近世代数部分习题参考答案

第 11 章 半群和幺半群

11.3.5

证明：设$(S,\circ)$为有限半群，且$|S|=n$。设$b\in S$，则可得：$b^1,b^2,\cdots,b^n,b^{n+1}\in S$

由S的有限性知，$\exists i,j\in[1,n+1]$使得$b^j=b^i$，不妨设$j>i$，即$j=i+k$，$k>0$。

从而有：$b^i\circ b^k=b^i$,则两边同时不断左乘b使得$b^p\circ b^k=b^p$，且满足$p=q\cdot k$，

从而$b^p=b^p\circ b^k=(b^p\circ b^k)\circ b^k=b^p\circ b^{2k}=\cdots=b^p\circ b^{qk}$，即$b^p\circ b^p=b^p$，令

$a=b^p$即可。

11.3.8

证明：

1）结合律：由集合论知识知集合的对称差运算"Δ"满足结合律，故$(2^S,\Delta)$为半群；

2）单位元：对$\forall A\in 2^S$有$\phi\Delta A=A\Delta\phi=A$；

3）逆元：对$\forall A\in 2^S$有$A\Delta A=A\Delta A=\phi$，即为自身。

故$(2^S,\Delta)$为群。

11.4.1

证明：记$H=\{x|\exists a_1,a_2,\cdots,a_n\in A使x=a_1a_2\cdots a_n,n\geq 1\}$，下证$G(A)=H$，根据$G(A)$的定义即证$H$为$A$的生成子半群。

先证H为包含A的子半群。

① 显然$A\subseteq H$（令$n=1$即可知），

② "$\circ$"在H上的运算封闭：对$\forall x,y\in H$，有$x=a_1a_2\cdots a_n$，$y=b_1b_2\cdots b_m$，其中$a_i,b_j\in A$。从而$x\circ y\in H$。

故H为包含A的子半群。

③ 下证H即为A的生成子半群。

设P为包含A的任意一个子半群，下证$H\subseteq P$。

对 $\forall x \in H$ ， $\exists a_1, a_2, \cdots, a_i \in A$ 使得 $x = a_1 a_2 \cdots a_i$ ， 又 $A \subseteq P$ ， 所以 $a_1, a_2, \cdots, a_i \in P$，则由 P 为子半群知 $a_1 a_2 \cdots a_i \in P$，即 $x \in P$，所以 $H \subseteq P$。

综上 $G(A) = H$。

11.5.1

证明：记 $S = \varphi^{-1}(e_2)$，则 $S = \{x | \varphi(x) = e_2\}$，显然有 $S \subseteq M_1$

①S 非空：由 $\varphi(e_1) = e_2$ 知 $e_1 \in S$。

②封闭性：对 $\forall x, y \in S$ 有： $\varphi(x) = e_2$， $\varphi(y) = e_2$，

则 $\varphi(x \circ y) = \varphi(x) * \varphi(y) = e_2 * e_2 = e_2$，所以 $x \circ y \in S$

故 S 是 M_1 的一个子幺半群。

若 S 是 M_1 的理想，则有 $SM_1 \subseteq S$， $M_1 S \subseteq S$

对 $\forall x \in S$， $\forall y \in M_1$， $\varphi(x \circ y) = \varphi(x) * \varphi(y) = e_2 * \varphi(y) = \varphi(y)$

同理 $\varphi(y \circ x) = \varphi(y) * \varphi(x) = \varphi(y) * e_2 = \varphi(y)$

所以如果 $\varphi(y) = e_2$，则 $x \circ y (y \circ x) \in S$，此时 S 是 M_1 的理想，否则不是。

11.5．2

证明：设 $\varphi : (S_1, *) \to (S_2, \bullet)$ 同态，$\psi : (S_2, \bullet) \to (S_3, \Delta)$ 同态，记 $f = \psi \circ \varphi$，由映射的符合知 f 为 $S_1 \to S_3$ 的映射。又对 $\forall x, y \in S_1$：

$$f(x * y) = \psi \circ \varphi(x * y) = \psi(\varphi(x * y)) = \psi(\varphi(x) \bullet \varphi(y)) = \psi(\varphi(x)) \Delta \psi(\varphi(y))$$

