第一周

第一题

写出$\mathbb{Z}_{15}$中所有可逆元，并求出相应逆元。

解：注意到

$$\mathbb{Z}_{15}=\{\overline{n}:0\leq n<15,n\in\mathbb{N}\} \tag{1}$$

因此

$$\mathbb{Z}_{15}^*=\{\overline{n}:(n,15)=1\}=\{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\} \tag{2}$$

同时

$$\overline{1}\cdot\overline{1}=\overline{1},\quad \overline{2}\cdot\overline{8}=\overline{1},\quad \overline{4}\cdot\overline{4}=\overline{1},\quad \overline{7}\cdot\overline{13}=\overline{1},\quad \overline{11}\cdot\overline{11}=\overline{1},\quad \overline{14}\cdot\overline{14}=\overline{1} \tag{3}$$

第二题

写出$\mathbb{Z}_3$中的加法表和乘法表。

解：加法表如下

$$\overline{0}+\overline{0}=\overline{0},\quad \overline{0}+\overline{1}=\overline{1},\quad \overline{0}+\overline{2}=\overline{2},\quad \overline{1}+\overline{1}=\overline{2},\quad \overline{1}+\overline{2}=\overline{0},\quad \overline{2}+\overline{2}=\overline{1} \tag{4}$$

乘法表如下

$$\overline{0}\times\overline{0}=\overline{0},\quad \overline{0}\times\overline{1}=\overline{0},\quad \overline{0}\times\overline{2}=\overline{0},\quad \overline{1}\times\overline{1}=\overline{1},\quad \overline{1}\times\overline{2}=\overline{2},\quad \overline{2}\times\overline{2}=\overline{1} \tag{5}$$

第三题

试说明$\mathbb{Z}$对于运算$a*b=a+b+4$是否构成群?

解：我们来逐条验证群的定义。

第一，对于$*$运算的封闭性。对于任意$a,b\in\mathbb{Z}$，显然成立$a*b=a+b+4\in\mathbb{Z}$。

第二，存在单位元。对于任意$a\in\mathbb{Z}$，$a*(-4)=(-4)*a=a+(-4)+4=a$，因此-4为单位元。

第三，存在逆元。对于任意$a\in\mathbb{Z}$，$a*(-a-8)=(-a-8)*a=a+(-a-8)+4=-4$，因此$-a-8$为$a$的逆元。

第四，满足结合律。对于任意$a,b,c\in\mathbb{Z}$，显然成立

$$(a*b)*c=(a+b+4)+c+4=a+b+c+8=a+(b+c+4)+4=a*(b*c) \tag{6}$$

因此$\mathbb{Z}$对于$*$运算构成群。事实上，$\mathbb{Z}$对于$*$运算构成Abel群。

第二周

第一题

在S_5中，设

$$\sigma_1=\begin{pmatrix}1&2&3&4&5\\3&1&5&2&4\end{pmatrix},\qquad \sigma_2=\begin{pmatrix}1&2&3&4&5\\4&5&1&3&2\end{pmatrix} \tag{7}$$

求$\sigma_1\sigma_2$，$\sigma_2\sigma_1$，σ_1^{-1}，$\sigma_1\sigma_2\sigma_1^{-1}$。

写出σ_1和σ_2的轮换分解式和对换分解式，并说明σ_1和σ_2是奇置换还是偶置换。

解：容易求出

$$\sigma_1\sigma_2=\begin{pmatrix}1&2&3&4&5\\2&4&3&5&1\end{pmatrix},\qquad \sigma_2\sigma_1=\begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix} \tag{8}$$

$$\sigma_1^{-1}=\begin{pmatrix}1&2&3&4&5\\2&4&1&5&3\end{pmatrix},\qquad \sigma_1\sigma_2\sigma_1^{-1}=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix} \tag{9}$$

$$\sigma_1=(13542)=(12)(14)(15)(13),\qquad \sigma_2=(143)(25)=(13)(14)(25) \tag{10}$$

σ_1为偶置换，σ_2为奇置换。

第二题

证明：对于$\sigma=(i_1\cdots i_r)$，以及任意$\tau\in S_n$，成立

$$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_r)) \tag{11}$$

证明：任取$k\in\{1,\cdots,r\}$，注意到

$$(\tau\sigma\tau^{-1})(\tau(i_k))=\tau\sigma\tau^{-1}\tau(i_k)=\tau\sigma(i_k)=\tau(i_{k+1}) \tag{12}$$

