代数学基础习题课

1. 集合的大小

集合包括有限集和无限集, 无限集又包括可数有限集和不可数有限集. 凡是能与 $\mathbb{Z}$ 能建立一一对应的称为可数集. 例如 $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}^n$ 都是可数集合, 而 $\mathbb{R}, \mathbb{C}, \mathbb{R}^n$ 都是不可数集合. 集合的基数, 是用来描述集合的大小的, 一般记为 $|A|$ 或 $\mathrm{card}(A)$. 利用反证法可以证明集合的幂集总是比自身大, 特别地, $|P(\mathbb{Z})| = |\mathbb{R}|$. 某些书上可数集的定义会包含有限集.

1.5. 注意集合大小的概念, 无限不等于可数.

由于 X 是无限集, $Y \subseteq X$ 有限, 因此 $X - Y$ 无限. 设 $Y = \{a_1, \ldots, a_k\}$. 取 $X - Y$ 中一串两两不同的元素 $a_{k+1}, \ldots, a_n, \ldots$ (可以用数学归纳法), 记 $A = \{a_{k+1}, \ldots, a_n, \ldots\}$, 令

$$\varphi : X - Y \to X$$

$$x \mapsto \begin{cases} a_{n-k}, & \text{若 } x = a_n \in A; \\ x, & \text{若} x \notin A. \end{cases}$$

容易验证 φ 是双射.

2. 关系的定义与理解

什么是关系? 设 A 是一个集合, $R \subseteq A \times A$ 称为 A 上面的一个关系. 一个关系总是定义在一个集合上, 就像一个映射总是定义在两个集合之间. 因而 $\geq$ 并不是一个关系, 如同 $f : x \mapsto x^2$ 并不是一个映射. 关系的定义并不要求有什么实际的意义, 任意一个 $A \times A$ 的子集, 包括空集, 都是其上的一个关系. 例子:

- A 为任意集合, $R = \emptyset$ 满足对称性, 传递性, 但不满足自反性.
- $A = \mathbb{R}, R = \{(a, b) \mid a, b \in A, a > b\}$, 满足传递性.
- $A = \mathbb{R}, R = \{(a, b) \mid a, b \in A, a \geq b\}$, 满足自反性, 传递性.
- $A = \mathbb{R}, R = \{(a, b) \mid a, b \in A, a \neq b\}$, 满足对称性.
- $A = \{\mathbb{R}^2$ 中所有直线 $\}, R = \{(a, b) \in A \mid a//b\}$, 满足对称性.
- $A = \{\mathbb{R}^2$ 中所有直线 $\}, R = \{(a, b) \in A \mid a$ 和 b 有公共点 $\}$, 满足自反性, 对称性.
- $A = \{$ 所有2维实向量 $\}, R = \{(a, b) \in A \mid a//b\}$, 满足自反性, 对称性.
- $A = \mathbb{Z}_{>0}, R = \{(a, b) \in A \mid a$ 整除 $b\}$, 满足自反性, 传递性.

1.7. 设这个关系为 $\sim$. 对任意 $a \in A$, 存在 $b \in A$, 使得 $a \sim b$. 由对称性 $b \sim a$, 由传递性 $a \sim a$. 因此 $\sim$ 满足自反性, $\sim$ 是等价关系.

3. 求和号 $\sum$ 的使用

注意 $\sum$ 的指标是没有实际意义的, 也就是说, 指标用 i 还是 j 表示本质上都是一样的.

1.11(4).

$$\begin{aligned}
&\sum_{i=1}^{n}\sum_{j=1}^{n}(i+j)^2 = \sum_{i=1}^{n}\sum_{j=1}^{n}(i^2+2ij+j^2)\\
=&\sum_{i=1}^{n}i^2\sum_{j=1}^{n}1 + 2\sum_{i=1}^{n}i\sum_{j=1}^{n}j + \sum_{i=1}^{n}1\sum_{j=1}^{n}j^2\\
=&2n \times \frac{n(n+1)(2n+1)}{6} + 2(\frac{n(n+1)}{2})^2\\
=&\frac{n^2(n+1)(2n+1)}{3} + \frac{n^2(n+1)^2}{2} = \frac{n^2(n+1)(7n+5)}{6}
\end{aligned}$$

或者

$$\begin{aligned}
&\sum_{i=1}^{n}\sum_{j=1}^{n}(i+j)^2 = \sum_{k=1}^{n}(k-1)k^2 + \sum_{k=n+1}^{2n}(2n+1-k)k^2\\
=&\sum_{k=1}^{n}(k-1-2n-1+k)k^2 + \sum_{k=1}^{2n}(2n+1-k)k^2\\
=&2\sum_{k=1}^{n}k^3 - 2(n+1)\sum_{k=1}^{n}k^2 + (2n+1)\sum_{k=1}^{2n}k^2 - \sum_{k=1}^{2n}k^3\\
=&\frac{n^2(n+1)^2}{2} - \frac{n(n+1)^2(2n+1)}{3} + \frac{n(2n+1)^2(4n+1)}{3} - n^2(2n+1)^2\\
=&\frac{7}{6}n^4 + 2n^3 + \frac{5}{6}n^2
\end{aligned}$$

2.1. 原题本意是要证明 2×2 的矩阵乘法满足结合律.

设 $A=(a_{ij})_{n\times m}, B=(b_{ij})_{m\times s}, C=(c_{ij})_{s\times t}$ 为3个矩阵, 设 $AB=(d_{ij})_{n\times s}$, $BC=(e_{ij})_{m\times t}$. 则由矩阵乘法,

$$d_{ik}=\sum_{j=1}^{m}a_{ij}b_{jk},\quad e_{jl}=\sum_{k=1}^{s}b_{jk}c_{kl},$$

$$(AB)C \text{ 的 } (i,l) \text{ 分量}=\sum_{k=1}^{s}d_{ik}c_{kl}=\sum_{k=1}^{s}\sum_{j=1}^{m}a_{ij}b_{jk}c_{kl}$$

$$=\sum_{j=1}^{m}\sum_{k=1}^{s}a_{ij}b_{jk}c_{kl}=\sum_{j=1}^{m}a_{ij}e_{jl}=A(BC) \text{ 的 } (i,l) \text{ 分量}.$$

因此, 矩阵乘法满足结合律.

4. 群与环的验证

证明一个集合上的二元运算构成群, 需要验证的一般只有3条. 但是常常我们需要首先验证运算的封闭性, 也就是验证它确实是一个二元运算.

由于大量已知群的存在, 我们常常可以把问题化为证明其是另一个群的子群, 这样可以节省大量的时间.

环的情形也与群类似.

2.7. (1) 首先容易看出 $X\triangle Y=Y\triangle X$.

$$\begin{aligned}(X\triangle Y)\triangle Z&=\big(((X\cap Y^c)\cup(X^c\cap Y))\cap Z^c\big)\cup\big(((X\cap Y^c)\cup(X^c\cap Y))^c\cap Z\big)\\&=(X\cap Y^c\cap Z^c)\cup(X^c\cap Y\cap Z^c)\cup\big(((X^c\cup Y)\cap(X\cup Y^c))\cap Z\big)\\&=(X\cap Y^c\cap Z^c)\cup(X^c\cap Y\cap Z^c)\cup(X^c\cap Y^c\cap Z)\cup(X\cap Y\cap Z),\end{aligned}$$

因此

$$\begin{aligned}X\triangle(Y\triangle Z)&=(Z\triangle Y)\triangle X\\&=(Z\cap Y^c\cap X^c)\cup(Z^c\cap Y\cap X^c)\cup(Z^c\cap Y^c\cap X)\cup(Z\cap Y\cap X)\\&=(X\triangle Y)\triangle Z.\end{aligned}$$

结合律满足.

(2)

$$\emptyset\triangle X=X\triangle\emptyset=(X\cap A)\cup(X^c\cap\emptyset)=X.$$

因此 $\emptyset$ 是幺元.

(3)

$$X\triangle X=(X\cap X^c)\cup(X^c\cap X)=\emptyset.$$

因此任意元素有逆.

因此命题得证.