$$= \psi \circ \varphi(x) \Delta \psi \circ \varphi(y) = f(x) \circ f(y)$$

所以 $f = \psi \circ \varphi$ 为 $S_1 \to S_3$ 的同态，即两个同态的合成还是同态。

第 12 章 群

12.2.2

证明：由 $\forall a \in G$， $a^2 = e \Rightarrow a = a^{-1}$。

从而对 $\forall a,b \in G$， $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$

12.2.3

证明：设 $G = \{e,a,b,c\}$， $(G,\circ)$ 为群。其乘法表为：

•	e	a	b	c
e	e	a	b	c
a	a	aa	ab	ac
b	b	ba	bb	bc
c	c	ca	cb	cc

验证交换性只须验证乘法表中的矩阵的对称性即可，即只须验证：

1）ab 与 ba：显然 $ab \neq a,b$，故 $ab = e,c$

若 $ab = e$，即 a 与 b 互逆，则必有 $ba = e$，从而 $ab=ba$；
若 $ab = c$，则 $ba = c$，否则若 $ba = e$，则必有 $ab = e$，从而 $c = e$ 矛盾。
综上 $ab=ba$。

同理可得：$ac=ca$，$bc=cb$。

12.2.4

证明：设 $(G,\circ)$ 为非交换群，且 $|G|>2$。只须找到元素 $a \in G$，且 $a^{-1} \neq a$ 即可。

即只须在 G 中找到一个元素，其阶大于 2 即可。若 G 中不存在这样的元素，即对 $\forall a \in G$ 均有 $a^2 = e$，则由 2 题知 G 为交换群，矛盾。故 $\exists a \in G$，其阶大于 2，即 $a^{-1} \neq a$，从而令 $b = a^{-1}$，显然有 $b \neq a$，但 $ab = ba$。

12.2.5

证明：设 $(G,\circ)$ 为有限群，$|G|= n$，对 $\forall a \in G$，若 a 的阶为 r 且 $r > 2$，即 $a^r = e$，则 a^{-1} 的阶也为 r，即 $(a^{-1})^r = e$，且 $a^{-1} \neq a$，从而阶大于 2 的元素成对出现，故阶大于 2 的元素个数必为偶数。

12.2.9

证明：考查元素序列：$e, a_1, a_1a_2, a_1a_2a_3, \cdots, a_1a_2\cdots a_n \in G$，而 $|G|= n$

故上述 $n+1$ 个元素中至少有两个元素相同，若其中一个为 e，则有：$a_1a_2\cdots a_i = e$

此时令 $p = 1, q = i$ 即可；若两个元素均不为 e，则存在 $i, j \in [1,n]$，不妨设 $i < j$，使得 $a_1a_2\cdots a_i = a_1a_2\cdots a_j = a_1a_2\cdots a_ia_{i+1}\cdots a_j$，由消去律得：$a_{i+1}\cdots a_j = e$，此时

令 $p=i+1, q=j$ 即可。

//

补充思考题解答：

1）设群 G 中元素 a 的阶为 n，且有正整数 m 使得 $a^m=e$，则是否一定有 $m=n$？

解：令 $m=kn+r$，$0\le r<n$ 则 $a^m=a^{kn+r}=e\Rightarrow a^r=e\Rightarrow r=0$，所以 $n\mid m$。

2）设群 G 中元素 a 的阶为 n，则 a^{-1} 的阶是否也一定为 n？

解：有 $a^n=e\Rightarrow (a^{-1})^n=e$，故可设 a^{-1} 的阶为 r，即有 $(a^{-1})^r=e$，则由上题知 $r\mid n$，又 $(a^{-1})^r=e\Rightarrow a^r=e$，由 $a^n=e$，得 $n\mid r$，故 $r=n$。

3）设群 G 不一定为交换群，则是否一定有 ab 的阶和 ba 的阶相同?（$a,b\in G$）

解：不妨设它们阶均有限，即有 $(ab)^m=e$，$(ba)^n=e$。由 $ba=a^{-1}(ab)a$，知 $(ba)^n=a^{-1}(ab)^n a=e\Rightarrow (ab)^n=e$，从而 $m\mid n$，同理可得 $n\mid m$，故 $n=m$。

