^{-1}的阶是相同的。也就是说, 如果a阶大于2, 则a^{-1}也大于2。
下面只需证明 : 群G中阶大于2的元素a与a^{-1}成对出现即可。
首先, $a \neq a^{-1}$, 如果$a = a^{-1}$, 即$a^2 = e$, 与a的阶大于2矛盾。其次, 如果两个阶大于2的元素a, b有$a \neq b$, 则必有$a^{-1} \neq b^{-1}$。

✍ **Exercise 2.5** 若群G中每一个元素都适合$x^2 = e$那么群G为交换群

Proof $\forall a, b \in G$要验证$ab = ba$而$x^2 = e$即$x = x^{-1}$
此时 $(ab) = b^{-1}a^{-1} = ba$

✍ **Exercise 2.6** 若群G的阶数为偶数那么群G中一定有奇数个二阶元

Proof 群G中若元素$x, |x| \geqslant 3$那么$\left|x^{-1}\right| = |x|$成对出现
且还有一个$\{e\}$单独, 那么就一定会有奇数个二阶元

✍ **Exercise 2.7** p^m(p为素数, $m \geqslant 1$)阶群一定有一个p阶子群

Proof 设G是一个p^m阶的群, 那么, 我们只需证明群G中存在p阶元
在G中任意取一个非单位元的元素a, 则由*Lagrange*定理的推论得 : $|a|$整除群G的阶p^m, 由于p是素数, 只有$|a| = p^k$(其中$1 \leqslant k \leqslant m$)
取$b = a^{p^{k-1}} \in G$, 则可知b的阶为p, 得$H = (b)$是一个G的p阶子群。

✍ **Exercise 2.8** 设G是6阶群, 则G中至少含有一个3阶子群H.

Proof 要证G中含有3阶子群, 其实只需证明G中含有3阶元素即可.
由于G为6阶群, 那么G中元素的阶只能是$1, 2, 3, 6$.假设G中没有3阶元, 那么G中也不能有6阶元
如果G中的元素a为6阶元, 那么a^2即为3阶元, 与G中没有3阶元矛盾.
也就是说, 当G中没有3阶时, G中的元素只能是1阶元与2阶元, 即G中除单位元e外的五个元素都是2阶元.从而知G是交换群
在G中取两个2阶元a, b, 则有$ab \in G$, 易知$ab \neq e, ab \neq a, ab \neq b$, 这样我们在$G$中得到一个含有4个元素的子集$K = \{e, a, b, ab\}$
且满足 : $a^2 = e, b^2 = e, (ab)^2 = e$.根据上面的讨论可得运算表 :

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

则$K \cong B_4$是G的一个子群, 由$Lagrange$定理知G的子群K的阶整除G的阶, 即4整除6, 矛盾.
因此, G中必存在3阶元g, 则$H = (g)$即为G的3阶子群.

Exercise 2.9 设G是群, $|G| = mp, p$是素数, $m < p$.证明 : G的p阶子群是G的不变子群。

Proof 设G的p阶子群显然素数阶群为循环群, 此时 WTS : $\forall x \in G \ \ xHx^{-1} = H$
不妨设$H = \left\{e, a \cdots a^{p-1}\right\} \quad xHx^{-1} = \left\{e, b, \cdots b^{p-1}\right\}$
假设$xHx^{-1} \neq H$此时$xHx^{-1} \cap H < H$那么$Ord\left(xHx^{-1} \cap H\right) | Ord\left(H\right)$
那么$Ord\left(xHx^{-1} \cap H\right)$要么为$p$要么为1
如果$Ord\left(xHx^{-1} \cap H\right)$为$p$那么两个群应该完全相等那么$xHx^{-1} = H$与假设矛盾
如果$Ord\left(xHx^{-1} \cap H\right)$为1即只有$e$单位元处于交集中
那么断言$\left\{a_s b_j : \ a_s \in H; b_j \in xHx^{-1}\right\}$两两不同
若不然存在$a_s \neq a_m$或者$b_j b_n$使得$a_s b_j = a_m b_n \Rightarrow \underbrace{a_m^{-1} a_s}_{\in H} = b_n b_j^{-1} \in xHx^{-1}$
所以$b_n b_j^{-1} = a_m^{-1} a_s \in \left(xHx^{-1} \cap H\right) = e \Longrightarrow a_s = a_m$另一方面同理矛盾
故$xHx^{-1} = H$

Exercise 2.10 设A, B是G的子群, C是由$A \cup B$生成的子群, 若B是C的不变子群, 则$C = AB$

Proof 要证明此题, 首先要清楚题中的几个集合 :
$AB = \{ab \mid a \in A, b \in B\}$;
根据生成子群的结构, 我们有$C = (A \cup B) = \{x_1 x_2 \cdots x_n \mid x_i \in A \cup B\}$, 再将同一个子群中的元素合并, 则可得
$C = \left\{a_1 b_1 a_2 b_2 \cdots a_k b_k \mid a_i \in A, \quad b_j \in B\right\}$
从上面两个集合的结构显然可得 : $AB \subseteq C$;
反之, $\forall a_1 b_1 a_2 b_2 \cdots a_k b_k \in C$, 因为$b_1 a_2 \in B a_2$, 由于$B$是$C$的不变子群, 从而有$b_1 a_2 \in B a_2 = a_2 B$, 则存在$b_1' \in B$使得$b_1 a_2 \in a_2 b_1'$, 所以
$a_1 b_1 a_2 b_2 \cdots a_k b_k = a_1 \left(b_1 a_2\right) b_2 \cdots a_k b_k$
$= a_1 \left(a_2 b_1'\right) b_2 \cdots a_k b_k = \left(a_1 a_2\right) \left(b_1' b_2\right) \cdots a_k b_k$,
以此类推可得$a_1 b_1 a_2 b_2 \cdots a_k b_k = \left(a_1 a_2 \cdots a_k\right) b_k' \in$ AB, 得$C \subseteq AB$。所以我们证得 : $AB = C$。

Exercise 2.11 设G是一个群, $a, b \in G$, 记$\langle a, b\rangle = a^{-1} b^{-1} ab$, 称为$G$的换位元
证明 :
(1)G的有限个换位元的乘积全体所成的集合G'是G的不变子群
(2)G/G'为交换群
(3)若$H \triangleleft G$, 且G/H为交换群, 则$G' \subseteq H$ (即在群G中为G的正规交换子群中, 最小的就是换位子群)

Proof (1)设$\alpha,\beta\in G'$,即$\begin{cases}\alpha=\langle a_1,b_1\rangle\langle a_2,b_2\rangle\cdots\langle a_k,b_k\rangle,\\ \beta=\langle c_1,d_1\rangle\langle c_2,d_2\rangle\cdots\langle c_l,d_l\rangle,\end{cases}$
有$a\beta=\langle a_1,b_1\rangle\cdots\langle a_k,b_k\rangle\langle c_1,d_1\rangle\cdots\langle c_l,d_l\rangle\in G'$
由于$\langle a,b\rangle^{-1}=\left(a^{-1}b^{-1}ab\right)^{-1}=b^{-1}a^{-1}ba=\langle b,a\rangle\in G'$
有$a^{-1}=[\langle a_1,b_1\rangle\langle a_2,b_2\rangle\cdots\langle a_k,b_k\rangle]^{-1}=\langle a_k,b_k\rangle^{-1}\cdots\langle a_2,b_2\rangle^{-1}\langle a_1,b_1\rangle^{-1}=\langle b_k,a_k\rangle\cdots\langle b_2,a_2\rangle\langle b_1,a_1\rangle\in G'$。
至此我们验证了子群,下面验证正规性
$\forall x\in G,\langle a,b\rangle\in G'$,有
$x\langle a,b\rangle x^{-1}=x\left(a^{-1}b^{-1}ab\right)x^{-1}$
$=\left(xa^{-1}x^{-1}\right)\left(xb^{-1}x^{-1}\right)\left(xax^{-1}\right)\left(xbx^{-1}\right)$
$=\left(xax^{-1}\right)^{-1}\left(xbx^{-1}\right)^{-1}\left(xax^{-1}\right)\left(xbx^{-1}\right)$
$=\langle xax^{-1},xbx^{-1}\rangle\in G'$,
所以,$xax^{-1}=x\langle a_1,b_1\rangle\langle a_2,b_2\rangle\cdots\langle a_k,b_k\rangle x^{-1}=\left(x\langle a_1,b_1\rangle x^{-1}\right)\left(x\langle a_2,b_2\rangle x^{-1}\right)\cdots\left(x\langle a_k,b_k\rangle x^{-1}\right)\in G'$,
从而证得G'是G的一个不变子群