2.9. (1) 设 $y_i(x)=\frac{a_ix+b_i}{c_ix+d_i}, i=1,2$, 则

$$\begin{aligned}(y_1\circ y_2)(x)&=\frac{a_1y_2(x)+b_1}{c_1y_2(x)+d_1}\\&=\frac{a_1(a_2x+b_2)+b_1(c_2x+d_2)}{c_1(a_2x+b_2)+d_1(c_2x+d_2)}\\&=\frac{(a_1a_2+b_1c_2)x+a_1b_2+b_1d_2}{(c_1a_2+d_1c_2)x+c_1b_2+d_1d_2},\end{aligned}$$

$(a_1a_2+b_1c_2)(c_1b_2+d_1d_2)-(a_1b_2+b_1d_2)(c_1a_2+d_1c_2)=(a_1d_1-b_1c_1)(a_2d_2-b_2c_2)\neq 0$,

因此该集合关于函数复合封闭.

显然函数复合满足结合律, 恒等映射 $\mathrm{id}(x)=x$ 是幺元.

令 $z(x)=\frac{dx-b}{-cx+a}$, 则

$$(y\circ z)(x)=(z\circ y)(x)=x.$$

因此 z 是 y 的逆.

故该集合构成群.

(2) 令 G 为这样的函数全体,

$$H=\{A\in \mathrm{GL}_2(\mathbb{R})\mid \det A=\pm 1\}.$$

则容易看出对任意 $A,B\in H$, $\det(AB^{-1})=\pm 1, AB^{-1}\in H$, 故 $H\leqslant \mathrm{GL}_2(\mathbb{R})$. 令

$$\varphi: H\to G$$

$$A=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\mapsto y,\ y(x)=\frac{ax+b}{cx+d}.$$

对任意 $y\in G, y(x)=\frac{ax+b}{cx+d}$, 令 $\alpha=\sqrt{|ad-bc|}$, $A=\alpha^{-1}\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, 则 $A\in H$ 且 $\varphi(A)=y$. 因此 φ 是满射. φ 显然是单射, 从而是一一对应.

如果 $\left(\begin{smallmatrix}x'\\ y'\end{smallmatrix}\right)=A\left(\begin{smallmatrix}x\\ y\end{smallmatrix}\right)$, 则 $x'/y'=\varphi(A)(x/y)$. 因此设 $\left(\begin{smallmatrix}x_1\\ y_1\end{smallmatrix}\right)=A\left(\begin{smallmatrix}x\\ 1\end{smallmatrix}\right), \left(\begin{smallmatrix}x_2\\ y_2\end{smallmatrix}\right)=B\left(\begin{smallmatrix}x_1\\ y_1\end{smallmatrix}\right)$, 则 $\varphi(A)(x)=x_1/y_1$,

$$\varphi(B)(\varphi(A)(x))=\varphi(B)(x_1/y_1)=x_2/y_2=\varphi(BA)(x),$$

因此 φ 保持两边的二元运算. 由于 H 是群, 因此 G 是群.

2.4. (3) 由于

$$\left(\begin{smallmatrix}a_1 & b_1\\ 0 & c_1\end{smallmatrix}\right)\left(\begin{smallmatrix}a_2 & b_2\\ 0 & c_2\end{smallmatrix}\right)^{-1}=\left(\begin{smallmatrix}a_1a_2^{-1} & (a_2b_1-a_1b_2)a_2^{-1}c_2^{-1}\\ 0 & c_1c_2^{-1}\end{smallmatrix}\right),$$

因此该集合是 $\mathrm{GL}_2(\mathbb{R})$ 的子群.

2.5. 设 $x\in\mu_n, y\in\mu_m$, 则

$$(xy^{-1})^{mn}=(x^n)^m(y^m)^{-n}=1^{m-n}=1.$$

因此 $xy^{-1}\in\mu_{mn}$, $\cup_{n\geq 1}\mu_n$ 是 $\mathbb{C}^\times$ 的子群.

2.10. 设 $a_1,b_1,a_2,b_2\in\mathbb{Z}$, 则

$$(a_1+b_1\sqrt{2})-(a_2+b_2\sqrt{2})=(a_1-a_2)+(b_1-b_2)\sqrt{2}\in\mathbb{Z}(\sqrt{2}),$$

因此 $\mathbb{Z}(\sqrt{2})$ 是 $\mathbb{R}$ 的加法子群.

又因为 $1\in\mathbb{Z}(\sqrt{2})$,

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}\in\mathbb{Z}(\sqrt{2}),$$

因此 $\mathbb{Z}(\sqrt{2})$ 是 $\mathbb{R}$ 的子环.

注: 将 $\sqrt{2}$ 改成 $\sqrt{d}$ 也构成环, 其中 $d\in\mathbb{Z}$.

2.8. 设 $a_1, b_1, a_2, b_2 \in \mathbb{Q}$, 则

$$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

因此 $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{R}$ 的加法子群.

又因为 $1 \in \mathbb{Q}(\sqrt{2})$, 且若 $a_2 + b_2\sqrt{2} \neq 0$,

$$\frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = \frac{(a_1a_2 - 2b_1b_2) + (-a_1b_2 + a_2b_1)\sqrt{2}}{a_2^2 - 2b_2^2} \in \mathbb{Q}(\sqrt{2}),$$

因此 $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{R}$ 的子域.

注: 将 $\sqrt{2}$ 改成 $\sqrt{d}$ 也构成域, 其中 $d \in \mathbb{Q}$.

2.17. (1) 令 $R = \{\frac{x+y\sqrt{-3}}{2} \mid x, y \in \mathbb{Z}, x + y \text{ 是偶数}\}$, 则

$$\frac{x_1 + y_1\sqrt{-3}}{2} - \frac{x_2 + y_2\sqrt{-3}}{2} = \frac{(x_1 - x_2) + (y_1 - y_2)\sqrt{-3}}{2},$$

且 $(x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2)$ 是偶数. 因此 R 是 $\mathbb{C}$ 的加法子群. $1 = \frac{2+0\sqrt{-3}}{2} \in G$.

$$\frac{x_1 + y_1\sqrt{-3}}{2} \cdot \frac{x_2 + y_2\sqrt{-3}}{2} = \frac{x_1x_2 - 3y_1y_2}{4} + \frac{x_1y_2 + x_2y_1}{4}\sqrt{-3},$$

而

$$x_1x_2 - 3y_1y_2 = (x_1 + y_1)x_2 - y_1(x_2 + y_2) - 2y_1y_2,$$
$$x_1y_2 + x_2y_1 = (x_1 + y_1)y_2 - y_1(x_2 + y_2)$$

都是偶数, 因此 $\frac{x_1x_2-3y_1y_2}{2}, \frac{x_1y_2+x_2y_1}{2} \in \mathbb{Z}$.

又

$$\frac{x_1x_2 - 3y_1y_2}{4} + \frac{x_1y_2 + x_2y_1}{4} = \frac{x_1 + y_1}{2} \cdot \frac{x_2 + y_2}{2} - y_1y_2 \in \mathbb{Z},$$

因此 $\frac{x_1x_2-3y_1y_2}{4} + \frac{x_1y_2+x_2y_1}{4}\sqrt{-3} \in R$. 从而 R 是 $\mathbb{C}$ 的子环.

(2) 令该集合为 S, 其余略.

(3) 令

$$\varphi : R \to S, \varphi(\frac{x + y\sqrt{-3}}{2}) = \frac{1}{2}\begin{pmatrix} x_1 & y_1 \\ -3y_1 & x_1 \end{pmatrix}.$$

验证单射/满射/同态即可.

实际上, $R = \mathbb{Z} + \mathbb{Z}\alpha = \mathbb{Z}[\alpha], \alpha = \frac{1+\sqrt{-3}}{2}$. 同理, 对于任意无平方因子非零整数 $d \equiv 1 \bmod 4$, 均有环 $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ (习题).

2.18. 记该集合为 R, 容易看出这个集合关于加法构成阿贝尔群. 又因为 $1 \in R$, 且

$$\begin{aligned}
&\sum_{k=m_1}^{n_1} (a_k \cos kx + b_k \sin lx) \sum_{l=m_2}^{n_2} (a'_l \cos lx + b'_l \sin lx) \\
&= \sum_{k=m_1}^{n_1} \sum_{l=m_2}^{n_2} (a_ka'_l \cos kx \cos lx + a_kb'_l \cos kx \sin lx \\
&\qquad + b_ka'_l \sin kx \cos lx + b_kb'_l \sin kx \sin lx).
\end{aligned}$$

由于

$$\cos kx \cos lx = (\cos(k + l)x + \cos(k - l)x)/2$$
$$\cos kx \sin lx = (\sin(k + l)x - \sin(k - l)x)/2$$
$$\sin kx \sin lx = (-\cos(k + l)x + \cos(k - l)x)/2$$

因此该式最终可以化成 $\sin tx$ 和 $\cos tx$ 的线性组合, 也就是说, R 关于乘法封闭, 构成实函数整体环的子环.