//

12.3.5

证明：记 $S=\varphi^{-1}(e_2)$，则 $S=\{x\mid \varphi(x)=e_2, x\in G_1\}$，显然 $S\subseteq G_1$

1）S 非空：对 $\forall y\in G_2$，由 φ 为满射，则 $\exists x\in G_1$，使得 $y=\varphi(x)$，从而 $\varphi(e_1)*y=\varphi(e_1)*\varphi(x)=\varphi(e_1\circ x)=\varphi(x)=y$，同理有 $y*\varphi(e_1)=\varphi(x)=y$，所以：$\varphi(e_1)*y=y*\varphi(e_1)=y$，则 $\varphi(e_1)=e_2$，所以 $e_1\in S$。

2）封闭性：对 $\forall x,t\in S$，有 $\varphi(x)=e_2$，$\varphi(t)=e_2$，则 $\varphi(x\circ t)=\varphi(x)*\varphi(t)=e_2$，所以 $x\circ t\in S$。

3）结合律：显然。

4）单位元：$e_1\in S$。

5）逆元：对 $\forall x\in S$，有 $\varphi(x)=e_2$，则：$e_2=\varphi(e_1)=\varphi(x\circ x^{-1})=\varphi(x)*\varphi(x^{-1})$

$=e_2*\varphi(x^{-1})=\varphi(x^{-1})$，即 $\varphi(x^{-1})=e_2$，所以 $x^{-1}\in S$。

12.4.1

证明：显然对 $\forall f\in G$，f 为双射。

1）封闭性：对 $\forall f,g\in G$，设 $f(x)=ax+b$，$g(x)=cx+d$，$a\neq 0,c\neq 0$，

则 $f\circ g(x)=f(g(x))=f(cx+d)=a(cx+d)+b=(ac)x+ad+b$，所以 $f\circ g\in G$

2）结合律：映射的复合满足结合律。

3）单位元：$I_R(x)=x$

4）逆元：显然对 $\forall f\in G$，由 f 为双射，故 f 可逆，且 $f^{-1}(x)=\frac{1}{a}x-\frac{b}{a}$，则 $f^{-1}\in G$。

12.5.3

证明：由 $a^r\in G$，则 $(a^r)\subseteq G$。设 a^r 的阶为 k，即 $(a^r)^k=e$。

因为 $(a^r)^n=(a^n)^r=e^r=e$，所以 $k\mid n$。又由 $(a^r)^k=e\Rightarrow a^{rk}=e$，而 $a^n=e$，

所以 $n\mid rk$，由已知 $(n,r)=1$，则有：$n\mid k$，所以 $k=n$，即 a^r 的阶为 n，从而 $(a^r)=G$。

另证：由 $(n,r)=1\Rightarrow\exists k_1,k_2\in Z$，$k_1\cdot n+k_2\cdot r=1$，则有：

$a^1=a^{k_1\cdot n+k_2\cdot r}=a^{k_1\cdot n}a^{k_2\cdot r}=ea^{k_2\cdot r}=(a^r)^{k_2}$，即 $a=(a^r)^{k_2}$，即 G 的生成元 a 可由 a^r 生成，故有：$(a^r)=G$。

12.5.5

证明：设 a^r 的阶为 k，则 $(a^r)^k=e$，即 $a^{rk}=e$。又 $a^n=e$，所以 $n|rk$，又 $(r,n)=d$，

则有：$\frac{n}{d}|\frac{r}{d}k$，而 $(\frac{n}{d},\frac{r}{d})=1$，所以 $\frac{n}{d}|k$。

又由 $(a^r)^{\frac{n}{d}}=a^{\frac{nr}{d}}=(a^n)^{\frac{r}{d}}=e^{\frac{r}{d}}=e$ 得：$k|\frac{n}{d}$，从而 $k=\frac{n}{d}$

12.6.1

证明：设 $(G,\circ)$ 为六阶群。则对 $\forall x\in G(x\neq e)$，其阶只能为 2，3，6。

1）若 $\exists a\in G$，且 a 的阶为 6 ，即 $a^6=e$，则 $G=(a)$，则由循环群的子群知存在三阶子群为：$S=\{e,a^2,a^4\}$