(2)$\forall aG',bG'\in G/G'$,因为由于$(aG')(bG')=(ab)G'$与$(bG')(aG')=(ba)G'\Longrightarrow(ba)^{-1}ab=a^{-1}b^{-1}ab=\langle a,b\rangle\in G'$
所以,$(aG')(bG')=(ab)G'=(ba)G'=(bG')(aG')$,证得:$G/G'$为交换群

(3)$\forall a,b\in G$,由于G/H是交换群,则有$(ab)H=(aH)(bH)=(bH)(aH)=(ba)H$
得$\langle a,b\rangle=a^{-1}b^{-1}ab=(ba)^{-1}ab\in H$,即证得$H$中包含所有的换位元$\langle a,b\rangle$
由于H是G的子群,因此H关于G的运算封闭,所以H中包含所有有限个换位元的乘积,即$G'\subseteq H$

✍ **Exercise 2.12** 设H是群G的非空子集,并且H的每一个元素的阶都有限
证明:H为G的子群的充分必要条件为:对于$\forall a,b\in H$有$ab\in H$。

Proof 必要性显然。而对于充分性,我们只需证:$\forall a\in H$,有$a^{-1}\in H$
因为$a\in H$,而H中的元素都是有限阶的,即存在正整数m,使得$a^m=\underbrace{aa\cdots a}_{m个a}==e$,得$a^{-1}=a^{m-1}$在$G$中
且$a^{m-1}=aa\cdots a$有$\forall a,b\in H$有$ab\in H$性质知道$a^{m-1}\in H$故$a^{-1}\in H$

✍ **Exercise 2.13** 设H是G的一个子群,且$[G:H]=2$,则H是G的正规子群.
特别的$A_n\lhd S_n$

Proof $\forall a\in G$,若$a\in H$,那么有$aH=H=Ha$.
若$a\notin H$,则$aH\cap H=\varnothing$,由题设$[G:H]=2$,故$G=H\cup aH$,同样有$G=H\cup Ha,H\cap Ha=\varnothing$.
也就是说,由$H\cup aH=H\cup Ha$和$H\cap aH=H\cap Ha=\varnothing$,得$aH=G-H=Ha$,即对于$\forall a\in G$,均有$aH=Ha$.得$H$是$G$的正规子群.

✍ **Exercise 2.14** 1.设G是群,H,K,L都为G的子群,如果$H\subseteq K\cup L$则$H\subseteq K$或者$H\subseteq L$
2.一个群不可以写为两个真子群的并

3.一个群有可能可以写为三个真子群的并

Proof 1.同理取集合差的元素

2.反证法如果可以$G=A\cup B$其中A，B都是G的真子群

首先显然的有$A\neq B$不然就与$G=A\cup B$矛盾了

取$a=A-B\quad b=B-A$

那么有$ab\in G=A\cup B$

那么不妨设$ab\in A\Rightarrow b\in A$矛盾。同理可证另一方向

证毕

3.例如$Klein$四元群中每个元素都是二阶即可

✍ **Exercise 2.15** 设H为群G的非空有限子集,那么$H<G\Leftrightarrow\forall a,b\in H$有$ab\in H$

该定理说明判断一非空有限子集只需要判断封闭性即可

Proof 先说明充分性

我们断言$\langle x\rangle$由x生成群中必定存在$k,l\in\mathbb{Z}^+\quad st.x^k=x^l$

若不然那么对于任何的k,l都不存在$x^k=x^l$那么$\langle x\rangle$生成群无限阶了而我们知道$\langle x\rangle\subseteq G$

这与G群的阶有限矛盾

$\Longrightarrow$我们一定可以得到形如$x^s=x^t$的形式那么就有如下$x^{-1}=x^k$的形式

进而而x^k由条件封闭性知道属于G故x^{-1}也属于G

故我们说明了逆元封闭性，乘积封闭性,故为子群

必要性显然

✍ **Exercise 2.16** 设交换群G中元素的最大阶数为n,则G中每一个元素的阶数都是n的因子

Proof 反证法

设$o(g)=n\quad\forall a\in G$ 设$o(a)=n_0$若$n_0\nmid n$

由素数分解我们可以设$n=p^rl\quad n_0=p^sk$

因为最大的阶数是n且$n_0\nmid n$那么一定会有$r<s$或$l<k$其中一个严格成立不妨设为$k>l$

$o(g^l)=\dfrac{n}{(n,l)}=p^r\quad o\left(a^{p^s}\right)=\dfrac{n_0}{(n_0,p^s)}=k$

那么$o\left(g^la^{p^s}\right)=kp^r>lp^r=n$与最大阶数为$n$矛盾

反证法,设$a^n=e$与$b^l=e$且$l<n,l\nmid n$

设$d=(n,l)$则$o\left(b^d\right)=\dfrac{l}{(l,d)}=\dfrac{l}{d}$

那么因为a与b^d可交换且$o(a)=n$与$o\left(b^d\right)=\dfrac{l}{d}$互素那么$o\left(ab^d\right)=n\cdot\dfrac{l}{d}$

断言$n\dfrac{l}{d}>n\Longleftrightarrow l>d$若不然因为$d=(n,l)$得到$l=d$得到$l\mid n$矛盾

✍ **Exercise 2.17**

设G为一有限交换群

G为循环群的充分必要条件是对于所有正整数m，在G中适合方程$x^m = e$的元素个数不超过m

Proof 先证充分性。按上个定理，在G中有一个元素g，它的阶n是G中所有元素的阶的倍数
换句话说，群G中所有元素都适合方程$x^n = e$由定理的条件不超过n个则，$|G| \leqslant n$
显然$e, g, g^2 \cdots g^{n-1}$都在G中故，$n \leqslant |G|$，因而$|G| = n$. 这就证明了$G = \langle g \rangle$为循环群.
必要性显然

✍ **Exercise 2.18** 设 $\mathrm{SL}(n, \mathbb{Z})$的元素为整数且行列式为1的$n$阶方阵的全体.
(1)证明 : $\mathrm{SL}(n, \mathbb{Z})$是 $\mathrm{GL}(n, \mathbb{R})$的子群.
(2)设$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
证明 : 其中任两个元素都是 $\mathrm{SL}(2, \mathbb{Z})$的生成元.

Proof

✍ **Exercise 2.19** 设G为一奇数阶群，那么G中任何一个元都是一个唯一确定的元的平方

Proof $\forall x \in G$那么$x^{2k+1} = e \Rightarrow \left(x^{k+1}\right)^2 = x$
唯一性我们要运用好有限群的性质有限群上的单射即满射，满射即单射
故构造$\varphi : x \to x^2$故根据第一行我们显然知道为满射此时那么也为单射故唯一性证毕

✍ **Exercise 2.20** 设G为群，$H < G$. $N \lhd G$，若 $[G : H]$和$|N|$互素，则N是H的正规子群

Proof 若$N \lhd G$, 则$HN < G$, 因 $[NH : H] < [G : H]$有限, 从而有 $[N : N \cap H] = [NH : H]$
首先, $[NH : H] \mid [G : H] = q \Longleftarrow [G : H] = [G : NH][NH : H]$
其次 $[NH : H] = [N : N \cap H] \| N| = p \Longleftarrow |N| = [N : N \cap H] | N \cap H \mid$
从而 $(p, q) = 1 \Longrightarrow [NH : H] = 1 \Longrightarrow NH = H \Longrightarrow N < H$
而N正规了故$N \lhd H$

✍ **Exercise 2.21** 设H是群G的正规子群, $|H| = n$, $[G : H] = m$, 且 $(m, n) = 1$.证明 : H是G的唯一的n阶子群.

