9.14

1. 剩余类环是关于给定素数P的所有剩余类构成的环。将模P的全部剩余类记为$K_0, K_1, \cdots, K_p$，其中$K_r\ (r=0,1,\cdots,p-1)$是由一切形如$qp+r\ (q=0,\pm1,\pm2\cdots)$的整数组成的，定义r为剩余类$K_r$的代表元。

设$\forall m,n,s\in\{0,1,\cdots,p-1\}$，$a_m=q_mp+m$，$a_n=q_np+n$，$a_s=q_sp+s$ $(q_m,q_n,q_s=0,\pm1,\pm2\cdots)$

(1) 定义加法：$a_m+a_n=(q_m+q_n)p+r_{m+n}$，其中$r_{m+n}\equiv m+n \pmod p$，$r_{m+n}\in\{0,1,\cdots,p-1\}$

(2) 定义乘法：$a_m\cdot a_n=(q_m\cdot q_n)p+r_{mn}$，其中$r_{mn}\equiv mn \pmod p$，$r_{mn}\in\{0,1,\cdots,p-1\}$

检验域公理：

(1) 加法结合律 $(a_m+a_n)+a_s=[(q_m+q_n)p+r_{m+n}]+q_sp+r_s=(q_m+q_n+q_s)p+r_{(m+n)+s}$

$a_m+(a_n+a_s)=q_mp+r_m+(q_n+q_s)p+r_{n+s}=(q_m+q_n+q_s)p+r_{m+(n+s)}$

$r_{(m+n)+s}\equiv r_{m+(n+s)}\equiv m+n+s \pmod p$，$r_{(m+n)+s}$、$r_{m+(n+s)}\in\{0,1,\cdots,p-1\}$

故 $r_{(m+n)+s}=r_{m+(n+s)}\Rightarrow(a_m+a_n)+a_s=a_m+(a_n+a_s)$

(2) 加法交换律：$a_m+a_n=r_{m+n}+\cancel{a_n+a_m=r_{n+m}}(q_m+q_n)p$，$a_n+a_m=(q_m+q_n)p+r_{n+m}$

$r_{n+m}\equiv r_{m+n}\equiv m+n \pmod p$，$r_{m+n}, r_{n+m}\in\{0,1,\cdots,p-1\}$

故 $r_{n+m}=r_{m+n}\Rightarrow a_m+a_n=a_n+a_m$

(3) 加法单位元：$\exists 0\in Z_p$ st $a_m+0=q_mp+m+0=a_m$.

(4) 负元：$a_m=q_mp+m$，设$a_m'=(-q_m)p+(-m)=(-q_m-1)p+(p-m)$

$p-m\in\{0,1,\cdots,p-1\}$，故$a_m'\in Z_p$，又有：$a_m+a_m'=0$，故a_m'为a_m负元

(5) 乘法结合律：$(a_ma_n)a_s=[(q_mq_n)p+r_{mn}](q_sp+r_s)=(q_mq_nq_s)p+r_{(mn)s}$

$a_m(a_na_s)=(q_mp+r_s)[(q_nq_s)p+r_{ns}]=(q_mq_nq_s)p+r_{m(ns)}$

$r_{(mn)s}\equiv r_{m(ns)}\equiv mns \pmod p$，$r_{(mn)s}, r_{m(ns)}\in\{0,1,\cdots,p-1\}$

故 $r_{(mn)s}=r_{m(ns)}\Rightarrow(a_ma_n)a_s=a_m(a_na_s)$

(6) 乘法交换律：$a_ma_n=q_mq_np+r_{mn}$，$a_na_m=q_mq_np+r_{nm}$

$r_{mn}\equiv r_{nm}\equiv mn \pmod p$，$r_{mn}, r_{nm}\in\{0,1,\cdots,p-1\}$

故 $r_{mn}=r_{nm}\Rightarrow a_ma_n=a_na_m$

(7)乘法单位元：$\exists 1\in Z_p$ st $a_m\cdot 1=(q_m p+m)(p+1)=q_m p+m=a_m$

(8)乘法逆元：$a_m=q_m p+m$，设a_m逆元x形如$x=ap+b$.