2.7′. 设 A 是集合, 则 $(P(A), \triangle, \cap)$ 是环. 若 A 为 n 元有限集, 则该环同构于 $\mathbb{F}_2^n$.
留作练习.

2.4. 判断一个命题是错的, 只需要举出反例即可.
(1) 由于 $\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)=\left(\begin{smallmatrix}0&1\\2&0\end{smallmatrix}\right)$, 因此该集合关于乘法不封闭, 不构成群.
(2) 由于 $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, 因此该集合关于乘法不封闭, 不构成群.
(3) 由于上三角方阵关于乘法封闭, 可逆矩阵的乘积还是可逆矩阵, 因此该集合关于乘法和矩阵的逆封闭, 因此构成 $\mathrm{GL}_2(\mathbb{R})$ 的子群.
(4) 由于 $\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)$ 在这个集合中没有逆, 因此该集合不构成群.

2.2. 设 $f:\mathbb{R}^2\to\mathbb{R}^2$ 为平面上的保距映射. 若 $f(x)=f(y)$, 则 $d(x,y)=d(f(x),f(y))=0, x=y$, 因此 f 是单射. 这里 $d(x,y)$ 表示 x 与 y 的距离.
任取平面上两个不同的点 A 和 B, 则 $f(A)\neq f(B)$. 对于平面上任意一点 D,

$$d(D,f(A))+d(D,f(B))\geq d(f(A),f(B))=d(A,B)\geq|d(D,f(A))-d(D,f(B))|,$$

因此以 A 和 B为圆心, $d(D,f(A))$ 和 $d(D,f(B))$ 为半径的两个圆相交于 $E=E_1,E_2$ 或相切于 E. 这些切点或交点的像 E' 满足 $d(E',f(A))=d(E,A)=d(D,f(A)), d(E',f(B))=d(D,f(B))$, 因此要么 $E'=D$, 要么 E' 为 D 关于 AB 的对称点 D', 总之 $f(\{E_1,E_2\})\subset\{D,D'\}$ 或 $f(E)=D$. 若是第一种情形, 由于 f 是单射, 因此 $f(E_1)$ 或 $f(E_2)=D$. 故 f 是满射. 显然保距映射的复合还是保距映射. 由于映射满足结合律, 因此保距映射也满足结合律. 单位元为恒等映射. 保距映射 f 的逆映射 f^{-1} 也保距. 因此所有保距映射在复合意义下构成群.

5. 算术基本定理

算术基本定理的存在保证了利用素数分解来计算诸如公因子、公倍数、因子的相关计算.

3.4. (1) 设 $a=\prod\limits_p p^{v_p(a)}, b=\prod\limits_p p^{v_p(b)}$, 则

$$\begin{aligned}v_p((a^n,b^n))&=\min\{nv_p(a),nv_p(b)\}=n\min\{v_p(a),v_p(b)\}\\&=nv_p((a,b))=v_p((a,b)^n),\end{aligned}$$

因此 $(a^n,b^n)=(a,b)^n$.
(2) 设 $a=\prod\limits_{p\in S} p^{v_p(a)}, b=\prod\limits_{q\in T} q^{v_q(b)}$, 且 $S\cap T=\emptyset$.

$$c^n=ab=\prod_{p\in S}p^{v_p(a)}\prod_{q\in T}q^{v_q(b)},$$

因此 $v_p(a)$ 和 $v_q(b)$ 是 n 的倍数, 故 a,b 都是正整数的 n 次方幂. 设 $a=s^n, b=t^n, s,t>0$, 则 $(s,t)=1, st=c$,

$$a=s^n=(a,c)^n,\quad b=t^n=(b,c)^n.$$

一般地, 若 $a_1,\dots,a_k$ 两两互素且 $\prod\limits_{j=1}^{k}a_j=c^n$, 则对任意 $1\leq i\leq k$, a_i 与 $\prod\limits_{j\neq i}a_j$ 互素, 因此 a_i 是 n 次方幂.

3.12. (1) 设 $n=\prod\limits_p p^{v_p(n)}$, 则 $\sigma_0(n)=\prod\limits_p(1+v_p(n))$. 因此 n 是完全平方数等价于 $v_p(n)$ 全是偶数, 即 $\sigma_0(n)$ 是奇数.

(2) 对任意素数 p, 我们考虑 $f(v)=\frac{\sqrt{p}^v}{v+1}$ 的最小值, 其中 v 是自然数. 由于

$$f(v)\le f(v-1)\iff \frac{\sqrt{p}^v}{v+1}\le\frac{\sqrt{p}^{v-1}}{v}\iff v\le\frac{1}{\sqrt{p}-1},$$

$$f(v)\le f(v+1)\iff \frac{1}{\sqrt{p}-1}\le v+1,$$

因此

$$\min_{v\in\mathbb{N}} f(v)=f([\frac{1}{\sqrt{p}-1}])=\begin{cases} f(2)=\frac{2}{3}, & \text{若 } p=2;\\ f(1)=\frac{\sqrt{3}}{2}, & \text{若 } p=3;\\ f(0)=1, & \text{若 } p\ge 5,\end{cases}$$

这里 [ ] 表示取整.

故

$$\frac{\sqrt{n}}{\sigma_0(n)}=\prod_p\frac{\sqrt{p}^{v_p(n)}}{v_p(n)+1}\ge\frac{2}{3}\times\frac{\sqrt{3}}{2}=\frac{1}{\sqrt{3}},$$

$$\sigma_0(n)\le\sqrt{3n}\le 2\sqrt{n}+1.$$

实际上, 我们用这种方法得到了 $\frac{\sqrt{n}}{\sigma_0(n)}$ 的最佳估计.

习题: 尝试给出 $\frac{n^{1/3}}{\sigma_0(n)}$ 的最佳估计.

(3)

$$\begin{aligned}\prod_{0<d|n} d&=\prod_p(\prod_{i=0}^{v_p(n)}p^i)^{\frac{\sigma_0(n)}{v_p(n)+1}}\\&=\prod_p p^{\frac{\sigma_0(n)v_p(n)}{2}}\\&=n^{\frac{\sigma_0(n)}{2}}.\end{aligned}$$

这道题也有其它解法.

$$\begin{aligned}\sigma_0(n)&=\sum_{0<d|n}1\\&=\sum_{0<d|n,d<\sqrt{n}}1+\sum_{\sqrt{n}<d|n}1+\sum_{\sqrt{n}|n}1\\&=\sum_{0<d|n,d<\sqrt{n}}1+\sum_{0<\frac{n}{d}|n,\frac{n}{d}<\sqrt{n}}1+\sum_{\sqrt{n}|n}1\\&=2\sum_{0<d|n,d<\sqrt{n}}1+\sum_{\sqrt{n}|n}1\\&\le 2\sqrt{n}+1,\end{aligned}$$

且 $\sigma_0(n)$ 是奇数等价于 $\sqrt{n}\mid n$, 即 n 是完全平方数.

$$(\prod_{0<d|n}d)^2=\prod_{0<d|n}d\prod_{0<\frac{n}{d}|n}d=\prod_{0<d|n}d\prod_{0<d|n}\frac{n}{d}=\prod_{0<d|n}n=n^{\sigma_0(n)},$$

故 n 的正约数之积等于 $n^{\frac{\sigma_0(n)}{2}}$.

6. 线性不定方程与同余方程

线性同余方程本质上用到的理论是Bezout等式、中国剩余定理、欧拉定理、费马小定理, 也经常用到欧几里得算法（辗转相除法）.

3.6. 由Bezout等式, 存在整数 x_0, y_0 满足 $ax_0 + by_0 = (a, b) = 1$, 于是 (nx_0, ny_0) 是 $ax + by = n$ 的一组特解, 通解为 $(nx_0 - bt, ny_0 + at), t \in \mathbb{Z}$. 设有带余除法 $nx_0 = bq + r, 0 \leq r \leq b - 1$, 令 $s = ny_0 + aq$, 则 $ar + bs = n$, 且

$$s = \frac{n - ar}{b} > \frac{ab - a - b - a(b-1)}{b} = -1,$$

故 $s \geq 0$, (r, s) 是 $ax + by = n$ 的一组非负整数解.