Proof 有上文显然 $|G| = mn$为有限群, 假设还有一n阶子群T, 那么 $[G : T] = m$由上个命题直$T \lhd H$但是二者均是n阶故二者相等
故只唯一的一个n阶子群H

✍ **Exercise 2.22** $N < G, H < G, (|N|, |G : H|) = 1$, 若$N, H$中有一个是正规子群，则$N < H$.

Proof 设$|N| = p$, $|G : H| = q$
(1)若$H \lhd G$，考虑典范满同态$\pi : G \to G/H, \ker\pi = H$

首先, 由第一同构定理Q有$\pi(N) \cong N/\ker\pi \Rightarrow |\pi(N)| = \dfrac{|N|}{|\ker\pi|} \Longrightarrow |\pi(N)|||N| = p$

其次$N < G \Longrightarrow \pi(N) < G/N \Longrightarrow |\pi(N)|||G/N| = q$

而 $(p,q) = 1 \Longrightarrow |\pi(N)| = 1 \Longrightarrow \pi(N) = e' \Longrightarrow N < H$

(2)若$N \triangleleft G$, 则$HN < G$, 因 $[NH : H] < [G : H]$有限, 从而有 $[N : N \cap H] = [NH : H]$

首先, $[NH : H] \mid [G : H] = q \Longleftarrow [G : H] = [G : NH][NH : H]$

其次 $[NH : H] = [N : N \cap H]||N| = p \Longleftarrow |N| = [N : N \cap H]|N \cap H|$

从而 $(p,q) = 1 \Longrightarrow [NH : H] = 1 \Longrightarrow NH = H \Longrightarrow N < H$

✍ **Exercise 2.23** 试证有限群G的一个真子群的全部共轭子群之并不能覆盖整个群G.结论对无限群是否成立?

Proof 设H是G的真子群, 则H共有 $[G : N_G(H)]$ 个共轭子群.令Σ是H的所有共轭子群之并, 则

$$\underbrace{|\Sigma| \leqslant (|H| - 1)\,[G : N_G(H)] + 1}_{\text{每个共轭子群都有单位元会重复}} = \frac{|G|}{|N_G(H)|} \cdot |H| - [G : N_G(H)] + 1.$$

若H是正规子群, 则$N_G(H) = G$, 于是$|\Sigma| \leqslant |H| - 1 + 1 = |H| < |G|$.

若H不是正规子群, 则$N_G(H) \neq G$, 于是 $[G : N_G(H)] > 1, |\Sigma| \leqslant \dfrac{|G|}{|H|} \cdot |H| - [G : N_G(H)] + 1 < |G| - 1 + 1 = |G|$.

综合以上, $|\Sigma| < |G|$, 即H的全部共轭子群之并不能覆盖G.

这一结论对无限群不再成立.例如, 令$G = GL(n,\mathbb{C})$, H是n阶上三角可逆复矩阵作成的真子群.

由$Jordan$标准型知任一n阶可逆阵A相似于某一H中的元, 这表明G是H的所有共轭子群之并.

✍ **Exercise 2.24**

设G是一个群.那么$a \to a^{-1}$是G的自同构 $\Longleftrightarrow$ G是交换群;

Proof 记映射$a \to a^{-1}$为σ.因G是群, 故σ是G到G的一一对应.

若σ是G的自同构, 则由$\sigma(a)\sigma(b) = \sigma(ab) = (ab)^{-1} = b^{-1}a^{-1} = \sigma(b)\sigma(a), \quad \forall a, b \in G$, 知$G$是$Abel$群.

反之, 若G是$Abel$群, 则由$\sigma(ab) = (ab)^{-1} = b^{-1}a^{-1} = \sigma(a)\sigma(b), \quad \forall a, b \in G,$

✍ **Exercise 2.25** 设α是群G的自同构且满足 : 若$\alpha(g) = g$, 则$g = e$.证明下列结论 :

1)$g \to \alpha(g)g^{-1}$是单射的;

2)若G是有限群, 则G的每个元素均可写成$\alpha(g)g^{-1}$形式;

3)又若$\alpha^2 = \mathrm{id}_G$, 则G为奇数阶交换群.

Proof 1)设$g_1, g_2 \in G$, 且$\alpha(g_1)g_1^{-1} = \alpha(g_2)g_2^{-1}$.于是$\alpha(g_2)^{-1}\alpha(g_1) = g_2^{-1}g_1$.由$\alpha$是自同构, 知$\alpha\left(g_2^{-1}g_1\right) = g_2^{-1}g_1$.再由$\alpha$的性质知$g_1 = g_2$.

故$g \to \alpha(g)g^{-1}$是单射的.

2)若G是有限群, 又已知$g \to \alpha(g)g^{-1}$是单射的, 故$|G| = \left|\left\{\alpha(g)g^{-1} \mid g \in G\right\}\right|$.于是$G = \left\{\alpha(g)g^{-1} \mid g \in G\right\}$, 则$G$的每个元素均可写成$\alpha(g)$

3)由于对任何$h \in G$, 有$g \in G$使得$h = \alpha(g)g^{-1}$, 故$h^{-1} = g\alpha\left(g^{-1}\right)$.此外, $\alpha(h) = \alpha^2(g)\alpha\left(g^{-1}\right) = g\alpha\left(g^{-1}\right)$, 于是$\alpha(h) = h^{-1}$.

此时说明群为交换群：$\forall m,n\in G$此时有α为G上自同构所以$m=\alpha\left(g_1\right),n=\alpha\left(g_2\right)$
$mn=\alpha\left(g_1g_2\right)=g_2^{-1}g_1^{-1}=\alpha\left(g_2\right)\alpha\left(g_1\right)=nm$故为$Abel$群
此时$\forall g\in G$我们有$\alpha\left(g\right)=g^{-1}=g\Longrightarrow g=e$这也意味着在$G$中二阶元的只有一个$e$
故此时考察一阶元二阶元只有e,考察三阶元及其以上都必定是a与a^{-1}成对故共奇数阶

✍ **Exercise 2.26** 设G是奇数阶有限群,$\alpha\in\mathrm{Aut}(G)$且$\alpha^2=1$.令$G_1=\{g\in G\mid\alpha(g)=g\},\quad G_{-1}=\left\{g\in G\mid\alpha(g)=g^{-1}\right\}$.
试证：$G=G_1G_{-1}$且$G_1\cap G_{-1}=1$.

Proof 知$(2,|G|)=1$,那么$\varphi:G\to G\quad g\mapsto g^2$是群自同构.因此$G$中任一元均可写成某一元的平方的形式.
对任一$g\in G$,设$g^{-1}\alpha(g)=x^2$.因$\alpha(x)^2=\alpha\left(g^{-1}\alpha(g)\right)=\alpha(g)^{-1}g=\left(g^{-1}\alpha(g)\right)^{-1}=x^{-2}$
由群同构知道$\alpha(x)=x^{-1}$,即$x\in G_{-1}$.
又因为$\alpha(gx)=\alpha(g)\alpha(x)=\alpha(g)x^{-1}=gx$,即$gx\in G_1$,故$g=(gx)x^{-1}\in G_1G_{-1}$,即$G=G_1G_{-1}$.
若$g\in G_1\cap G_{-1}$,则$g^2=1$.但$|G|$是奇数,故$g=1$,即$G_1\cap G_{-1}=1$.