2）若 $\exists a\in G$，且 a 的阶为 3 ，即 $a^3=e$，此时显然有三阶子群为：$S=\{e,a^1,a^2\}$

3）若不存在 $a\in G$，使得 a 的阶为 3 或 6，则对 $\forall a\in G$ 有 $a^2=e$，从而此时群 $(G,\circ)$ 为交换群。令 $A=\{a,b\}$，其中 $a,b\in G$ 且均不为单位元。则 $(A)=\{e,a,b,ab\}$，$|(A)|=4\nmid 6$ 矛盾。

12.6.2

证明：设$(G,\circ)$为群，$|G|=p^m$。取$a\in G(a\neq e)$，设其阶为r，则$r\mid p^m$，

由p为素数得：$r=p^k$，$k\geq 1$。

1）若$k=1$，则群G的一个p阶子群为$H=(a)$；

2）如$k>1$，取$b=a^{p^{k-1}}\in G$，设b的阶为q，即$b^q=e$。由$b^p=(a^{p^{k-1}})^p=a^{p^k}=e$

$\Rightarrow$

$q\mid p$，又$b^q=(a^{p^{k-1}})^q=a^{qp^{k-1}}=e$，则有$r\mid qp^{k-1}$，即：$p^k\mid qp^{k-1}$，从而$p\mid q$，所以$q=p$。此时群$G$的一个$p$阶子群为$H=(b)$。

12.7.2

证明：设$H=A\cap B$，则由定理知H仍为群G的子群，则由拉格朗日定理得：

$|B|=|H|\cdot[B:H]$，记$j=[B:H]=\dfrac{|B|}{|H|}$，则$B=Hb_1\cup Hb_2\cup\cdots\cup Hb_j$，

$b_i\in B(i=1,.\cdots,j)$其中$Hb_i(i=1,\cdots,j)$为互不相同的右陪集。则$AB=AHb_1\cup AHb_2\cup\cdots\cup AHb_j$，又$AH=A$，所以$AB=Ab_1\cup Ab_2\cup\cdots\cup Ab_j$，

又$Ab_i\cap Ab_l=\phi$，否则，若$Ab_i\cap Ab_l\neq\phi$，则由陪集的性质得：$Ab_i=Ab_l$，从而$b_ib_l^{-1}\in A$，又$b_ib_l^{-1}\in B$，所以$b_ib_l^{-1}\in A\cap B$，即$b_ib_l^{-1}\in H$，所以$Hb_i=Hb_l$，矛盾。因此根据容斥原理有：$|AB|=|Ab_1|+|Ab_2|+\cdots+|Ab_j|=j\cdot|A|$

即$|AB|=\dfrac{|B|}{|H|}\cdot|A|=\dfrac{|A||B|}{|A\cap B|}$

12.7.3

证明：由前面的习题结论知六阶群中一定有三阶子群，假设不唯一，设A,B为六阶群G两个不同的三阶子群。不妨设$A=\{e,a,b\}$，$B=\{e,c,d\}$，则$A\cap B=\{e\}$。

从而$|AB|=\dfrac{|A||B|}{|A\cap B|}=9>6$矛盾。

12.7.1

证明：假设不成立，则$\exists a\in G$，使得$a^{-1}Ha\cap H=\{e\}$，记$P=a^{-1}Ha$，由H为G

的子群易知 P 也为 G 的子群，且 $|P|=|H|=n$（由映射 $\varphi(h)=a^{-1}ha$ 为单射），则由 1 题的结论：$|PH|=\frac{|P||H|}{|P\bigcap H|}=\frac{n\cdot n}{1}=n^2$，又 $PH\subseteq G$，$|G|=n^2$，所以 $PH=G$，则由书上例题 12.7.1 结论知 $P\bigcap H=H\neq\{e\}$，矛盾。

12.7.4

证明：设 H 为群 G 的子群，且有 $[G:H]=2$，则其左陪集构成的划分为：$H,aH(a\notin H)$，其右陪集构成的划分为：$H,Ha(a\notin H)$，从而 $aH=G\setminus H$ $Ha=G\setminus H$，所以 $aH=Ha$，故 H 为群 G 的正规子群。