若 $n = ab-a-b = a(b-1)-b$, 则 $ax+by = n$ 的通解为 $(b-1-bt, -1+at), t \in \mathbb{Z}$. 若该解非负, 则 $1 > \frac{b-1}{b} \geq t \geq \frac{1}{a} > 0$, 这不可能, 因此 $ax + by = n$ 无非负整数解.

4.8(2).

$$60 = 37 + 23,\ 37 = 23 + 14,\ 23 = 14 + 9,\ 14 = 9 + 5,\ 9 = 5 + 4,\ 5 = 4 + 1,$$

$$\begin{aligned} 1 &= 5 - 4 = 5 - (9 - 5) = 2 \times 5 - 9 = 2 \times (14 - 9) - 9 = 2 \times 14 - 3 \times 9 \\ &= 2 \times 14 - 3 \times (23 - 14) = 5 \times 14 - 3 \times 23 = 5 \times (37 - 23) - 3 \times 23 \\ &= 5 \times 37 - 8 \times 23 = 5 \times 37 - 8 \times (60 - 37) = 13 \times 37 - 8 \times 60, \end{aligned}$$

$$x \equiv -8 \times 60x \equiv -8 \times 7 \equiv 18 \pmod{37}.$$

或者

$$x \equiv \frac{7}{60} \equiv \frac{7}{-14} \equiv \frac{1}{-2} \equiv \frac{-36}{-2} \equiv 18 \pmod{37}.$$

7. 整数互素

3.2. $(n+1)!+1 = (n+1)(n!+1)-n, n!+1 = n\times(n-1)!+1$, 因此 $((n+1)!+1, n!+1) = 1$.

3.3. 设 $d = (2^m - 1, 2^n + 1)$, 则

$$\begin{aligned} 2^{mn} &\equiv (2^m)^n \equiv 1 \\ &\equiv (2^n)^m \equiv (-1)^m \equiv -1 \pmod{d}, \end{aligned}$$

从而 $d \mid 2$, 但是 $2^m - 1$ 是奇数, 因此 $d = 1$.

另证: 首先利用辗转相除法证明 $(2^x - 1, 2^y - 1) = 2^{(x,y)} - 1$, 于是

$$\begin{aligned} (2^m - 1, 2^n + 1)(2^m - 1, 2^n - 1) &= (2^m - 1, 2^{2n} - 1) = 2^{(m,2n)} - 1 \\ &= 2^{(m,n)} - 1 = (2^m - 1, 2^n - 1), \end{aligned}$$

因此 $(2^m - 1, 2^n + 1) = 1$.

3.9. (1) 若 m 不为 2 的方幂, 则存在大于1的奇数 $d \mid m$, 于是 $2^{m/d}+1$ 是 2^m+1 的真因子, 从而 2^m+1 不是素数.

(2) 由于 $F_m - 2 = 2^{2^m} - 1 = (2^{2^{m-1}}+1)(2^{2^{m-1}}-1) = F_{m-1}(F_{m-1}-2)$, 因此

$$F_m - 2 = (F_n - 2)\prod_{k=n}^{m} F_k,$$

$F_n \mid F_m - 2$.

(3) $(F_m, F_n) = (F_m - (F_m - 2), F_n) = (2, F_n) = 1$.

3.10. 类似于习题3.9.

3.8. 由于 $n!-1$ 和 $1, 2, \ldots, n$ 互素, 因此存在素数 $p \mid n!-1$, 且 $n < p < n!$, 命题得证.

这里的 $n!-1$ 可以换成 $p_1 \cdots p_k - 1$, 其中 $p_1, \ldots, p_k$ 为 $1, \ldots, n$ 中的所有素数. 如同证明素数个数无限中将 $p_1 \cdots p_n + 1$ 换成 $p_n! + 1$ 一样.

若素数个数有限, 设最大的为 n, 则 n 与 $n!-1$ 之间存在素数, 矛盾! 因此素数个数无限.

或者由 $3, 3!, (3!)!, ((3!)!)!, \ldots$ 两两之间存在素数知素数个数无限.

8. 整数的同余性质

利用同余的符号我们可以迅速得到一批计算整数的余数的方法.

4.2. 设 $n = \sum_{i=0}^{k} a_i \times 10^i$, $0 \le a_i \le 9$, 则

$$T(n) = \sum_{i=0}^{k} a_i \times (-1)^i \equiv \sum_{i=0}^{k} a_i \times 10^i = n \pmod{11}.$$

类似地, 我们很容易得到

$$n \equiv \sum_{i=0}^{k} a_i \pmod{9},$$

$$n \equiv a_0 \pmod{2} \text{ 或 } \pmod{5},$$

$$n \equiv \overline{a_2a_1a_0} - \overline{a_5a_4a_3} + \overline{a_8a_7a_6} - \overline{a_{11}a_{10}a_9} + \cdots \pmod{7 \times 11 \times 13}.$$

4.4. (1)

$$n^2 \equiv 0^2, (\pm 1)^2 \equiv 0, 1 \pmod{3},$$

$$(2k)^2 \equiv 0 \pmod{4}, \quad (4k \pm 1)^2 \equiv 1 \pmod{4},$$

$$n^2 \equiv 0^2, (\pm 1)^2, (\pm 2)^2 \equiv 0, \pm 1 \pmod{5}.$$

(2)

$$(3k)^3 \equiv 0 \pmod{9}, \quad (3k \pm 1)^3 = 27k^3 \pm 27k^2 + 9k \pm 1 \equiv \pm 1 \pmod{9},$$

$$(2k)^4 = 16k^4 \equiv 0 \pmod{16}, \quad (4k \pm 1)^4 \equiv \pm 4 \times 4k + 1 \equiv 1 \pmod{16}.$$

4.5. (1) 数学归纳法. $n=1$ 时, 设 $a=4k\pm1$, $a^2=(4k\pm1)^2=16k^2\pm8k+1\equiv1 \pmod 8$. 若 $a^{2^n}\equiv1 \pmod{2^{n+2}}$, 设 $a^{2^n}=1+2^{n+2}k$, 则

$$a^{2^{n+1}}=(1+2^{n+2}k)^2=1+2^{n+3}k+2^{2n+4}k^2\equiv1 \pmod{2^{n+3}}.$$

因此由数学归纳法知原命题成立.

(2) 由于

$$a^{2^n}-1=(a-1)\prod_{k=0}^{n-1}\frac{a^{2^{k+1}}-1}{a^{2^k}-1}=(a-1)\prod_{k=0}^{n-1}(a^{2^k}+1).$$

由于 $a-1$ 和 $a^{2^k}+1$ 都是偶数, 且 $a-1$ 和 $a+1$ 有一个是4的倍数, 因此右边是 2^{n+2} 的倍数, 即 $a^{2^n}\equiv1 \pmod{2^{n+2}}$.

9. 欧拉函数

欧拉定理决定了欧拉函数在同余中的重要作用.

4.6. (1) 设 $1\le a\le n-1$. 如果 $(a,n)=1$, 则 $(n-a,n)=(-a,n)=(a,n)=1$. 令

$$A=\{a\mid 1\le a<\frac{n}{2},(a,n)=1\},$$
$$B=\{a\mid \frac{n}{2}<a\le n,(a,n)=1\}=\{n-a\mid a\in A\},$$
$$C=\{a\mid a=\frac{n}{2},(a,n)=1\},$$

则

$$\varphi(n)=|A|+|B|+|C|=2|A|+|C|.$$

若 C 非空, 则 n 是偶数, 且 $1=(\frac{n}{2},n)=\frac{n}{2}$, $n=2$, 与 $n\ge3$ 矛盾. 因此 $C=\emptyset$, $\varphi(n)$ 是偶数. 或者: 若 n 有奇素因子 p, 且 $p^\alpha||n$. 设 $n=p^\alpha m$, 则

$$\varphi(n)=\varphi(p^\alpha)\varphi(m)=p^{\alpha-1}(p-1)\varphi(m).$$

由于 $p-1$ 是偶数, 因此 $\varphi(n)$ 是偶数. 若 n 没有奇素因子, 则 $n=2^k,k\ge2,\varphi(n)=2^{k-1}$ 是偶数.