✍ **Exercise 2.27**
设G是有限$Abel$群，构造$\varphi_k:G\to G\quad g\mapsto g^k$该由$k$诱导的映射
证明：$\varphi_k\in Hom\left(G\right)$且$\varphi_k$是$G$的自同构$\Longleftrightarrow k$和$|G|$互素.

Proof 显然$\varphi_k\in Hom\left(G\right)$是$G$上的自同态,且我们知道在有限群上映射为自同构当且仅当为单射或者满射
一方面：若$(k,|G|)=1,$,我们来证明此时φ_k为单射.于是任取$g^k=h^k$此时$WTS:g=h$
设$o\left(g\right)=d_1$与$o\left(h\right)=d_2$而我们知道$d_1\mid|G|$与$d_2\mid|G|\Longrightarrow(k,d_1)=1$且$(k,d_2)=1\Longrightarrow(k,d_1d_2)=1$
故存在u,v使得$uk+vd_1d_2=1$故$g=g^{uk+vd_1d_2}=\left(g^k\right)^u=\left(h^k\right)^u=h^{uk+vd_1d_2}=h$

另一方面,若φ_k为G上的自同构,我们来证k与$|G|$互素.
反证法若$(k,|G|)=d>1$　我们来说明φ_k实际上不是单射,我们希望找到一个$g\neq e$使得$\varphi_k\left(g\right)=g^k=e$
此时我们有$\left(\frac{k}{d},|G|\right)=1$那么由必要性我们就是知道$\varphi_{k/d}$为$G$上自同构
于是乎我们希望找到一个$g\neq e$使得，$\left(g^d\right)^{k/d}=e$由$\varphi_{k/d}$为G上自同构,故我们希望找到$g\neq e$使得$g^d=e$
那么任取$e\neq h\in G$(此时我们默认$|G|>1$否则是显然的),不妨设$o\left(h\right)=m$
$(m,k)\mid d$此时$h^{m\cdot\frac{d}{(m,k)}}=\left(h^{\frac{m}{(m,k)}}\right)^d=e$且断言$h^{\frac{m}{(m,k)}}\neq e$否则与$o\left(h\right)=m$矛盾
故$h^{\frac{m}{(m,k)}}$就是我们希望找到的g

✍ **Exercise 2.28** 举例说明下面的命题不正确：设G,G'是群，$N\triangleleft G,N'\triangleleft G'$，且有$G\simeq G',N\simeq N'$，则必有$G/N\simeq G'/N'$

Proof 我们考虑$G=G'=\{\mathbb{Z},+\},N=2\mathbb{Z}\simeq\mathbb{Z},N'=3\mathbb{Z}\simeq\mathbb{Z}$，从而$N\simeq N'$
但显然$G/N=\mathbb{Z}_2\ncong\mathbb{Z}_3=G'/N'$从而既是一个反例.

✍ **Exercise 2.29** 设p是一个奇素数. 对任意$a \in \mathbb{Z}_p^*$，定义$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{存在} b \in \mathbb{Z}_p^* \text{ 使得} a \equiv b^2 (\mathrm{mod} p), \\ -1, & \text{不存在} b \in \mathbb{Z}_p^* \text{ 使得} a \equiv b^2 (\mathrm{mod} p). \end{cases}$

(1) 证明 : $\varphi(a) = \left(\frac{a}{p}\right)$是$\mathbb{Z}_p^*$到$\{1,-1\}$的满同态

(2) 证明 : 由题, 定义$f_2 : \mathbb{Z}_p^* \to \mathbb{Z}_p^* \ \ a \to a^2$说明$f_2$是$\mathbb{Z}_p^*$的自同态且$\mathbb{Z}_p^*/\mathrm{Im} f_2 \cong \{1,-1\}$, 记同构映射为$\psi$.

进一步，$\varphi = \psi \circ \pi$，其中，π是$\mathbb{Z}_p^*$到$\mathbb{Z}_p^*/\mathrm{Im} f_2$的自然同态.

Proof (1) 我们先证明这是满射, 显然$\varphi(1) = 1$

且若假设不存在$\varphi(a) = -1$, 从而任意$a \in \mathbb{Z}_p^*$, 存在b_a使得$a \equiv b_a^2 (\mathrm{mod} p)$, 从而$\left(\mathbb{Z}_p^*\right)^2 = \mathbb{Z}_p^*$

但注意到$1^2 \equiv (p-1)^2 (\mathrm{mod} p)$, 从而可知矛盾, 因此一定存在$a$使得$\varphi(a) = -1$

下证其是一个同态, 我们考虑证明如下的*Euler*判别法, 即成立$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p), \quad \forall a \in \mathbb{Z}_p^*$

(i) 若a可被平方表示, 从而有$a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 (\mathrm{mod} p)$，其中用到了*Fermat*小定理

(ii) 若a不可被平方表示, 从而有任意$i \in \mathbb{Z}_p^*$存在$j \in \mathbb{Z}_p^*$满足$ij \equiv a (\mathrm{mod} p)$, 因为只需要取$j = i^{-1}a$即可

那么根据上述说法我们就可以把$1 \sim p-1$分成$\frac{p-1}{2}$对, 每一对相乘模p余a

对所有数乘积则得$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 (\mathrm{mod} p)$其中用到了*Wilson*定理

从而综上可知*Euler*判别法成立

因此利用*Euler*别法，不难看到φ为一个同态，进而为满同态

(2) 定义f_2显然为$\mathbb{Z}_p^*$上的自同态, $Ker\varphi = \left\{a \in \mathbb{Z}_p^* : \ \left(\frac{a}{p}\right) = 1\right\}$且$\mathrm{Im} f_2 = Ker\varphi$

由同态第一基本定理即可

✍ **Exercise 2.30**

证明 : $(\mathbb{Q}, +)$ 的任一有限生成子群必是循环群

Proof 任意有限生成子群$S = \langle \frac{q_1}{p_1}, \cdots, \frac{q_n}{p_n} \rangle$

设$P = p_1 \cdots p_n, \quad Q = \gcd(q_1 p_2 \cdots p_n, \cdots, q_n p_1 \cdots p_{n-1})$ 下证$S = \langle \frac{Q}{P} \rangle$

一方面, 任一$g \in S$, 可知其可表示为$g = \sum_{i=1}^{n} k_i \cdot \frac{q_i}{p_i} = \frac{1}{P} \sum_{i=1}^{n} k_i q_i p_1 \cdots \widetilde{p_i} \cdots p_n = K \cdot \frac{Q}{P} \in \langle \frac{Q}{P} \rangle$从而$S \subseteq \langle \frac{Q}{P} \rangle$

另一方面由*Bezout*定理，可知$\frac{Q}{P} \in S$，从而$S = \langle \frac{Q}{P} \rangle$，即证任一有限生成子群为循环群

✍ **Exercise 2.31**

群G若只有有限个子群 $\Longleftrightarrow$ G为有限群

Proof 一方面：G为有限群那么, G的子集也就总共$2^{|G|}$个有限故G也只有有限个子群

另一方面：若G为无限群我们断言G有无穷个子群, 我们下面分两步来证明断言

第一步 : 若G中有无限阶元g, 那么对于任意的素数p, $\langle g^p \rangle$为G的子群且这些子群互不相同, 若不然则$\langle g^{p_1} \rangle = \langle g^{p_2} \rangle$

得到$g^{p_1} = (g^{p_2})^k \Longrightarrow g$的阶有限矛盾, 故我们断言了$G$有无穷个子群

第二步 : 若G中每个元阶数都有限, 断言G有无穷个子群, 若不然, G仅有有限个子群

先取G中元g_1, 得到$\langle g_1 \rangle$为一子群，因为每个元阶有限那么g_1自然也有限.那么$\langle g_1 \rangle$就为一个有限群