则$a_m\cdot x=(q_m\cdot a)p+bm=1$，故$a=0$，$bm\equiv 1\pmod p$

由裴蜀定理，$(m,p)=1$，故$\exists c,d\in Z$ st $cm+dp=1$，$cm\equiv 1\pmod p$

取$b=c$，即$x=c$，则有$x=a_m^{-1}$

(9)乘法分配律：$a_m(a_n+a_s)=(q_m p+m)[(q_n+q_s)p+\cancel{r_{n+s}}]$

$=(q_m q_n+q_m q_s)p+r_{m(n+s)}$

$a_m a_n+a_m a_s=(q_m q_n)p+r_{mn}+(q_m q_s)p+r_{ns}$

$=(q_m q_n+q_m q_s)p+\cancel{(r_{mn}+r_{ms})}\ r_{mn+ms}$

$r_{m(n+s)}\equiv \cancel{r_{mn}+r_{ms}}\ r_{mn+ms}\equiv mn+ms\pmod p$，$r_{m(n+s)},r_{mn+ms}\in\{0,1,\cdots,p-1\}$

故$r_{m(n+s)}=r_{mn+ms}$，$a_m(a_n+a_s)=a_m a_n+a_m a_s$

2.反证：假设有理数不满足Archimedes公理

则$\forall m\in N^+$，都有$mx\le y$。由$x>0$得：$m\le\frac{y}{x}$

则$\frac{y}{x}$为正整数的一个上界，矛盾。故Q满足Archimedes公理

3.(1)$0^*\ne\phi$，故$\alpha\ne\phi$；$\exists p=2\in Q$ st $p^2>2$，$p\notin\alpha$，故$\alpha\ne Q$

(2)对于$\forall q\in\{p|p\ge0,p^2<2\}$，$\begin{cases}\forall p\ge0,p^2<2\text{ 且 }p<q,\ p\in\{p|p\ge0,p^2<2\}\subseteq\alpha\\ \forall p<0\text{ 且 }p<q,\ p\in 0^*\subseteq\alpha\end{cases}$

对于$\forall q\in 0^*$，$\forall p<q$，都有$p\in 0^*\subseteq\alpha$，

故若$q\in\alpha$，$\forall p<q$，都有$p\in\alpha$

(3)假设α有最大元$\frac{p}{q}$（p,q互质），$(\frac{p}{q})^2<2$，$p,q\in Z$

则$p^2<2q^2$，$2q^2-p^2>0$。由$\frac{2q}{p}\cdot\frac{p}{q}=2$，构造有理数$\frac{4}{\frac{p}{q}+\frac{2q}{p}}=\frac{4pq}{p^2+2q^2}$

$(\frac{4pq}{p^2+2q^2})^2-2=\frac{(4pq)^2-2(p^2+2q^2)^2}{(p^2+2q^2)^2}=\frac{-(p^2-2q^2)^2}{(p^2+2q^2)^2}<0$，故$\frac{4pq}{p^2+2q^2}\ \cancel{\frac{p}{q}}\in\alpha$

而$\frac{4pq}{p^2+2q^2}>\frac{4pq}{2q^2+2q^2}=\frac{p}{q}$，故矛盾（$\frac{p}{q}$非最大元）

故α中无最大元

综上：α为一个Dedekind分割

(4) $Q\setminus\alpha=\{p\mid p>0,\ p^2>2\}$ 假设 $Q\setminus\alpha$ 中有最小元 $\frac{m}{n}$ $(m,n\in Q)$，$(\frac{m}{n})^2>2$，$m^2-2n^2>0$

由 $\frac{m}{n}\cdot\frac{2n}{m}=2$，构造有理数 $\frac{\frac{m}{n}+\frac{2n}{m}}{2}=\frac{m^2+2n^2}{2mn}$

$(\frac{m^2+2n^2}{2mn})^2-2=\frac{(m^2-2n^2)^2}{4m^2n^2}>0$，故 $\frac{m^2+2n^2}{2mn}\in\alpha$

而 $\frac{m^2+2n^2}{2mn}-\frac{m}{n}=\frac{2n^2-m^2}{2mn}<0$，故 $\frac{m^2+2n^2}{2mn}$，$\frac{m}{n}$ 非最小元，矛盾

综上 $Q\setminus\alpha$ 中无最小元，故α为 Dedekind 无理分割

~~4. $E\subseteq R$，设 r 为 E 的一个上界（E应当非空且无下界）~~

~~由确界存在定理，非空有上界集合E必有上确界，记上确界为 p_0，$\forall e\in E$，$e\le p_0$~~

~~(1) $E\neq\varphi\Rightarrow\alpha\neq\varphi\Rightarrow\beta\neq\varphi$；$\forall e\in E$，$e\le p_0\Rightarrow\alpha\le p_0\Rightarrow\beta\le p_0\Rightarrow\beta\neq Q$~~