(2) 此即

$$\sum_{a\in A\cup B}a=\sum_{a\in A}a+\sum_{a\in A}(n-a)=\sum_{a\in A}n=n|A|=\frac{1}{2}n\varphi(n).$$

4.12.

$$\varphi(360)=\varphi(2^3\times3^2\times5)=2^2\times3\times(3-1)\times(5-1)=96.$$
$$\varphi(429)=\varphi(3\times11\times13)=(3-1)(11-1)(13-1)=240.$$

4.13. 由于 $\varphi(100)=\varphi(2^2\times5^2)=2\times5\times(5-1)=40$, 由欧拉定理 $3^{40}\equiv1 \pmod{100}$, 因此 $3^{400}\equiv1 \pmod{100}$. 实际上由于 $\varphi(25)=20,\varphi(4)=2$, 因此对任意 $(a,10)=1,a^{20}\equiv1 \pmod{25}$ 且 $a^{20}\equiv1 \pmod4$, 故 $a^{20}\equiv1 \pmod{100}$. 此即习题4.15.

4.14. 由于

$$m^{\varphi(n)}\equiv1 \pmod n,\quad n^{\varphi(m)}\equiv1 \pmod m,$$

因此

$$m^{\varphi(n)}+n^{\varphi(m)}\equiv1 \pmod n,\quad m^{\varphi(n)}+n^{\varphi(m)}\equiv1 \pmod m,$$

从而

$$m^{\varphi(n)}+n^{\varphi(m)}\equiv1 \pmod{mn}.$$

10. 多项式的欧式算法

5.2(2).

$$\begin{aligned} x^7+1 &= (x^6+x^5+x^4+1)(x+1)+x^4+x,\\ x^6+x^5+x^4+1 &= (x^4+x)(x^2+x+1)+x^3+x^2+x+1,\\ x^4+x &= (x^3+x^2+x+1)(x+1)+x+1,\\ x^3+x^2+x+1 &= (x+1)(x^2+1), \end{aligned}$$

因此 $(f,g)=x+1$. 实际计算时, 可以在草稿纸上利用类似计算除法的长除式来计算多项式相除.

5.5(2). 我们想要寻找 $v(x)$, 使得 $v(x)(1-x)^n-1$ 是 x^m 的倍数, 因此我们可以取得 $v(x)(1-x)^n$ 是 x^m 的多项式, 而且是 $(1-x)^n$ 的倍数, 例如取 $(1-x^m)^n$. 设 $v_0(x)=\frac{(1-x^m)^n}{1-x^n}\in\mathbb{Q}[x]$, 则

$$u_0(x)=-\frac{(1-x^m)^n-1}{x^m}=\sum_{i=0}^{n-1}\binom{n}{i+1}(-x^m)^i\in\mathbb{Q}[x].$$

因此 (u_0,v_0) 是原方程的一组特解, 通解为

$$\begin{cases} u(x)=(1-x)^nf(x)+\displaystyle\sum_{i=0}^{n-1}\binom{n}{i+1}(-x^m)^i\\ v(x)=-x^mf(x)+\dfrac{(1-x^m)^n}{1-x^n}, \end{cases} \qquad f(x)\in\mathbb{Q}[x].$$

11. 零点与重数

5.8. 由于 $f'(x)=\sum_{k=0}^{n-1}\frac{x^k}{k!}$,

$$(f(x),f'(x))=(\sum_{k=0}^{n}\frac{x^k}{k!},\sum_{k=0}^{n-1}\frac{x^k}{k!})=(x^k,\sum_{k=0}^{n-1}\frac{x^k}{k!})=1,$$

因此 $f(x)$ 无重根.

5.9. 令 $f(x)=x^{2n}-nx^{n+1}+nx^{n-1}-1$, 则

$$\begin{aligned} f(1) &= 1-n+n-1=0,\\ f'(1) &= 2nx^{2n-1}-n(n+1)x^n+n(n-1)x^{n-2}|_{x=1}\\ &= 2n-n(n+1)+n(n-1)=0,\\ f''(1) &= 2n(2n-1)x^{2n-2}-n^2(n+1)x^{n-1}+n(n-1)(n-2)x^{n-3}|_{x=1}\\ &= 2n(2n-1)-n^2(n+1)+n(n-1)(n-2)=0,\\ f'''(1) &= 2n(2n-1)(2n-2)x^{2n-3}-n^2(n+1)(n-1)x^{n-2}\\ &\quad +n(n-1)(n-2)(n-3)x^{n-4}|_{x=1}\\ &= 2n(n^2-1)\neq 0, \end{aligned}$$

因此 1 是 f 的3重零点.

5.10. 由于域上 2,3 次多项式不可约当且仅当它在域上没有零点, 因此我们设 $f(x)=x^2+ax+b\in\mathbb{F}_2[x]$ 不可约, 则

$$f(0)=b\neq 0, f(1)=1+a+b\neq 0,$$

于是 $b=1, a=1, f(x)=x^2+x+1$. 类似地, 设 $f(x)=x^3+ax^2+bx+c\in\mathbb{F}_2[x]$ 不可约, 则

$$f(0)=c\neq 0, f(1)=1+a+b+c\neq 0,$$

于是 $c=1, a\neq b$, $f(x)=x^3+x^2+1, x^3+x+1$. 同理, 域 $\mathbb{F}_3$ 上面的2,3次首一不可约多项式为

$$x^2+1,\ x^2\pm x-1,$$

$$x^3-x\pm(x^2+1),\ x^3-x\pm 1,$$

$$x^3+x\pm(x^2-1),\ x^3\pm(x^2-1).$$

5.12. 设 $g(x)=xf(x)-1$, 则 $\deg g=p-1$ 且 $g(1)=g(2)=\cdots=g(p-1)=0, g(0)=-1$, 因此

$$g(x)=a\prod_{i=1}^{p-1}(x-i)=a(x^{p-1}-1),$$

$$-1=g(0)=-a,$$

于是 $a=1, g(x)=x^{p-1}-1, f(x)=x^{p-2}$.

12. 群中元素的阶

6.1. 计算可知

$$A^2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}, A^4=I,$$

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

因此 A, B 的阶分别为 $4, 3$. 由于 $AB=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, 归纳可知

$$(AB)^n=\begin{pmatrix}1&n\\0&1\end{pmatrix},$$

因此 AB 的阶为无穷大. 由于 $BA=\begin{pmatrix}1&0\\-1&1\end{pmatrix}$, 归纳可知

$$(BA)^n=\begin{pmatrix}1&0\\-n&1\end{pmatrix},$$

因此 BA 的阶为无穷大.

6.4. 设 x^k 的阶为 d, 则 $x^{kd}=1$, 因此

$$n\mid kd, [n,k]\mid kd, \frac{[n,k]}{k}\mid d.$$

另一方面, $(x^k)^{\frac{[n,k]}{k}}=x^{[n,k]}=1$, 因此 $d=\frac{[n,k]}{k}$.

6.12. 由于

$$a^k = 1 \iff a^{-k} = 1 \iff (a^{-1})^k = 1,$$

因此 a 与 a^{-1} 的阶相同. 由于

$$(ab)^k = 1 \iff a(ba)^{k-1}b = 1 \iff ba(ba)^{k-1} = 1 \iff (ba)^k = 1,$$

因此 ab 与 ba 的阶相同.

6.8. 首先我们证明, 如果 $(I+pX)^q = I$, 那么 $X = 0$, 其中 q 是一个素数. 假如 $X \neq 0$. 设 X 的分量是 p^{t-1} 的倍数但不全是 p^t 的倍数, 那么存在 $Z \in M_2(\mathbb{Z}), X = p^{t-1}Z$. 如果 $p = q$,

$$I = (I+pX)^p = (I+p^tZ)^p = I + p^{t+1}Z + \sum_{i=2}^{p} \binom{p}{i} (p^tZ)^i = I + p^{t+1}Z + p^{t+2}Y,$$

其中 $Y \in M_2(\mathbb{Z})$; 如果 $p \neq q$,

$$I = (I+pX)^q = (I+p^tZ)^q = I + qp^tZ + \sum_{i=2}^{q} \binom{q}{i} (p^tZ)^i = I + qp^tZ + p^{t+1}Y,$$

其中 $Y \in M_2(\mathbb{Z})$, 因此总有 Z 的分量都是 p 的倍数, 这不可能! 所以 $X = 0$. 回到原题, 由于 $I+pX$ 的任意整数次方都是 $I+pY$ 的形式, 因此若 $I+pX$ 的阶为 $d > 1$, 那么存在素数 $q \mid d$, 于是

$$((I+pX)^{\frac{d}{q}})^q = I \implies (I+pX)^{\frac{d}{q}} = I,$$

这与 d 的最小性矛盾! 因此 $I+pX = I, X = 0$.