此时因为G为无限群那么在$G \setminus \langle g_1 \rangle$中选取$g_2$构造$\langle g_2 \rangle$为一有限群

类似的我们可以构造诸如此类,但注意到G仅有有限个子群故这样的操作在有限步停止
但是我们构造的都是有限群,这样有限群的个数也只有有限个,与$|G|=\infty$矛盾,故断言成立
证毕

✍ **Exercise 2.32**

S_n的中心$C(S_n)$
当$n=1$是$C(S_n)=S_n=\{id\}$,当$n=2$时$C(S_n)=S_n=\{(1),(12)\}$,当$n\geqslant 3$时$C(S_n)=\{(1)\}$

Proof $n=1.2$情况显然下当$n\geqslant 3$时
设$\sigma\in S_n$且$\sigma\neq 1$,从而存在指标i使得$\sigma(i)=j\neq i$，因为$n\geqslant 3$从而可以取到$k\neq j,k\neq i$
从而考虑$\tau=(jk)$，从而$\tau\sigma(i)=\tau(j)=k,\sigma\tau(i)=\sigma(i)=j$，从而$\sigma\tau\neq\tau\sigma$，即$\sigma\notin C(S_n)$，从而即证.

✍ **Exercise 2.33**

1.置换群G中若有奇置换,则G中一定有指数为2的正规子群
2.设$G=2n$.其中n为奇数,证明:G有指数为2的正规子群

Proof 1.置换群G实际上为一个S_n对称群的子群,此时若G中有奇置换φ
此时,将G中偶置换集合记作H,显然H是G的正规子群.此时G中任一奇置换ψ
$\varphi^{-1}\psi$为一偶置换记作$\varphi^{-1}\psi=h\Longrightarrow\psi=\varphi h$故$G=H\cup\varphi H$
故G中有H该指数为2的正规子群

2.根据$Caley$定理我们有$G\cong S$其中S为S_{2n}的一个子群　记同构映射为$\varphi:G\to S\ \ g\mapsto L_g$
下面证明S有一指数为2的正规子群,此时$|S|=|G|=2n$为偶数阶则S中有二阶元L_h
则我们可以将L_h写为若干不相交的对换乘积$\left(\text{这是由于}L_h\text{二阶得到的}\right)$,且对于$\forall a\in G$，$L_h(a)=ha\neq a\left(\text{否则}h=e\text{与阶矛盾}\right)$
因此每个元素均在对换中出现$\left(\text{否则若}k\text{不在出现则}L_h(a)=a\right)$,从而$L_h$为$n$个不相交的对换乘积,从而为奇置换
进而有1.可得

✍ **Exercise 2.34** 设G是群，$a\in G$是有限阶元且$\operatorname{ord}(a)=mn$且$\gcd(m,n)=1$
(1) 存在$b,c\in G$满足$bc=cb,\operatorname{ord}(b)=m,\operatorname{ord}(c)=n,a=bc$
(2) 如果$b',c'\in G$也满足$b'c'=c'b',\operatorname{ord}(b')=m,\operatorname{ord}(c')=n,a=b'c'$；那么$b'=b,c'=c$

Proof (1) 因为$\gcd(m,n)=1$，存在整数s,t使得$ms+nt=1$此时$(s,n)=(t,m)=1$
而$a=a^1=a^{ms+nt}=a^{ms}a^{nt}$令$b=a^{nt},c=a^{ms}$；则$a=bc,bc=cb$，且
$$\operatorname{ord}(b)=\operatorname{ord}(a^{nt})=\frac{mn}{\gcd(nt,mn)}=\frac{m}{\gcd(t,m)}=m$$
$$\operatorname{ord}(c)=\operatorname{ord}(a^{ms})=\frac{mn}{\gcd(ms,mn)}=\frac{n}{\gcd(s,n)}=n$$
证毕

(2) 由于$bc=cb,\operatorname{ord}(b)=m,\operatorname{ord}(c)=n$，所以$a^{nt}=(bc)^{nt}=b^{nt}c^{nt}=b^{nt}\cdot 1=b^{1-ms}=b^1b^{-ms}=b(b^m)^{-s}=b$
同样有$b'c'=c'b',\operatorname{ord}(b')=m,\operatorname{ord}(c')=n$
所以同样计算得$b'=a^{nt}$。故$b'=b$。类似地证明$c'=c$

✍ **Exercise 2.35** 若一无限群G是循环群 $\Longleftrightarrow$ 能够与其任一非平凡真子群同构

Proof $\Longrightarrow$：设G为无限循环群，则G同构于$(\mathbb{Z},+)$，而$\mathbb{Z}$加法群的子群都形如$m\mathbb{Z}$形式
$\Longleftarrow$：若G为无限但不循环群，则任取$e\neq g\in G$则$\langle g\rangle$为G的一循环真子群$\left(\text{若}\langle g\rangle=G\text{则}G\text{循环与一开始假设矛盾}\right)$
此时又$g\neq e$则$\langle g\rangle$为一循环非平凡真子群，则$G\cong\langle g\rangle$故G为循环群矛盾

✍ **Exercise 2.36** 令H,K,N都为G的子群且有$H<K$，$H\cap N=K\cap N$，且$HN=KN$
则有$H=K$(证明相互包含)

Proof

✍ **Exercise 2.37** 令G的阶为$2n$，则G包含二阶元，且若n为奇数且G为$abel$群，则仅仅只有一个二阶元

Proof G包含二阶元是肯定的，因为只要a不是二阶元，此时a与a^{-1}是同阶元配对的
故G只要为偶数阶的，则G的二阶元一定是奇数个
若n为奇数且G为$abel$群，则仅仅只有一个二阶元
若不然G不仅仅只有一个二阶元，则G至少还有两个二阶元记作b,c
此时构造子群$\{e,a,b,ab\}$则由拉格朗日定理$4|2n\Longrightarrow 2|n$但n为奇数矛盾

✍ **Exercise 2.38**
1.设H，K为G的子群，则$[H\vee K:H]\geqslant[K:H\cap K]$其中$H\vee K=\langle H\cup K\rangle$
2.若$p>q$均为素数，则一个阶为pq的群，至多只有一个阶为p的子群

Proof 设$\mathscr{A}$与$\mathscr{L}$分别是K对$H\cap K$陪集全体　与　$H\vee K$对H陪集全体
设$\varphi:\mathscr{A}\to\mathscr{L}\quad(H\cap K)k\mapsto Hk$
此时$Hk_1=Hk_2\Longleftrightarrow k_2k_1^{-1}\in H\Longleftrightarrow k_2k_1^{-1}\in H\cap K\Longrightarrow(H\cap K)k_1=(H\cap K)k_2$
故φ为单射此时$[H\vee K:H]\geqslant[K:H\cap K]$

若H，K为两个不同的阶为p的子群，则此时
$H=\left\{e,a\cdots a^{p-1}\right\}\quad K=\left\{e,b\cdots b^{p-1}\right\}$均为循环群
H中任一非e的元均为生成元，K中任一非e的元均为生成元
则若$H\cap K\neq\{e\}$则$H=K$故矛盾
故$H\cap K=\{e\}$利用1.再次得到矛盾

✍ **Exercise 2.39**

Let $N<S_4$ consist of all those permutations σ such that $\sigma(4)=4$. Is N normal in S_4?

Proof No, N is not normal in S_4.

Recall that a subgroup N of a group G is normal if for every $g \in G$ and every $n \in N$, the conjugate $gng^{-1} \in N$. Here, $G = S_4$ and N is the subgroup of permutations that fix 4, which is isomorphic to S_3.