12.7.5

证明：设 H_1,H_2 为群 G 的两个正规子群，记 $H=H_1\bigcap H_2$。则对 $\forall a\in G,h\in H$，由 H_1,H_2 为群 G 的两个正规子群得：$aha^{-1}\in H_1$，$aha^{-1}\in H_2$，所以 $aha^{-1}\in H_1\bigcap H_2$，即 $aha^{-1}\in H$，从而 $aHa^{-1}\subseteq H$，故 H 是 G 的正规子群。

12.7.6

证明：对 $\forall a,b\in NH$，则 $\exists n_1,n_2,h_1,h_2\in NH$，使得 $a=n_1h_1,b=n_2h_2$，则 $ab^{-1}=n_1h_1h_2^{-1}n_2^{-1}$。又由 N 是 G 的正规子群，则对 $\forall x\in G$，$xN=Nx$。故 $\exists n_3\in N$ 使得 $h_2^{-1}n_2^{-1}=n_3h_2^{-1}$，则 $ab^{-1}=n_1h_1n_3h_2^{-1}$，同理 $\exists n_4\in N$，使得 $h_1n_3=n_4h_1$，从而 $ab^{-1}=n_1n_4h_1h_2^{-1}=(n_1n_4)(h_1h_2^{-1})\in NH$，则由子群的判定定理知 NH 是 G 的子群。

12.7.8

证明：设 G 为群且 $|G|=2n$，则偶数阶群 G 中一定存在一个阶为 2 元素，即 $\exists a\in G$，$a^2=e$，从而 $H=(a)=\{e,a\}$。由 G 为交换群，则对 $\forall x\in G$，$xH=Hx=\{x,ax\}=\{x,xa\}$，故 H 为群 G 的一个 2 阶正规子群，根据拉格朗日定理以及正规子群和商群的关系知 G 必有一个 n 阶商群。

12.7.9

证明：

必要性 $\Rightarrow$：对 $\forall a,b\in G$，由 H 为 G 的正规子群可得：$aH\cdot bH=a(Hb)H=a(bH)H=abHH=abH$，仍为 H 的左陪集。

充分性$\Leftarrow$：由已知可得：对$\forall a \in G$，$aH \cdot a^{-1}H = cH$，因为$e \in aH \cdot a^{-1}H$，从而$e \in cH$，；又$e \in H$，即$e \in cH \cap H$，则由左陪集的性质得：$cH = H$，所以$aH \cdot a^{-1}H = H$，则对$\forall h \in H$，$\exists h_1, h_2 \in H$，使得$aha^{-1}h_1 = h_2 \Rightarrow aha^{-1} = h_2 h_1^{-1} \in H$即$aHa^{-1} \subseteq H$，故$H$为$G$的正规子群。

12.7.12

证明：设$P \subseteq N \subseteq G$，其中$N$是群$G$的子群，$P$是$G$的换位子群。对$\forall a \in G, h \in N$，$aha^{-1} = (aha^{-1}h^{-1})h$，而$aha^{-1}h^{-1} \in P$，所以$aha^{-1}h^{-1} \in N$，从而$(aha^{-1}h^{-1})h \in N$，即$aha^{-1} \in N$，即$aNa^{-1} \subseteq N$，所以$N$是群$G$的正规子群。

12.8.1

证明：必要性$\Rightarrow$：设$\varphi : G \to \overline{G}$的满同态，根据群同态基本定理有：$G/Ker\,\varphi \cong \overline{G}$，则$|G/Ker\,\varphi| = |\overline{G}| = n$，又根据拉格朗日定理得：$|G/Ker\,\varphi| = \frac{|G|}{|Ker\,\varphi|} = \frac{m}{|Ker\,\varphi|}$，即$m = n \cdot |Ker\,\varphi|$，所以$n \mid m$。

充分性$\Leftarrow$：设$G = (a), a^m = e$，$\overline{G} = (b), b^n = \bar{e}$，$\varphi : G \to \overline{G}$，且对$\forall a^k \in G$，$\varphi(a^k) = b^k$