其中$i_{r+1}=r_1$，这说明$(\tau(i_1)\cdots\tau(i_r))$构成轮换。

任取$x\in\Omega\setminus\{i_1,\cdots,i_k\}$，那么$(\tau\sigma\tau^{-1})(x)=x$。

综上所述，$\tau\sigma\tau^{-1}=(\tau(i_1)\cdots\tau(i_r))$，原命题得证！

第四周

第一题

定义

$$k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}, \qquad k \in \mathbb{N}^* \tag{13}$$

证明：$(k\mathbb{Z}, +)$为群$(\mathbb{Z}, +)$的循环子群。

证明：显然$k\mathbb{Z} \subset \mathbb{Z}$。任取$a, b \in k\mathbb{Z}$，那么存在$m, n \in \mathbb{Z}$，使得成立$a = km, b = kn$，注意到

$$a - b = k(m - n) \in k\mathbb{Z} \tag{14}$$

因此$k\mathbb{Z}$为$\mathbb{Z}$的子群。

下面证明$k\mathbb{Z} = \langle k \rangle$，任取$a \in k\mathbb{Z}$，那么存在$n \in \mathbb{Z}$，使得成立$a = kn = nk$，因此$k\mathbb{Z}$为由$k$生成的循环群。

第二题

在域$\mathbb{Q}$上行列式为1的2阶矩阵乘法群$\mathrm{SL}_2(\mathbb{Q})$中，设

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \tag{15}$$

证明：$|A| = 4, |B| = 3, |AB| = \infty$

证明：容易知道

$$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{16}$$

$$B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{17}$$

记

$$C = AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{18}$$

那么由归纳法容易得到

$$C^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \tag{19}$$

于是

$$|A| = 4, |B| = 3, |AB| = \infty \tag{20}$$

第三题

求6阶循环群$G = \langle a \rangle$的所有子群。

证明：G的全部子群为

$$\langle e \rangle, \qquad \langle a \rangle, \qquad \langle a^2 \rangle, \qquad \langle a^3 \rangle \tag{21}$$

第五周

第一题

在$\mathbb{Z}_9^*$中，$\overline{2}$的阶是多少？是否成立$(\mathbb{Z}_9^*,\times)\cong(\mathbb{Z}_6,+)$？

证明：在$\mathbb{Z}_9^*$中，$|\overline{2}|=6$，而在$\mathbb{Z}_6$中，$|\overline{2}|=3$，因此$(\mathbb{Z}_9^*,\times)\ncong(\mathbb{Z}_6,+)$。

第二题

定义群映射

$$\begin{aligned} f:&(\mathbb{R},+)\to(\mathbb{C}\setminus\{0\},\times) && (22)\\ &x\mapsto \mathrm{e}^{2\pi ix} && (23)\end{aligned}$$

第一问

证明：f是群同态映射。

证明：显然f是定义良好的。任取$x,y\in\mathbb{R}$，那么
$f(x+y)=\mathrm{e}^{2\pi i(x+y)}=\mathrm{e}^{2\pi ix}\mathrm{e}^{2\pi iy}=f(x)f(y)$，因此$f$是群同态映射。

第二问

求$\mathrm{Ker}\ f$和$\mathrm{Im}\ f$。

证明：

$$\mathrm{Ker}\ f=\{x\in\mathbb{R}:f(x)=1\}=\{x\in\mathbb{R}:\mathrm{e}^{2\pi ix}=1\}=\mathbb{Z} \tag{24}$$

$$\mathrm{Im}\ f=\{f(x):x\in\mathbb{R}\}=\{\mathrm{e}^{2\pi ix}:x\in\mathbb{R}\}=\partial\mathbb{D} \tag{25}$$

其中$\mathbb{D}=\{z\in\mathbb{C}:|z|<1\}$。

第三题

定义群映射

$$\begin{aligned} f:&(\mathbb{C}\setminus\{0\},\times)\to(\mathbb{C}\setminus\{0\},\times) && (26)\\ &z\mapsto \frac{z}{|z|} && (27)\end{aligned}$$