To show that N is not normal, we exhibit a counterexample. Consider the permutation $n \in N$ given in cycle notation as $n = (1\ 3)$, which swaps 1 and 3 and fixes 2 and 4. Thus, $n(4) = 4$. Now consider $g \in S_4$ given by $g = (3\ 4)$, which swaps 3 and 4. Note that $g^{-1} = (3\ 4)$ as well.

We compute the conjugate gng^{-1} and evaluate it at 4:

$$(gng^{-1})(4) = g(n(g^{-1}(4))).$$

Since $g^{-1}(4) = 3$, we have:

$$n(g^{-1}(4)) = n(3) = 1 \quad \text{(because } n \text{ swaps 1 and 3)}.$$

Then:

$$g(n(g^{-1}(4))) = g(1) = 1 \quad \text{(because } g \text{ fixes 1)}.$$

Thus, $(gng^{-1})(4) = 1 \neq 4$, so $gng^{-1} \notin N$. Therefore, N is not normal in S_4.

✍ Exercise 2.40

If H is a cyclic subgroup of a group G and H is normal in G, then every subgroup of H is normal in G.

Proof

Let H be a cyclic subgroup of a group G and H is normal in G. We want to show that every subgroup of H is normal in G.

Let K be a subgroup of H. Since H is cyclic, we can write $H = \langle a \rangle$ for some $a \in G$, and $K = \langle a^n \rangle$ for some integer n.

To show that K is normal in G, we need to show that for all $g \in G$ and for all $a^n \in K$, we have $ga^ng^{-1} \in K$.

Since H is normal in G, we know that for all $g \in G$, $gag^{-1} \in H$. Therefore, $gag^{-1} = a^k$ for some integer k.

Now, for any $a^n \in K$:

$$ga^ng^{-1} = (gag^{-1})^n = (a^k)^n = a^{kn} \in \langle a^n \rangle = K$$

Thus, K is normal in G.

✍ Exercise 2.41

If H is a normal subgroup of a group G such that H and G/H are finitely gengerated ,then so is G

Proof

just we can assume $H = \langle a_1 \cdots a_m \rangle$ and $G/H = \langle g_1H \cdots g_kH \rangle$

it is enough to check $G = \langle a_1, \cdots a_m, g_1, \cdots g_k \rangle$

✍ Exercise 2.42

Let H, K, N be nontrivial normal subgroups of a group G and suppose $G = H \times K$. Prove that N is in the center of G or N intersects one of H, K non-trivially. Give examples to show that both possibilities can actually occur when G is nonabelian.

Proof

Assume that N is not contained in the center $Z(G)$ of G, and that $N \cap H = \{e\}$ and $N \cap K = \{e\}$, where e is the identity element of G. We will derive a contradiction.

Since N is normal in G, for any $n \in N$ and $h \in H$, the commutator $[n, h] = nhn^{-1}h^{-1}$ lies in N. Also, since H is normal in G, $[n, h] \in H$. Thus, $[n, h] \in N \cap H = \{e\}$, so $[n, h] = e$, i.e., n commutes with h. Similarly, for any $n \in N$ and $k \in K$, we have $[n, k] = e$, so n commutes with k.

Now, any element $g \in G$ can be written as $g = hk$ with $h \in H$ and $k \in K$. Then

$$ng = n(hk) = (nh)k = (hn)k = h(nk) = h(kn) = (hk)n = gn.$$

Hence, n commutes with every $g \in G$, so $n \in Z(G)$. This implies $N \subseteq Z(G)$, contradicting the assumption that N is not contained in $Z(G)$.

Therefore, if N is not contained in $Z(G)$, then either $N \cap H \neq \{e\}$ or $N \cap K \neq \{e\}$.

We now give examples to show that both possibilities can occur when G is nonabelian.

例题 **2.1**

N is contained in the center of G. Let $H = D_4$ and $K = D_4$, where D_4 is the dihedral group of order 8 (nonabelian). Then $G = D_4 \times D_4$, and the center is $Z(G) = Z(D_4) \times Z(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let $N = \{(e, e), (r^2, r^2)\}$, where r is a rotation in D_4 (so $r^4 = e$). Then N is a normal subgroup of G (since $N \subseteq Z(G)$), and $N \cap (D_4 \times \{e\}) = \{(e, e)\}$, similarly $N \cap (\{e\} \times D_4) = \{(e, e)\}$. Thus, N is contained in the center and intersects H and K trivially.

例题 **2.2**

N intersects one of H, K non-trivially. Take $G = H \times K$ with H and K nonabelian groups (e.g., D_4). Let $N = H$. Then N is a normal subgroup of G, and $N \cap H = H$ is nontrivial. Since H is nonabelian, N is not contained in the center of G.

✍ Exercise 2.43

Proof

✍ Exercise 2.44

Proof

✍ Exercise 2.45

Proof

✍ Exercise 2.46

Proof

✍ Exercise 2.47

Proof

第 3 章 环论习题

✍ **Exercise 3.1**

设R是一个含么环，$a \in R$满足a在R中有不止一个右逆，则可以得到如下一些结论

1、a在R中无左逆

2、$L_a : R \to R, g \mapsto ag$是一个满射，$R_a : R \to R, g \mapsto ga$是一个单射。

3、R是无限环。

4、a在R中有无限个右逆

Proof 否则设d是a的左逆, 则有$d = d \cdot 1 = dab = b = dac = c$, 矛盾

前者是因为$\forall g \in R, L_a(bg) = abg = g$，后者是因为$\forall g, h \in R, ga = ha \Rightarrow g = gab = hab = h.$

若R是一个有限环, 则结论2告诉我们, R_a是双射, 但这是不可能的, 因为结论1说明a无左逆

记$a_n = b + (1 - ba)a^n, n = 0, 1, \ldots$, 易验证，$aa_n = 1, \forall n \in \mathbb{N}$.特别地，若存在$0 \leq i < j \in \mathbb{N}$, 使得$b + (1 - ba)a^i = b + (1 - ba)a^j$
则两边同时右乘b^j整理得，$0 = 1 - ba$, 这与结论1矛盾，故$\{a_n\}$是一个无限集, 从而a有无限个右逆

✍ **Exercise 3.2**

设R为环, $a \in R$, 若$a \neq 0$且$a^2 = a$, 则称a为幂等元.证明：

(1)若环R的所有非零元素都是幂等元, 则R必为交换环;

(2)若R为无零因子环, 且存在幂等元, 则R只有唯一的幂等元, 且R为么环.

Proof 此时$a \neq 0$, 那么$(-a) \neq 0$那么$(-a)^2 = -a \Longrightarrow a = -a$
此时对于$\forall a, b \neq 0$我们有$(a + b) = (a + b)^2 = a + b + ab + ba \Longrightarrow ab = -ba = ba$(这是针对两个非零元素的交换性)
若a, b其中有一个0元素显然可交换

不防设存在幂等元$a\ (a \neq 0)$, $a^2 = a$;
$\forall b \in R$, 此时$a\ (ab - b) = ab - ab = 0 \Longrightarrow ab - b = 0 \Longrightarrow ab = b$同理$(ba - b)\ a \Longrightarrow ba = b$
故a为一个幺元我们记为e
假设还有一个幂等元那么这幂等元同样是幺元此时$e = ee^* = e^*$故只有一个幂等元

✍ **Exercise 3.3** 设环R中存在唯一的左么元, 试证明R为幺环.

Proof 假设存在唯一的左幺元$e_L, \forall a, b$; 有$(ae_L - a + e_L)\ b = ab - ab + b = b$
那么$ae_L - a + e_L = e_L \Longrightarrow ae_L = a$故$a$为幺元

✍ **Exercise 3.4** 设R是无零因子环, e是R的关于乘法的左 (右) 幺元, 证明：e必是R的幺元.