这题也可以用特征多项式来做. 由于

$$\det(I+pX) = I + p\mathrm{Tr}X + p^2 \det(X),$$

因此 $p \mid \mathrm{Tr}X$, $p^2 \mid (\mathrm{Tr}(I+pX) - 2)$. 由于 $I+pX$ 阶有限, 它的特征值是单位根 $\alpha, \bar{\alpha}$, 对应的多项式为 $\lambda^2 - 2\mathrm{Re}(\alpha)\lambda + 1 = 0$, 于是

$$-2 \leq \mathrm{Re}(\alpha) \leq 2, \quad -4 \leq \mathrm{Tr}(I+pX) - 2 \leq 0,$$

而 $p^2 \mid (\mathrm{Tr}(I+pX) - 2)$, 因此 $\mathrm{Tr}(I+pX) = 2$, $\alpha = 1$, $I+pX = I$.

6.18. (1) 显然 $d(G)$ 是 G 中所有元素的阶的倍数, 因此是它们阶的最小公倍数 d 的倍数. 而 $g^d = 1, \forall g \in G$. 因此 $d(G) = d$, $d(G) \mid |G|$.

(2) 设 $d(G) = \prod_{i=1}^{t} p_i^{k_i}$, 那么由最小公倍数的定义, 存在元素 x_i, 它的阶包含因子 $p_i^{k_i}$, 于是 x_i 的某个次方 y_i 的阶恰好为 $p_i^{k_i}$. 对于 G 中两个元素 a, b, 他们的阶 m, n 互素, 那么 $1 = (ab)^k = a^k b^k$ 当且仅当

$$a^k = b^{-k}, a^{kn} = b^{kn} = 1, b^{km} = a^{km} = 1, m \mid k, n \mid k, mn \mid k,$$

因此 ab 的阶为 mn. 于是 $y_1 \cdots y_t$ 的阶为 $d(G)$.

(3) 由(1)知如果 G 是循环群, 存在 $g \in G$ 的阶为 $|G|$, 于是 $d(G) = |G|$. 由(2)知如果 $d(G) = |G|$, 那么存在元素 $g \in G$ 的阶为 $|G|$, 于是 G 是循环群.

13. 有限群元素之积

6.5. 设 $A = \{a \in G \mid a^2 = 1\}$, $B = G - A$, 则对任意 $b \in B$, $b \neq b^{-1}$, 因此 B 可以分拆为一些 $\{b_i, b_i^{-1}\}$ 的无交并. 于是

$$\prod_{g \in G} g = \prod_{a \in A} a \prod_i b_i \cdot b_i^{-1} = \prod_{a \in G, a^2 = 1} a.$$

6.6. (1) 设 $x^2 \equiv 1 \bmod p^k$, 则 $p^k \mid (x+1)(x-1)$, 由于 $(x+1, x-1) = (x+1, 2) \mid 2$, 所以 $p^k \mid x+1$ 或 $x-1$, $x \equiv \pm 1 \bmod p$. 因此 $(\mathbb{Z}/p^k\mathbb{Z})^\times$ 只有一个2阶元 -1.

(2) 由习题6.5和(1)立得.

(3) 在(2)中取 $k=1$ 即可.

6.7. (1) 设 $m = \prod_{i=1}^{k} p_i^{v_i}$. 如果 $x^2 \equiv 1 \bmod m$, 则

$$x^2 \equiv 1 \bmod p_i^{v_i}, \quad x \equiv \pm 1 \bmod p_i^{v_i}.$$

对于每个 i, 选择 $+1$ 或 -1 有两种取法, 一共有 2^k 中取法, 分别对应 $x \bmod m$ 的 2^k 个不同的解. 因此 $(\mathbb{Z}/m\mathbb{Z})^\times$ 有 $2^k - 1$ 个2 阶元.

(2) 设 $x \in \mathbb{Z}$ 使得 $x \bmod m$ 为所有2阶元之积, 则

$$x \equiv (-1)^{2^{k-1}} \equiv 1 \bmod p_i^{v_i},$$

因此 $x \equiv 1 \bmod m$, 即所有2阶元之积为1.

或者: 若 $x^2 = 1$, 则 $(-x)^2 = 1$, 且由于 m 是奇数, $x \neq -x$. 于是所有2阶元之积为

$$\prod_x x \times (-x) = (-1)^{2^{k-1}} = 1.$$

14. 有限生成

6.15. 假设 $\mathbb{Q}$ 由有限个 $\frac{p_i}{q_i}, 1 \le i \le k$ 生成. 设 $M = q_1 \cdots q_k$, 则 $M\frac{p_i}{q_i} \in \mathbb{Z}$, 于是它们生成的元素 x 也满足 $Mx \in \mathbb{Z}$, 但是如果

$$\frac{1}{2M} = \sum_{i=1}^{k} \lambda_i \frac{p_i}{q_i},$$

$$\frac{1}{2} = \sum_{i=1}^{k} \lambda_i \frac{p_i M}{q_i} \in \mathbb{Z},$$

矛盾! 因此 $\mathbb{Q}$ 不是有限生成的.

6.16. 设 G 是 S^1 的一个 n 阶子群, 则对任意 $g \in G$, $g^n = 1$, 于是 $G \leqslant \mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$. 但是 μ_n 的大小也是 n, 因此 $G = \mu_n = \langle e^{\frac{2\pi i}{n}} \rangle$ 是循环群.

15. 置换群和交错群

7.1. 因为置换可以看成是一个有限集合上的映射, 所以作用的时候是从右往左的.

$$\sigma = (456)(567)(71) = (16)(45).$$

7.3. $\sigma = (23)(412) = (1324)$, $\sigma(f)(x_1, x_2, x_3, x_4) = f(x_3, x_4, x_2, x_1)$.

7.4. 设 $G \leqslant S_3$, 则 $|G| \mid |S_3| = 6$, $|G| = 1, 2, 3, 6$.

(1) 如果 $|G| = 1$, $G = \{1\}$; 如果 $|G| = 6, G = S_3$.

(2) 如果 $|G| = 2$, $G = \{1, (12)\}, \{1, (13)\}, \{1, (23)\}$.

(3) 如果 $|G| = 3$, $G = \{1, (123), (132)\}$.

设 $G \leqslant A_4$, 则 $|G| \mid |A_4| = 12$, $|G| = 1, 2, 3, 4, 6, 12$.

(1) 如果 $|G| = 1$, $G = \{1\}$; 如果 $|G| = 12, G = A_4$.

(2) 如果 $|G| = 2$, $G = \{1, (12)(34)\}, \{1, (13)(24)\}, \{1, (14)(23)\}$.

(3) 如果 $|G| = 3$, $G = \langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$.

(4) 如果 $|G| = 4$, 由于 A_4 不含4阶元且恰有3个2阶元, 所以 $G = \{1, (12)(34), (13)(24), (14)(23)\}$.

(5) 如果 $|G| = 6$, 由于 A_4 包含3个2阶元和8个3阶元, 因此 G 一定包含3阶元. 但是如果 G 只含3阶元和1, 则 G 的阶为奇数, 矛盾! 因此 G 包含2阶元 σ 和3 阶元 τ. 如果 G 是交换群, 则 $\sigma\tau$ 是6阶元, 这与 A_4 不含6阶元矛盾! 因此 $G = \{1, \sigma, \tau, \sigma\tau, \tau^2, \sigma\tau^2\}$ 且 $\tau\sigma = \sigma\tau^2$. 于是 G 包含3个2阶元 $\sigma, \sigma\tau, \sigma\tau^2$, 即包含子群 $\{1, (12)(34), (13)(24), (14)(23)\}$, 但是这与 $4 \nmid 6$ 矛盾!.

7.2. σ 可以写成 $[\frac{n}{2}]$ 个不交的对换之积, 因此它的奇偶性和 $[\frac{n}{2}]$ 的奇偶性相同, 即 σ 是偶置换如果 $n \equiv 0, 1 \bmod 4$; σ 是奇置换如果 $n \equiv 2, 3 \bmod 4$.