~~(2) E为实数R的子集，$\alpha\in E$，则α为Dedekind分割~~

~~对$\forall\alpha\in\beta$，$\forall r<\alpha$ 都有 $r\in\alpha\subseteq\beta$~~

4. $\beta=\bigcup_{\alpha\in E}\alpha$，E是R的一个子集，故$\alpha\in E\subseteq R$，$\alpha$为Dedekind分割

(1) $E\neq\varphi$（E应当非空）$\Rightarrow\alpha\neq\varphi\Rightarrow\beta\neq\varphi$；$\exists r$ st $\forall\alpha\in E$，$\alpha\le r\Rightarrow\forall\beta$，$\beta\le r$

(2) $\forall\alpha\in\beta$，~~$\exists r\in\alpha$ st $r>\alpha$~~ $\forall r<\alpha$ 都有 $r\in\alpha\subseteq\beta$

(3) 假设β中有最大元α_0，则$\forall\alpha\in E$，$\alpha\neq\alpha_0$，都有$\alpha<\alpha_0$.

由稠密性：$\exists\alpha_1$ st $\alpha<\alpha_1<\alpha_0$ 但$\alpha_1\notin E$，矛盾. 故β中无最大元

综上：β为Dedekind分割

5. ~~(1) $a+bi\le a+bi$ (2) $a+bi\le a+bi$ $a+bi\ge a+bi$~~

由定义可知：满足：自反性、反对称性、传递性、全序性（易证）

(1) 加法保序性 $a+bi\le c+di$，

<1> $a<c\Rightarrow(a+m)+(b+n)i<(c+m)+(d+n)i$

<2> $a=c,\ b<d\Rightarrow(a+m)+(b+n)i<(c+m)+(d+n)i$

<3> $a=c,\ b=d\Rightarrow(a+m)+(b+n)i=(c+m)+(d+n)i$

(2) 乘法保序性：若虚部非0，不可比较且与0大小；若虚部为0，易证成立

无最小上界性。反例：$\{1+ni\}$，$(n\in N_+)$

$1+ni<2$，2为其上界；由反证法可证其无上确界（无最大自然数）

6. 确界存在定理：非空有上(下)界数集必有上(下)确界

[证明] 实数无限小数表示 ~~⇒ 提取每一位的最大值 a_0~~（以上确界证明为例）

⇒ 整数部分最大值 a_0、小数部分每一位最大值 $a_1, a_2 \cdots a_n \cdots$

⇒ 往证 $\beta = a_0.a_1a_2\cdots a_n\cdots$ 为其上确界

<1> 逐位比较可知，数集A中 $\forall x\in A$，都有 $x\le\beta$，β为A的一个上界

<2> 设 $\forall x_0\in A$，$x_0<\beta$，则 $\exists N$ st x_0在第N位小数后的数小于β

对于 ~~β N~~ $\beta - x_0 \le \frac{1}{10^N} < \varepsilon$，可得 $x_0 > \beta-\varepsilon$，即任意小于β的数均非上界

故β为上确界

9.15.

1. $\alpha>0^*$，$\beta-\sigma\geq 0^*\Rightarrow\exists p^*\ st\ \alpha>p^*>0^*$

$M_{\alpha(\beta-\sigma)}\supset M_{p^*(\beta-\sigma)}$，故$\alpha\beta$时$\sup M_{\alpha(\beta-\sigma)}\geq\sup M_{p^*(\beta-\sigma)}=p^*(\beta-\sigma)\geq 0$

故$\alpha(\beta-\sigma)\geq 0\Rightarrow\alpha\beta\geq\alpha\sigma$

2. ~~设α=设~~ ~~$B\subset X$，$B\neq\emptyset$且有下界，记L为B的所有下界的集~~，

~~则有$\alpha=\sup L\in X$~~

已知有序集X有最小上界性，设$B\subset X$，$B\neq\emptyset$且有下界，记L为B所有下界的集，

往证则有$\alpha=\sup L\in X$，且$\alpha=\inf X$.