Proof 设有e_L左幺元此时$\forall b\neq 0,\forall a$有$(ae_L-a)\,b=ab-ab=0\Longrightarrow ae_L-a=0\Longrightarrow e_L$为幺元

✍ **Exercise 3.5** 设R为幺环,e为幺元,$u,v\in R$满足$u^kvu^l=u^{k+l-1}$,其中k,l为正整数,且v是唯一的满足上述条件的元素
证明u,v为可逆元,且$v=u^{-1}$.

Proof 由题$u^k\,(vu-e)\,u^{l-1}=0\Longrightarrow u^k\,(v+vu-e)\,u^l=u^kvu^l=u^{k+l-1}\Longrightarrow v+vu-e=v\Longrightarrow v=e$
同理可得另一边

✍ **Exercise 3.6** 设R为幺环,e为幺元,$a\in R$.若元素c满足$ca=e(ac=e)$,则称c为a的一个右逆元 (左逆元).
若c既是a的左逆元,又是a的右逆元,则称c为a的逆元,这时称a可逆.
证明:对任何$a,b\in R,e-ab$可逆当且仅当$e-ba$可逆.

Proof 设$(e-ab)\,c=e\Longrightarrow b\,(e-ab)\,c=b\Longrightarrow bc-babc=b\Longrightarrow (e-ba)\,bc=b$
$\Longrightarrow (e-ba)\,bca=ba\Longrightarrow (e-ba)\,bca=e-(e-ba)\Longrightarrow (e-ba)\,(bca+e)=e$
同理可证另一边
故逆为$bca+e=b\,(e-ab)^{-1}\,a+e$

✍ **Exercise 3.7** 1.设R是交换环,I是R的理想,定义$\sqrt{I}=\{a\in R\mid \exists n\in\mathbb{N},a^n\in I\}$.试证明$\sqrt{I}$也是$R$的理想,称为理想$I$的根基.
特别地,R中所有幂零元组成的集合 (即理想$\{0\}$的根基) 构成R的理想,称为R的幂零根基,记为 Rad$R$.
2.证明对任何R的理想$I,\sqrt{\sqrt{I}}=\sqrt{I}$.
3.设R为交换环,Rad$R$为R的幂零根基.证明:商环$R/\mathrm{Rad}R$的幂零根基为零,从而$R/\mathrm{Rad}R$中没有非零的幂零元.

Proof 自己练习

✍ **Exercise 3.8** 设R为环,R中一个元素a称为右拟正则元,如果存在$b\in R$使得$a+b-ab=0$.
试证明:如果环R中有一个元素不是右拟正则元,而其他元素全是右拟正则元,则R是除环.

Proof 1.不妨假设e元素是唯一的非右拟正则元.即$\forall a$都有$e+a-ea\neq 0$
断言:$e+a-ea=e$
若不然:$e+a-ea\neq e$.那么$e+a-ea$为右拟正则元
那么$\exists b;\ s.t.\ \ (e+a-ea)+b-(e+a-ea)\,b=0\Longrightarrow e+(a+b-ab)-e\,(a+b-ab)=0$
$\Longrightarrow e$为右拟正则元.矛盾!
故$e+a-ea=e\Longrightarrow a=ea\Longrightarrow e$为左幺元

2.若e^*也是左幺元,断言$e^*=e$若不然$e^*\neq e$;
那么e^*为右拟正则元$\Longrightarrow\exists b\ \ s.t.\ e^*+b-e^*b=0\Longrightarrow e^*=0$与$e^*$为左幺元矛盾
$\Longrightarrow e$为R中唯一的左幺元$\Longrightarrow e$为R中幺元

3.$\forall a\neq 0;\ a\in R$;来证明a存在其对应的逆元

此时$a+e\neq e$从而$a+e$为右拟正则元$\Longrightarrow \exists b\ \ s.t.\ \ (a+e)+b-(a+e)b=0\Longrightarrow a(b-e)=e$

我们来证$(b-e)a=e$

引理：若$ac=0\ \ a\neq 0\Longrightarrow c=0$

反之若$c\neq 0$同理$c+e\neq e\Longrightarrow c(d-e)=e\Longrightarrow ac(d-e)=ae\Longrightarrow 0=a$矛盾

则对于$a(b-e)a=ea=ae=a\Longrightarrow a[(b-e)a-e]=0\Longrightarrow (b-e)a-e=0\Longrightarrow (b-e)a=e$

✍ **Exercise 3.9** 设$\mathbb{Q}(\mathrm{i})=\{a+bi\mid a,b\in\mathbb{Q}\}$

(1)$\mathbb{Q}$是$\mathbb{Q}(\mathrm{i})$ 的唯一真子城; (2)$\mathbb{Q}(i)$有且仅有两个自同构映射.

Proof (1)若任意一个F是一个真子域且$F\neq\mathbb{Q}$那么其就包含一个元素a那么$aa^{-1}=1\in F$且$a-a=0\in F$

那么由于$\mathbb{Q}$是最小的数域故F包含了$\mathbb{Q}$,其次,F又是一个真子域那么就有F一定包含一个$a+bi$此时$b\neq 0$

那么又$a\in\mathbb{Q}$此时$bi\in F$且$b\in F$那么$b^{-1}\in F$那么$i\in F$

那么F就扩充到了$Q(i)$不再是真子域

(2)不难得到若有f为$\mathbb{Q}(i)$上的同构映射那么$f(0)=0,f(1)=1$

$\Longrightarrow f(n)=n(n\in Z)$

$\Longrightarrow f(1)=f\left(\frac{1}{n}+\cdots+\frac{1}{n}\right)=nf\left(\frac{1}{n}\right)\Longrightarrow f\left(\frac{1}{n}\right)=\frac{1}{n}$

$\Longrightarrow f(a)=a(a\in\mathbb{Q})$

其次$-1=f(-1)=f\left(i^2\right)=f(i)f(i)\Longrightarrow f(i)=i$或$-i$

若$f(i)=i$那么$f(a+bi)=f(a)+f(bi)=a+f(b)f(i)=a+bi$

若$f(i)=-i$那么$f(a+bi)=f(a)+f(bi)=a+f(b)f(i)=a-bi$

所以就只有两个自同构映射为id或共轭映射

✍ **Exercise 3.10** 设R为一个除环,R^*为其非零元组成的乘法群,证明：R作为加法群与乘法群R^*不同构.

Proof 假设若有同构,则R中零元将映至R^*中的e，不妨设将R中e打到a

那么$f(0+e)=f(0)+f(e)\Longleftrightarrow a=f(e)=e+a\Longrightarrow e=0$矛盾

✍ **Exercise 3.11** 试证明实数域的自同构只有恒等同构.

Proof 设有一个自同构f;那么$f(0)=0;f(1)=1\Longrightarrow f(n)=n$($n$为整数)

进一步$f(n)=f\left(\frac{1}{n}+\cdots+\frac{1}{n}\right)=nf\left(\frac{1}{n}\right)\Longrightarrow f\left(\frac{1}{n}\right)=\frac{1}{n}$($n$为整数)$\Longrightarrow f\left(\frac{p}{q}\right)=\frac{p}{q}\left(\frac{p}{q}\right.$为有理数$\left.\right)$

若$x>0,x\in\mathbb{R}$.则$f(x)=f\left(\sqrt{x}\cdot\sqrt{x}\right)=\left(f\left(\sqrt{x}\right)\right)^2$因为同构所以$f\left(\sqrt{x}\right)$不会等于0故严格大于0

说明$x>0\Longrightarrow f(x)=\left(f\left(\sqrt{x}\right)\right)^2>0$有保序性!!!具体的若$a>b$那么$a-b>0\Longrightarrow f(a-b)>0\Longrightarrow f(a)>f(b)$

此时若不是恒等id,那么存在x使得$f(x)\neq x$.不妨假设$x<f(x)$

那么存在有理数$q\in(x,f(x))$此时$f(q)=q$

那么$f(x)>q=f(q)$另一方面因为$x<q$所以$f(x)<f(q)$矛盾

✍ **Exercise 3.12** 设R为无零因子环, 含有p个元素, p为素数.证明 : R为域, 且与$\mathbb{Z}_p$同构.