7.12. 注意到 $\xi = (\sigma, 1) \times (1, \tau)$, 而 $(\sigma, 1)$ 可以写成 n 个型与 σ 相同的不交的置换乘积, $\varepsilon((\sigma, 1)) = \varepsilon(\sigma)^n$. 同理 $\varepsilon((1, \tau)) = \varepsilon(\tau)^m$, 因此 $\varepsilon(\xi) = \varepsilon(\sigma)^n\varepsilon(\tau)^m$.

7.8. 设 $\sigma = (123\cdots n)$, 则 $\sigma^k(12)\sigma^{-k} = (k+1, k+2), 1 \leq k \leq n-2$, 而

$$(23)(12)(23) = (13),$$

$$(34)(13)(34) = (14),$$

$$\vdots$$

$$(n-1, n)(1, n-1)(n-1, n) = (1n),$$

因此 $(12), \sigma$ 可以生成 $(1k), 2 \leq k \leq n$, 而后者生成 S_n, 故 $(12), \sigma$ 生成 S_n.

7.11. 由于 σ 可以写成不交的轮换之积, 因此我们只需对 σ 是轮换的情形证明即可. 我们可以先对较小阶的轮换证明, 然后尝试计算

$$(12)(34)(56)\cdots(k, k+1) \times (23)(45)\cdots(k-1, k)$$

发现它是个轮换, 调整数字之间的顺序, 我们得到如下的做法:

不妨设 $\sigma = (12\cdots k)$, 如果 $k = 2a+1$ 是奇数, 那么

$$\sigma = (2a+1, 1)(2a, 2)\cdots(a+3, a-1)(a+2, a) \times (1, 2a)(2, 2a-1)\cdots(a, a+1),$$

如果 $k = 2a$ 是偶数, 那么

$$\sigma = (2a, 1)(2a-1, 2)\cdots(a+2, a-1)(a+1, a) \times (1, 2a-1)(2, 2a-2)\cdots(a-1, a+1).$$

或者: 由于 $\sigma = \alpha\beta$, $\sigma^{-1} = \beta\alpha, \sigma = \alpha^{-1}\sigma^{-1}\alpha$, 而 σ^{-1} 和 σ 型相同, 因此如果 $\sigma = (12\cdots n)$, 我们可以构造 α 如同习题7.2一样.

7.9. 容易看出置换矩阵 A 把列向量 $(x_1,\ldots,x_n)^T$ 变成某个 $(x_{\sigma_A(1)},\ldots,x_{\sigma_A(n)})^T$. 于是 AB 把列向量 $(x_1,\ldots,x_n)^T$ 变成 $(x_{\sigma_A\sigma_B(1)},\ldots,x_{\sigma_A\sigma_B(n)})^T$. 令

$$\begin{aligned}\varphi : G &\to S_n\\ A &\mapsto \sigma_A\end{aligned}$$

则 $\varphi(AB)=\sigma_A\sigma_B=\varphi(A)\varphi(B)$, 且任意 σ 有原像为 $(k,\sigma(k))$ 分量为 1, $1\le k\le n$, 其余分量为 0 的置换矩阵. 因此 φ 是满射, 而 $|G|=n!=|S_n|$, 因此 φ 是保持运算的双射, 于是 G 是群且同构于 S_n.

7.6. 我们将这样的置换按照阶小的轮换放前面, 阶大的轮换放后面的顺序排好, 那么这个置换对应了一个 n-排列, 因此有 $n!$ 种. 但是相同型之间是可以任意交换的, 每个 k- 轮换也有 k 种不同的写法, 因此实际的个数为

$$\frac{n!}{\prod_{i=1}^n \lambda_i! i^{\lambda^i}}.$$

所有的置换个数之和为 $n!$, 因此

$$\sum \frac{n!}{\prod_{i=1}^n \lambda_i! i^{\lambda^i}} = n!,$$

$$\sum \frac{1}{\prod_{i=1}^n \lambda_i! i^{\lambda^i}} = 1.$$

16. 原根

原根就是 $\mathbb{F}_p^\times$ 作为循环群的生成元.

8.1. 设 a,b 是模 p 的原根, 则存在正整数 n 使得 $b=a^n$ 且 $(n,p-1)=1$. 于是 n 是奇数, $ab=a^{n+1}$, $2\mid(n+1,p-1)$, 因此 ab 不是原根.

或者: 由 $(a^{\frac{p-1}{2}})^2=1$ 知 $a^{\frac{p-1}{2}}=-1$, 同理 $b^{\frac{p-1}{2}}=-1$, $(ab)^{\frac{p-1}{2}}=1$, ab 不是原根.

8.6. 注意到 $q>3$,

$$(\pm 2)^2 \not\equiv 1 \bmod q,$$

$$(\pm 2)^{2p} \equiv 1 \bmod q,$$

(1) 由于 $q\equiv 3 \bmod 8$,

$$2^p = 2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) = -1 \bmod q,$$

因此 2 是模 q 的原根.

(2) 由于 $q\equiv 7 \bmod 8$,

$$(-2)^p = (-2)^{\frac{q-1}{2}} \equiv \left(\frac{-2}{q}\right) = -1 \bmod q,$$

因此 -2 是模 q 的原根.

8.12.

$$\left(\frac{17}{23}\right)=\left(\frac{23}{17}\right)=\left(\frac{6}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

$$\left(\frac{19}{37}\right)=\left(\frac{37}{19}\right)=\left(\frac{-1}{19}\right)=-1.$$

$$\left(\frac{60}{79}\right)=\left(\frac{3}{79}\right)\left(\frac{5}{79}\right)=\left(\frac{79}{3}\right)\left(\frac{79}{5}\right)=-\left(\frac{1}{3}\right)\left(\frac{4}{5}\right)=-1.$$

$$\left(\frac{92}{101}\right)=\left(\frac{23}{101}\right)=\left(\frac{101}{23}\right)=\left(\frac{9}{23}\right)=1.$$

8.7. (1) 由于 $\left(\frac{-1}{p}\right)=1$, 因此 $\left(\frac{r}{p}\right)=1$ 等价于 $\left(\frac{p-r}{p}\right)=1$, 于是

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r=\frac{1}{2}\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r+(p-r)=\frac{p(p-1)}{4}.$$

(2) 由 (1) 知

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right)=\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r-\sum_{r=1,\left(\frac{r}{p}\right)=-1}^{p-1} r=2\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r-\sum_{r=1}^{p-1} r=0.$$

(3)

$$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{k^2}{p}\right]=\sum_{k=1}^{\frac{p-1}{2}}\frac{k^2}{p}-\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1}\frac{r}{p}=\frac{1}{6p}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot p-\frac{p-1}{4}=\frac{(p-1)(p-5)}{24}.$$

8.8. (1)

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv\sum_{k=1}^{\frac{p-1}{2}} k^2=\frac{(p^2-1)p}{24}\equiv 0 \bmod p.$$

或者: 设 $\left(\frac{a}{p}\right)=-1$, 则

$$\sum_{r=1,\left(\frac{r}{p}\right)=-1}^{p-1} r\equiv a\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r \bmod p,$$

$$(a+1)\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv\sum_{r=1}^{p-1} r=\frac{p(p-1)}{2}\equiv 0 \bmod p.$$

由于 $p\equiv 3 \bmod 4$, $\left(\frac{-1}{p}\right)=-1, a\not\equiv -1 \bmod p$,

$$\sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r\equiv 0 \bmod p.$$

(2) 由于 $\sum\limits_{r=1,\left(\frac{r}{p}\right)=-1}^{p-1} r \equiv a \sum\limits_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r \equiv 0 \bmod p$, 其中 a 是模 p 的二次非剩余, 因此

$$\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = \sum_{r=1,\left(\frac{r}{p}\right)=1}^{p-1} r - \sum_{r=1,\left(\frac{r}{p}\right)=-1}^{p-1} r \equiv 0 \bmod p.$$

8.10. 我们将会用到习题8.9的结论. 设 $d = \frac{D}{4a^2}$, 则 $f(x) = a((x+\frac{b}{2a})^2 - d)$,

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) = \left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^2-d}{p}\right).$$

而 $\sum\limits_{x=0}^{p-1}(\left(\frac{x^2-d}{p}\right)+1)$ 是 $\mathbb{F}_p$ 中方程 $y^2 = x^2 - d$ 的解的个数, 即

$$\sum_{x=0}^{p-1}(\left(\frac{x^2-d}{p}\right)+1) = \begin{cases} p-1, & \text{如果 } p \nmid d, \\ 2p-1, & \text{如果 } p \mid d, \end{cases}$$

因此

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & \text{如果 } p \nmid D, \\ (p-1)\left(\frac{a}{p}\right), & \text{如果 } p \mid D. \end{cases}$$

18. 同余方程解的个数

8.9. 我们不妨在 $\mathbb{F}_p$ 中考虑. 如果 $a \neq 0$, 那么 $(x+y)(x-y) = a$, 设 $x+y = s \neq 0$, $x - y = as^{-1}$, $x = \frac{s+as^{-1}}{2}, y = \frac{s-as^{-1}}{2}$. 显然不同的 s 对应不同的解, 因此一共有 $p-1$ 组解. 如果 $a = 0, x = \pm y$, 所有的解为 $(0,0), (1,\pm1), (2,\pm2), \ldots, (p-1, \pm(p-1))$, 共 $2p-1$组.