<1> $\forall a\in L$，$\forall b\in B$，都有$a\leq b$。对L而言，B中任一元素均为L的一个上界

由于$B\neq X$，故可对集合$L\cap X$使用S的最小上界性，得$\alpha=\sup L\in S$

<2> 若$\forall\beta<\alpha$，β非L上界，故$\beta\notin B$

若$\forall\beta\geq\alpha$，β是L上界，故$\beta\in B$

可知B中任一元素均大于等于α，故α为B一个下界

$\forall r>\alpha=\sup L$，$r\notin L$，故r非B的下界。即：B中比α大的元素非下界$\Rightarrow\alpha=\inf B$

综上：X有最大下界性.

3. X为全序集，故集合X为全序有限集

若$card(X)=0$，$X=\phi$. 成立

若$card(X)=1$，唯一元素即为最大元兼最小元

若$card(X)=2$，利用X中序关系可得最大元与最小元

归纳法，假设$card(X)=n$成立. 对$card(X)=n+1$. 提取其中任意一个n元有限子集$\{x_i\}$ $(i=1,\cdots,n)$，由归纳假设，其必有最大值与最小值。不失一般性，设最大值为x_n，最小值为x_1，记$x_{n+1}\in X\setminus\{x_i\}_{i=1}^n$.

<1> $x_{n+1}>x_n$，则$\forall x_i\in\{x_i\}_{i=1}^n$ $x_{n+1}>x_n\geq x_i$，故x_{n+1}为最大元，x_1为最小元

<2> $x_1>x_{n+1}$，则$\forall x_i\in\{x_i\}_{i=1}^n$ $x_{n+1}<x_1\leq x_i$，故x_{n+1}为最小元，x_n为最大元

(3) $x_1 \le x_{n+1}$ 且 $x_{n+1} \le x_n$. 则 $\forall x_i \in \{x_i\}_{i=1}^{n+1}$, $x_1 \le x_i \le x_n$, x_n 为最大元, x_1 为最小元

4. 若 $\alpha > 0^*$, 令 $\beta = \sup\{\sigma \mid 0^* < \sigma\alpha \le 1^*\} = \sup E$ (非空有上界)

下面证明 $\beta = \alpha^{-1}$, 即 $\alpha\beta = 1^*$

事实上: $\forall s > 0$. $\exists p$ st $p^* < \alpha < (p+s)^*$

$1^* = (p \cdot p^{-1})^* = p^*(p^{-1})^* < \alpha(p^{-1})^* \Rightarrow (p^{-1})^*$ 是 E 的一个上界

$1^* = [(p+s)(p+s)^{-1}]^* = (p+s)^*[(p+s)^{-1}]^* > [(p+s)^{-1}]^*\alpha$, $[(p+s)^{-1}]^* \in E$

由 $\beta = \sup\{\sigma \mid 0^* < \sigma\alpha \le 1^*\}$ 可知

$[(p+s)^{-1}]^* < \beta < (p^{-1})^*$

故 $\alpha\beta \le (p^{-1})^*(p+s)^* = (1 + \frac{s}{p})^* \Rightarrow \alpha\beta \le 1^*$

$\alpha\beta \ge p^*[(p+s)^{-1}]^* = (1 - \frac{s}{p+s})^* \Rightarrow \alpha\beta \ge 1^*$

故 $\alpha\beta = 1^*$

5. 假设不具有阿基米德性, 则 $\exists x_0, y_0$ st $\forall n \in \mathbb{N}, nx_0 < y_0$

记所有 nx_0 集合为 B, 由最小上界性. B 有最小上界 b_0. $b_0 < y_0$ 且 $\forall nx_0 < b_0$.

$\Rightarrow (n+1)x_0 < b_0 - x_0$, 对 $\forall n$ 成立. $\Rightarrow b_0 - x_0$ 为 B 最小上界 $\Rightarrow$ 与 b_0 为最小上界矛盾

故具有阿基米德性

6. 反证. 设 $(X, +, \cdot, \le)$ 无最小上界性,

对于域中有非空有序集合 S. 设 $E \subsetneq S$ 且 $E \ne \phi$, 设 $\exists \alpha \in S$ 且 $\alpha \notin E$, st $\forall e \in E$, $\alpha > e$

则 E 为 S 有序子集, 但无最小上界性, 故 $\sup E \notin S$

又由 $\sup E \ge e$, 故 $\forall s_0 \in S$, $\sup E > s_0$.

但 $\alpha \in S$, $\sup E > \alpha > e$, α 亦为 E 上界 $\Rightarrow$ 与上确界定义矛盾.

故 $(X, +, \cdot, \le)$ 无最小上界性.