Proof 有限半群满足消去律故构成群, 且对于R看成加法群p为素数故为素数阶循环群记为$\{0, a, 2a \cdots (p-1)a\}$
所以对于乘法也是可交换的故为域.那么R作为素数阶循环群必同构于$\mathbb{Z}_p$同构.

✍ **Exercise 3.13** 设φ为么环R_1到么环R_2的满同态
证明 : 若u为R_1的单位, 则$\varphi(u)$是R_2的单位, 试问$u \mapsto \varphi(u)$是R_1的单位群到R_2的单位群的满同态吗?

Proof 前半问是肯定的.首先因为为满同态故$\varphi(1_{R_1}) = 1_{R_2}$
若u为R_1的单位, 那么存在x使得$xu = ux = 1_{R_1}$那么$\varphi(xu) = \varphi(ux) = \varphi(x)\varphi(u) = \varphi(u)\varphi(x) = 1_{R_2}$
后者是否定的.若为么环$(\mathbb{Z}, +, \cdot) \to$ 么环$\mathbb{Z}_6$该满同态
前者单位群为1.后者单位群为$\{1, 5\}$故不是满同态

✍ **Exercise 3.14** R为除环, 证明R到任何环的非零同态一定是单同态.

Proof 因为R是除环所以为单环, 那么该非零同态φ的$Ker\varphi$必定是R的理想
此时$Ker\varphi = 0$或R.若$Ker\varphi$为0则为单同态, 且$Ker\varphi$不能为R(因为若$Ker\varphi = R$则同态为零同态)

✍ **Exercise 3.15** 设m_1, m_2为不同的正整数, 证明$m_1\mathbb{Z}$与$m_2\mathbb{Z}$作为加法群同构, 但作为环不同构.

Proof 作为加法群同构我们可以选择映射$\varphi : m_1\mathbb{Z} \to m_2\mathbb{Z} \quad km_1 \mapsto km_2\ (k \in \mathbb{Z})$
若作为环是同构的那么$m_1\mathbb{Z}$中的0映至$m_2\mathbb{Z}$中的0断言此时$f(m_1) \to m_2$
这是因为若$f(m_1) \neq m_2$不妨假设映至km_2那么其余元素im_1的像都被唯一确定了, 也不会为m_2那么不是同构了
此时$m_1 \to m_2 \quad 2m_1 \to 2m_2$此时, $f(2m_1 \cdot m_1) = 2m_1m_2$但是由同态有$f(2m_1 \cdot m_1) = 2m_2 \cdot m_2$
但$m_1 \neq m_2$矛盾

✍ **Exercise 3.16** 设R为交换环, 证明对任何R的理想I, J都有$\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$

Proof 自己练习

✍ **Exercise 3.17 挖补定理** 设R', S为两个环, $R' \cap S = \varnothing$.设S含有一个子环R使得R与R'同构.
证明 : 存在一个环S', 它与S同构, 且R'是S'的一个子环.

Proof 这个定理还是比较直观的, 说的是可以把S的子环R用 (同构意义下) 相同的R'代替[1]
得到的环S'与S是相同的 (同构意义下; 挖掉R补上R'没有区别, 只需补上部分等效替代就行)
换句话说, 设$\phi : R \to R'$为同构映射, 令$S' = R' \cup (S \backslash R)$取映射$\phi' : S \to S', \phi'(x) = \begin{cases} x & x \in S \backslash R \\ \phi(x) & x \in R \end{cases}$

并将S'中的加法定义为$\oplus : S' \times S' \to S', x \oplus y = \phi'(x' + y')$其中$+$为$S$中加法

而$x' = \begin{cases} x & x \in S \backslash R \\ \phi^{-1}x & x \in \phi(R) \end{cases}, y' = \begin{cases} y & y \in S \backslash R \\ \phi^{-1}y & y \in \phi(R) \end{cases}$

同理用S中乘法$\times$定义S'中乘法$\otimes$也即新环S'中补进去的R'中元素,完全以R中同构像的角色、以S中的方式参与运算;

因此$R' \cap S = \emptyset$不是必要的，只需要$R \supset R' \cap S$即可，甚至不要求同构映射ϕ满足和原来R中元素没有区别)

则$(S, +, \times)$与$(S', \oplus, \otimes)$同构且以ϕ'为同构映射

不过话说回来,如果S的子环R与R'同构,将R与R'同等看待,已经有了包含R的环S为什么考虑包含R'且与S同构的环S'呢

可能意义就在于，把R'同构于S的子环R(也即存在嵌入)和R'是某同构于S的环S'的子环(也即存在扩张)等价起来

如果觉得二者没区别，那这个定理也就没什么意义

比如认为“任意环都可以嵌入到含么环”或者“任意环都是含么环的子环两个结论同样令人满意

Exercise 3.18 中国剩余定理

设 R 是含么环，$I_1, I_2, ..., I_n$为环R的理想.当$i \neq j$时,$I_i + I_j = R$,则有环同构$R/(I_1 \cap ... \cap I_n) \cong \prod_{i=1}^{n} (R/I_i)$

推论：设R为么环,I_1, I_2为R的理想,且$R = I_1 + I_2$,试证明对任何$a_1, a_2 \in R$,必存在$a \in R$使得$a - a_1 \in I_1, a - a_2 \in I_2$.

此时下述证明的f是满同态故对$\forall x, y \in R$对于$(x + I_1, y + I_2)$存在a使得$f(a) = (a + I_1, a + I_2) = (x + I_1, y + I_2)$

即$a - x \in I_1, a - y \in I_2$

Proof 构造映射$f : R \to \prod_{i=1}^{n} (R/I_i), r \mapsto (r \pmod{I_1}, ..., r \pmod{I_n})$其中$r \pmod{I_1}$代表的意思是以$r$为代表的陪集，即$r + I_1$

现在证明f是环的同态：

$f(r_1 + r_2) = ((r_1 + r_2) \pmod{I_1}, ..., (r_1 + r_2) \pmod{I_n}) = (r_1 \pmod{I_1}, ..., r_1 \pmod{I_n}) + (r_2 \pmod{I_1}, ..., r_2 \pmod{I_n})$

$f(r_1 r_2) = ((r_1 r_2) \pmod{I_1}, ..., (r_1 r_2) \pmod{I_n}) = (r_1 \pmod{I_1}, ..., r_1 \pmod{I_n}) \bullet (r_2 \pmod{I_1}, ..., r_2 \pmod{I_n})$

再证明满射：由于$I_i + I_j = R$,易知R可写成$R = I_1 + I_2 I_3 ... I_n$

则存在$a \in I_1, b \in I_2$,使$a + b = 1$,令$r_1 = b$,则$f(r_1) = (1 \pmod{I_1}, 0 \pmod{I_2}, ..., 0 \pmod{I_n})$

上式因为$a + b = 1 = I_1 + I_2 = I_1 + I_3 \cdots$此外$r_1 - 1 = -a \in I_1$同理可得到$r_2 \cdots r_n$

对$\prod_{i=1}^{n} (R/I_i)$中的任意元素$a = (a_1 \pmod{I_1}, ...a_n \pmod{I_n})$

令$r = a_1 r_1 + ... + a_n r_n \in R$,则$f(r) = a$,证明了$f$是满同态.易知 Ker$f = I_1 \cap ... \cap I_n$,所以由环论的第一同构定理，$R/(I_1 \cap ... \cap I_n) \cong \prod_{i=1}^{n} (R/I_i)$。

Exercise 3.19

Proof

Exercise 3.20

Proof

Exercise 3.21

Proof

Exercise 3.22

Proof