证明：f是群同态映射，并求$\mathrm{Ker}\ f$和$\mathrm{Im}\ f$。

证明：显然f是定义良好的。任取$z,w\in\mathbb{C}\setminus\{0\}$，注意到
$f(zw)=\dfrac{zw}{|zw|}=\dfrac{z}{|z|}\dfrac{w}{|w|}=f(z)f(w)$，因此$f$是群同态映射。

$$\mathrm{Ker}\ f=\{x\in\mathbb{C}\setminus\{0\}:f(x)=1\}=\{x\in\mathbb{C}\setminus\{0\}:z/|z|=1\}=\mathbb{R}^+ \tag{28}$$

$$\mathrm{Im}\ f=\{f(x):x\in\mathbb{C}\setminus\{0\}\}=\{z/|z|:x\in\mathbb{C}\setminus\{0\}\}=\{z\in\mathbb{C}:|z|=1\} \tag{29}$$

第四题

证明：

$$(\mathbb{C}\setminus\{0\})/\mathbb{R}^+\cong\partial\mathbb{D} \tag{30}$$

其中$\mathbb{D}=\{z\in\mathbb{C}:|z|=1\}$。

证明：

方法一：构造映射

$$\begin{aligned}\varphi:&\mathbb{C}\setminus\{0\}\to\mathbb{C}\setminus\{0\} &(31)\\ \rho\mathrm{e}^{i\theta}&\mapsto\frac{\rho}{|\rho|}\mathrm{e}^{i\theta} &(32)\end{aligned}$$

首先证明φ为群同态映射。任取$\rho,\varrho\in\mathbb{R}^+$以及$\theta,\vartheta\in\mathbb{R}$，注意到

$$\varphi(\rho\mathrm{e}^{i\theta}\varrho\mathrm{e}^{i\vartheta})=\varphi(\rho\varrho\mathrm{e}^{i(\theta+\vartheta)})=\frac{\rho\varrho}{|\rho\varrho|}\mathrm{e}^{i(\theta+\vartheta)}=\frac{\rho}{|\rho|}\mathrm{e}^{i\theta}\frac{\varrho}{|\varrho|}\mathrm{e}^{i\vartheta}=\varphi(\rho\mathrm{e}^{i\theta})\varphi(\varrho\mathrm{e}^{i\vartheta}) \tag{33}$$

其次，注意到

$$\begin{aligned}&\mathrm{Ker}\,\varphi=\{\rho\mathrm{e}^{i\theta}:\varphi(\rho\mathrm{e}^{i\theta})=1,\rho\in\mathbb{R}^+,\theta\in\mathbb{R}\}=\{\rho\mathrm{e}^{i\theta}:\rho\mathrm{e}^{i\theta}/|\rho|=1,\rho\in\mathbb{R}^+,\theta\in\mathbb{R}\}=\mathbb{R}^+ &(34)\\ &\mathrm{Im}\,\varphi=\{\varphi(\rho\mathrm{e}^{i\theta}):\rho\in\mathbb{R}^+,\theta\in\mathbb{R}\}=\partial\mathbb{D} &(35)\end{aligned}$$

由同构定理

$$(\mathbb{C}\setminus\{0\})/\mathbb{R}^+\cong\partial\mathbb{D} \tag{36}$$

方法二：构造映射

$$\begin{aligned}\varphi:&(\mathbb{C}\setminus\{0\})/\mathbb{R}^+\to\partial\mathbb{D} &(37)\\ \rho\mathrm{e}^{i\theta}\mathbb{R}^+&\mapsto\mathrm{e}^{i\theta} &(38)\end{aligned}$$

首先考察此映射的定义良好性。任取$\rho,\varrho\in\mathbb{R}^+$以及$\theta,\vartheta\in\mathbb{R}$，满足$\rho\mathrm{e}^{i\theta}\mathbb{R}^+=\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+$，因此$\theta\equiv\vartheta\mod 2\pi$，进而$\varphi(\rho\mathrm{e}^{i\theta}\mathbb{R}^+)=\mathrm{e}^{i\theta}=\mathrm{e}^{i\vartheta}=\varphi(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+)$，于是$\varphi$是定义良好的。

其次证明φ为群同态映射。任取$\rho,\varrho\in\mathbb{R}^+$以及$\theta,\vartheta\in\mathbb{R}$，注意到

$$\varphi((\rho\mathrm{e}^{i\theta}\mathbb{R}^+)(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+))=\varphi(\rho\varrho\mathrm{e}^{i(\theta+\vartheta)}\mathbb{R}^+)=\mathrm{e}^{i(\theta+\vartheta)}=\mathrm{e}^{i\theta}\mathrm{e}^{i\vartheta}=\varphi(\rho\mathrm{e}^{i\theta}\mathbb{R}^+)\varphi(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+) \tag{39}$$