1）φ为映射：若$a^k = a^l$，则$a^{k-l} = e$，又$a^m = e$，所以$m \mid (k-l)$，又$n \mid m$，所以$n \mid (k-l)$，而$b^n = \bar{e}$，所以$b^{k-l} = \bar{e}$，则$b^k = b^l$，即$\varphi(a^k) = \varphi(a^l)$。

2）同态方程：对$\forall a^k, a^l \in G$，$\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = b^{k+l} = b^k b^l = \varphi(a^k)\varphi(a^l)$。

综上$G \sim \overline{G}$。

12.8.2

证明：设$G = (a)$，由H为循环群的子群，故H为正规子群。从而H为商群G/H的单位元，且对$\forall bH \in G/H (b \in G)$，$bH = a^k H = (aH)^k$，因此$G/H = (aH)$，即$aH$为商群$G/H$的生成元，故为循环群。

第 13 章 环和域

13.1.1

证明：

1）$(Z(\sqrt{2}),+)$ 为 Abel 群：

①封闭性：对 $\forall m_1+n_1\sqrt{2},m_2+n_2\sqrt{2}\in Z(\sqrt{2})$，有：

$$(m_1+n_1\sqrt{2})+(m_2+n_2\sqrt{2})=(m_1+m_2)+(n_1+n_2)\sqrt{2}\in Z(\sqrt{2})$$

②结合律：显然。

③单位元：$e=0$。

④逆元：对 $\forall m+n\sqrt{2},\in Z(\sqrt{2})$，$(m+n\sqrt{2})+((-m)+(-n\sqrt{2}))=0\in Z(\sqrt{2})$

⑤交换律：显然。

2）$(Z(\sqrt{2}),*)$ 为半群：

①封闭性：对 $\forall m_1+n_1\sqrt{2},m_2+n_2\sqrt{2}\in Z(\sqrt{2})$，有：

$$(m_1+n_1\sqrt{2})*(m_2+n_2\sqrt{2})=(m_1m_2+2n_1n_2)+(m_2n_1+m_1n_2)\sqrt{2}\in Z(\sqrt{2})$$

②结合律：显然。

3）分配律：显然。

13.1.2：证法同上。

13.1.3

证明：$Q(\sqrt[3]{2})$ 对乘法不封闭。

假设 $Q(\sqrt[3]{2})$ 对乘法封闭，则由 $\sqrt[3]{2}\in Q(\sqrt[3]{2})\Rightarrow(\sqrt[3]{2})^2\in Q(\sqrt[3]{2})$，设 $(\sqrt[3]{2})^2=a+b\sqrt[3]{2}$，

$$\Rightarrow 2=a\sqrt[3]{2}+b(\sqrt[3]{2})^2\Rightarrow 2=a\sqrt[3]{2}+b(a+b\sqrt[3]{2})\Rightarrow 2=ab+(a+b^2)\sqrt[3]{2}$$

$\Rightarrow\sqrt[3]{2}=\dfrac{2-ab}{a+b^2}$，而 $\dfrac{2-ab}{a+b^2}$ 为有理数，$\sqrt[3]{2}$ 为无理数，故矛盾。

注：证 $\sqrt[3]{2}$ 为无理数

假设 $\sqrt[3]{2}$ 为有理数，则有：$\sqrt[3]{2}=\dfrac{q}{p}$，$(p,q)=1$。

从而 $q^3=2p^3\Rightarrow p^3\mid q^3\Rightarrow(p^3,q^3)=p^3$，又由 $(p,q)=1$ 可得：

$$1=(p,q(p,q))=((p,pq),q^2)=(p,q^2)=\cdots=(p^3,q^3)$$，从而 $p^3=1\Rightarrow p=1$，所以

$\sqrt[3]{2}=q$，即$\sqrt[3]{2}$为整数，而$1<\sqrt[3]{2}<2$，矛盾。

13.1.9

证明：设$(S,+,\circ)$为环，记其唯一的左单位元为e_1，即对$\forall a\in S$，$e_1a=a$，下证$ae_1=a$，只须证：$ae_1-a=0$。因为$(e_1+ae_1-a)a=e_1a+(ae_1)a-aa=a$，所以$e_1+ae_1-a$也为一左单位元，故$e_1+ae_1-a=e_1$，所以$ae_1-a=0$，即$ae_1=a$。