因此φ为群同态映射。

最后证明φ为双射。任取$\rho,\varrho\in\mathbb{R}^+$以及$\theta,\vartheta\in\mathbb{R}$，注意到

$$\begin{aligned}&\varphi(\rho\mathrm{e}^{i\theta}\mathbb{R}^+)=\varphi(\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+) &(40)\\ \Longrightarrow\ &\mathrm{e}^{i\theta}=\mathrm{e}^{i\vartheta} &(41)\\ \Longrightarrow\ &\mathrm{e}^{i\theta}\mathbb{R}^+=\mathrm{e}^{i\vartheta}\mathbb{R}^+ &(42)\\ \Longrightarrow\ &\rho\mathrm{e}^{i\theta}\mathbb{R}^+=\varrho\mathrm{e}^{i\vartheta}\mathbb{R}^+, &(43)\\ & &(44)\\ &\varphi(\mathrm{e}^{i\theta}\mathbb{R}^+)=\mathrm{e}^{i\theta} &(45)\end{aligned}$$

因此φ为双射。

综合以上三点

$$(\mathbb{C}\setminus\{0\})/\mathbb{R}^+\cong\partial\mathbb{D} \tag{46}$$

第十周

第一问

证明：有限整环为域。

证明：如果R为有限整环，那么任取$r \in R \setminus \{0\}$，考虑主理想(r)。如果$|(r)| < |R|$，那么存在互异元素$a, b \in R$，使得成立$ar = br$。由消去律，$a = b$，矛盾！因此$|(r)| = |R|$，那么$(r) = R$。注意到$1 \in R = (r)$，那么存在$s \in R$，使得成立$rs = sr = 1$，进而R为域。

第二问

证明：域没有非平凡理想。

证明：如果R为域，任取R的非零理想I，那么存在$r \in I \setminus \{0\}$，而R为域，因此$1 = r^{-1}r \in I$，那么$I = R$，进而R仅存在平凡理想。

第三问

证明：如果交换幺环R没有非平凡理想，那么R为域。

证明：如果R不为域，那么存在$r_0 \in R \setminus \{0\}$，使得对于任意$r \in R$，成立$r_0 r \neq 1$，进而$\{0\} \subsetneq (r_0) \subsetneq R$，因此$R$存在非平凡理想$(r_0)$，矛盾！从而$R$为域。

第十一周

第一题

第一问

证明：对于满的环同态映射$\varphi: R \to S$，如果I为R的理想，那么$\varphi(I)$为S的理想。

证明：任取$a, b \in I$，那么$a - b \in I$，进而

$$\varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(I) \tag{47}$$

任取$r \in R$，那么$ar, ra \in I$，进而

$$\varphi(r)\varphi(a) = \varphi(ra) \in \varphi(I), \qquad \varphi(a)\varphi(r) = \varphi(ar) \in \varphi(I) \tag{48}$$

因此$\varphi(I)$为S的理想。

第二问

证明：对于满的环同态映射$\varphi: R \to S$，如果I为S的理想，那么$\varphi^{-1}(I)$为R的理想，且$\operatorname{Ker} \varphi \subset \varphi^{-1}(I)$。

证明：任取$a, b \in \varphi^{-1}(I)$，那么

$$\varphi(a - b) = \varphi(a) - \varphi(b) \in I \implies a - b \in \varphi^{-1}(I) \tag{49}$$

任取$r \in R$，那么$\varphi(a)\varphi(r), \varphi(r)\varphi(a) \in I$，进而

$$\varphi(ar) = \varphi(a)\varphi(r) \in I, \qquad \varphi(ra) = \varphi(r)\varphi(a) \in I \implies ar, ra \in \varphi^{-1}(I) \tag{50}$$

因此$\varphi^{-1}(I)$为R的理想。而$\{0\} \subset I$，因此$\operatorname{Ker} \varphi \subset \varphi^{-1}(I)$。

第二题

求解如下同余方程：

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases} \tag{51}$$

解：注意到

$$\begin{cases} x \equiv 1 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 0 \mod 7 \end{cases} \iff x \equiv 70 \mod 105 \tag{52}$$

$$\begin{cases} x \equiv 0 \mod 3 \\ x \equiv 1 \mod 5 \\ x \equiv 0 \mod 7 \end{cases} \iff x \equiv 21 \mod 105 \tag{53}$$

$$\begin{cases} x \equiv 0 \mod 3 \\ x \equiv 0 \mod 5 \\ x \equiv 1 \mod 7 \end{cases} \iff x \equiv 15 \mod 105 \tag{54}$$

因此

$$\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases} \iff x \equiv 23 \mod 105 \tag{55}$$

第十二周

第一题

证明：域F上一元多项式环$F[x]$的理想为主理想，其中非(0)主理想可以由首一多项式生成。

证明：取$F[x]$的理想I，如果$I=\{0\}$为平凡理想，那么$I=(0)$。如果$I\neq\{0\}$，那么取I中次数最小的非零首一多项式$g(x)$。对于任意$f(x)\in I$，作带余除法，成立$f(x)=g(x)q(x)+r(x)$，其中$\deg(r(x))<\deg(g(x))$。注意到$r(x)=f(x)-g(x)q(x)\in I$，因此$r(x)=0$，进而$f(x)=g(x)q(x)$。由$f(x)$的任意性，$I=(g(x))$。

第二题

构造含8个元素的有限域。

解：由于$\mathbb{Z}_2$为2阶域，那么取$\mathbb{Z}_2[x]$中的3次不可约多项式x^3+x+1，因此$\mathbb{Z}_2[x]/(x^3+x+1)$为8阶有限域，其中对于任意$f(x)\in\mathbb{Z}_2[x]/(x^3+x+1)$，存在且存在唯一$a_0,a_1,a_3\in\mathbb{Z}_2$，使得成立

$$f(x)=a_0+a_1x+a_2x^2+(x^3+x+1) \tag{56}$$

第三题

证明：$\sqrt{2}+\sqrt{3}$为代数数，并求$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上的极小多项式。

证明：注意到

$$\begin{aligned} & x=\sqrt{2}+\sqrt{3} && (57)\\ \Longrightarrow\ & (x-\sqrt{2})^3=3 && (58)\\ \Longleftrightarrow\ & x^2-1=2\sqrt{2}x && (59)\\ \Longrightarrow\ & (x^2-1)^2=8x^2 && (60)\\ \Longleftrightarrow\ & x^4-10x^2+1=0 && (61)\end{aligned}$$

因此$\sqrt{2}+\sqrt{3}$为整系数方程x^4-10x^2+1的根，因此$\sqrt{2}+\sqrt{3}$为代数数，且

$$x^4-10x^2+1=(x+(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{3}-\sqrt{2}))(x+(\sqrt{2}-\sqrt{3})) \tag{62}$$

因此x^4-10x^2+1为$\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上的极小多项式。

第四题

设$t\in\mathbb{C}$为$f(x)=x^3-x+1$的根，在代数数域$\mathbb{Q}[t]$中求

$$(5t^2+3t-1)(2t^2-2t+6),\qquad (3t^2-t+2)^{-1} \tag{63}$$

解：由于$t^3=t-1$，那么

$$\begin{aligned}(5t^2+3t-1)(2t^2-2t+6)=&10x^4-4x^3+22x^2+20x-6 && (64)\\ =&10t(t-1)-4(t-1)+22t^2+20t-6 && (65)\\ =&32t^2+6t-2 && (66)\end{aligned}$$

令

$$
\begin{aligned}
& (3t^2 - t + 2)(at^2 + bt + c) = 1 && (67)\\
\Longleftrightarrow\ & 3at^4 + (3b - a)t^3 + (2a - b + 3c)t^2 + (2b - c)t + (2c - 1) = 0 && (68)\\
\Longleftrightarrow\ & 3at(t - 1) + (3b - a)(t - 1) + (2a - b + 3c)t^2 + (2b - c)t + (2c - 1) = 0 && (69)\\
\Longleftrightarrow\ & (5a - b + 3c)t^2 + (-4a + 5b - c)t + (a - 3b + 2c - 1) = 0 && (70)\\
\Longleftrightarrow\ & \begin{cases} 5a - b + 3c = 0 \\ -4a + 5b - c = 0 \\ a - 3b + 2c = 1 \end{cases} && (71)\\
\Longleftrightarrow\ & a = -\frac{2}{7}, b = -\frac{1}{7}, c = \frac{3}{7} && (72)
\end{aligned}
$$

因此

$$
(3t^2 - t + 2)^{-1} = (-2t^2 - t + 3)/7 \tag{73}
$$