13.1.10

证明：由$(a-b^{-1})b=ab-1\Rightarrow a-b^{-1}=(ab-1)b^{-1}$，则$(a-b^{-1})^{-1}=b(ab-1)^{-1}$。

又$(a-b^{-1})((a-b^{-1})^{-1}-a^{-1})=1-(1-b^{-1}a^{-1})=b^{-1}a^{-1}$，则：

$((a-b^{-1})^{-1}-a^{-1})=(a-b^{-1})^{-1}b^{-1}a^{-1}=b(ab-1)^{-1}b^{-1}a^{-1}$，

从而$((a-b^{-1})^{-1}-a^{-1})^{-1}=ab(ab-1)b^{-1}=aba-a$。

13.1.13

证明：设a_l为a的左逆元，即$a_la=1\Rightarrow a_la-1=0$。则$a(a_la-1)=(aa_l)a-a=0$。

从而$(aa_l)a=a$，由于R为无零因子环满足消去律，故$aa_l=1$。

另证：由$a_la=1\Rightarrow aa_laa_l=aa_l$，则由消去律得：$aa_l=1$。

13.1.15

证明：

1）$a(-b)=-(ab)=-(ba)=(-b)a$

2）$a(-ab)=(-a)(ab)=(-a)(ba)=-(aba)=(-ab)a$

3）$a(b+c)=ab+ac=ba+ca=(b+c)a$

4）$a(a+c)=aa+ac=aa+ca=(a+c)a$

13.2.1

证明：设$(F,+,\circ)$为域。

1）由$|F|=4$，故$(F,+)$的特征数只能是1，2，4（关于加法群的阶，根据拉格朗日定理可得），又F为域，则其特征数为素数，所以F的特征数是2。

2）由已知可设$F=\{0,e,a,a^{-1}\}$（因为出了零元素外，剩余3元素也构成群），且$a^2=a^{-1}$（因为$F\setminus\{0\}$为三阶群，由于阶为素数故$F\setminus\{0\}$为循环群，即$a^3=e$）。

① 当$x=a$时，显然有$a+e=0$或a^{-1}，

若$a+e=0\Rightarrow e+a^{-1}=0\Rightarrow a=a^{-1}$，矛盾。

故只能有$a+e=a^{-1}$，即$a+e=a^2$，满足方程$x^2=x+e$

② 当$x=a^{-1}$时，显然有$a^{-1}+e=0$或a，

若$a^{-1}+e=0\Rightarrow e+a=0\Rightarrow a=a^{-1}$，矛盾。

故只能有$a^{-1}+e=a\Rightarrow a^{-1}+e=a^{-2}=(a^{-1})^2$，满足方程$x^2=x+e$

13.2.2

解：不是。如$p=6$，则$[2]\neq[0]$，$[3]\neq[0]$，但$[2][3]=[6]=[0]$，与域为无零因子环矛盾。

13.2.3

证明：先证$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$

1）当$n=1$时，由定理知成立。

2）假设当$n=k$时也成立，即$(a\pm b)^{p^k}=a^{p^k}\pm b^{p^k}$

则当$n=k+1$时，$(a\pm b)^{p^{k+1}}=((a\pm b)^{p^k})^p=(a^{p^k}\pm b^{p^k})^p$，又根据已证定理可得：$(a^{p^k}\pm b^{p^k})^p=(a^{p^k})^p\pm(b^{p^k})^p=a^{p^{k+1}}\pm b^{p^{k+1}}$，即$(a\pm b)^{p^{k+1}}=a^{p^{k+1}}\pm b^{p^{k+1}}$。

再证$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$

$(a_1+a_2+\cdots+a_n)^p=((a_1+a_2+\cdots+a_{n-1})+a_n)^p=(a_1+a_2+\cdots+a_{n-1})^p+a_n^p$

$=(a_1+a_2+\cdots+a_{n-2})^p+a_{n-1}^p+a_n^p=\cdots=a_1^p+a_2^p+\cdots+a_{n-2}^p+a_{n-1}^p+a_n^p$。