8.11. (1) 显然 $x \equiv 1 \bmod 2$ 是解.

(2) 由于对任意整数 x, $x^2 \equiv 0, 1 \bmod 4$, 而 a 是奇数, 因此如果有解则 $a \equiv 1 \bmod 4$. 反之, 如果 $a \equiv 1 \bmod 4$, $x \equiv 1 \bmod 4$, $x \equiv \pm1$ 共两个解.

(3) 由于对任意整数 x, $x^2 \equiv 0, 1, 4 \bmod 8$, 而 a 是奇数, 因此如果有解则 $a \equiv 1 \bmod 8$. 反之, 我们利用数学归纳法. 假设 $a \equiv 1 \bmod 8$. 对于 $k = 3$, $x \equiv 1 \bmod 8$, $x \equiv \pm1, \pm3$. 设 $x^2 \equiv a \bmod 2^k$ 有解 x_0. 如果 $x_0^2 - a$ 是 2^{k+1} 的倍数, 则 x_0 是 $x^2 \equiv a \bmod 2^{k+1}$ 的一个解. 如果 $x_0^2 - a$ 不是 2^{k+1} 的倍数, 则 $(x_0 + 2^{k-1})^2 - a \equiv x_0^2 - a + 2^k x_0 \equiv x_0^2 - a + 2^k \equiv 0 \bmod 2^{k+1}$, 因此 $x_0 + 2^{k-1}$ 是 $x^2 \equiv a \bmod 2^{k+1}$ 的一个解.

不妨设 x_0 满足 $x_0^2 \equiv a \bmod 2^{k+1}$, 则 $x^2 \equiv x_0^2, 2^{k+1} \mid (x - x_0)(x + x_0)$, 而 x_0 是奇数, 因此 $x - x_0, x + x_0$ 不可能都是 4 的倍数, 于是 $2 \mid x \pm x_0, 2^k \mid x \mp x_0$, $x = \pm x_0, \pm x_0 + 2^k$.

19. 有限域上多项式

8.14. 如果 $p = 2$, 则 $x^2 - 15 = (x+1)^2$ 可约.

如果 $p = 3, 5$, 则 $x^2 - 15 = x^2$ 可约.

如果 $p \geq 7$, 则 $x^2 - 15$ 可约等价于有根, 即 $\left(\frac{15}{p}\right) = 1$. 而

$$\left(\frac{15}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)\left(\frac{p}{5}\right).$$

因此

$$p \equiv 1 \bmod 4,\ p \equiv 1 \bmod 3,\ p \equiv \pm 1 \bmod 5,$$

或

$$p \equiv 1 \bmod 4,\ p \equiv -1 \bmod 3,\ p \equiv \pm 2 \bmod 5,$$

或

$$p \equiv -1 \bmod 4,\ p \equiv -1 \bmod 3,\ p \equiv \pm 1 \bmod 5,$$

或

$$p \equiv -1 \bmod 4,\ p \equiv 1 \bmod 3,\ p \equiv \pm 2 \bmod 5,$$

即 $p \equiv \pm 1, \pm 7, \pm 11, \pm 17 \bmod 60$.

综上所述, $p = 2, 3, 5$ 或 $p \equiv \pm 1, \pm 7, \pm 11, \pm 17 \bmod 60$.

8.17. $x^2 + \alpha x + \beta = (x + \frac{\alpha}{2})^2 - \gamma, \gamma = \alpha^2/4 - \beta$, 该多项式不可约等价于没有根, 即 $\gamma \neq 0$ 且 $\left(\frac{\gamma}{p}\right) = -1$. 而这样的 γ 有 $\frac{p-1}{2}$ 个, α 任取, 因此一共有 $\frac{p(p-1)}{2}$ 个不可约多项式.

20. 整系数多项式

9.2. 数学归纳法. 首先注意到只需对非负整数 n 证明即可.

$n = 0, 1$ 显然.

设 $t = x + x^{-1}$. 如果对于 $0 \leq n \leq k$, $x^n + x^{-n} = f_n(t)$, f_n 是整系数多项式, 则

$$x^{k+1} + x^{-k-1} = (x^k + x^{-k})(x + x^{-1}) - (x^{k-1} + x^{1-k}) = tf_k(t) - f_{k-1}(t)$$

可以表示为 $t = x + x^{-1}$ 的整系数多项式.

9.4. 设 $g = c(g)g_1$, 则 $g_1 \in \mathbb{Z}[x]$ 本原, 于是 $f(x)g_1(x)$ 本原, $fg = c(g)fg_1$,

$$c(fg) = c(g)c(fg_1) = \pm c(g),$$

因此 $c(g) = \pm c(fg) \in \mathbb{Z}$, $g(x) \in \mathbb{Z}[x]$.

9.5. 设 $3x^3 + 2x^2 - 1$ 的三个根为 a, b, c, 则

$$a + b + c = -\frac{2}{3}, ab + ac + bc = 0, abc = \frac{1}{3}.$$

于是

$$a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + bc + ca) = \frac{4}{9},$$

$$a^2b^2 + b^2c^2 + c^2a^2 = (ab + bc + ca)^2 - 2abc(a + b + c) = \frac{4}{9},$$

$$a^2b^2c^2 = (abc)^2 = \frac{1}{9},$$

因此 a^2, b^2, c^2 是多项式 $f(x) = x^3 - \frac{4}{9}x^2 + \frac{4}{9}x - \frac{1}{9}$ 的三个根.

9.6. 由题设知在 $\mathbb{Q}[x]$ 中 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$. 不妨设在 $\mathbb{Q}[x]$ 中 $p(x) \mid f(x)$, 则存在 $q(x) \in \mathbb{Q}[x]$, $f(x) = p(x)q(x)$. 但是 $p(x)$ 是本原多项式, 由习题 9.4 知 $q(x) \in \mathbb{Z}[x]$, 因此在 $\mathbb{Z}[x]$ 中 $p(x) \mid f(x)$.

9.7. 由于它们都是首一的, 因此只需证明在 $\mathbb{Z}[x]$ 中不可约. (1) 设 $f(x)=x^4+3x+5$, 由于对任意整数 n, $f(n)$ 是奇数, f 没有整数解, 所以如果 f 可约, 必为两个2次整系数多项式之积. 设 $f(x)=(x^2+ax+b)(x^2-ax+c)$, 则

$$b+c-a^2=0,\ a(c-b)=3,\ bc=5.$$

由 $bc=5$ 知 $b-c=\pm 4\nmid 3$, 矛盾! 因此 f 不可约.

(2) 设 $f(x)=x^5+4x^4+2x^3+6x^2-x+5$, 由于对任意整数 n, $f(n)$ 是奇数, f 没有整数解, 所以如果 f 可约, 必为一个2次整系数多项式和一个3次整系数多项式之积. 设 $f(x)=(x^3+ax^2+bx+c)(x^2+(4-a)x+d)$, 则

$$a(4-a)+b+d=2,\ 6=c+b(4-a)+ad,\ -1=c(4-a)+bd,\ 5=cd.$$

于是

$$4-a=\frac{4d-6+c}{d-b},$$

$$-1=c\frac{4d+c-6}{d-b}+bd,$$

$$db^2+(1-d^2)b-d-20-c^2+6c=0.$$

由 $cd=5$ 知 $c\mid 5$. 如果 $c=5,d=1$, $b^2=16, b=\pm 4, a=5,3$, $a(4-a)+b+d=0$, 矛盾! 如果 $c=-5,d=-1$, $b^2=-74$, 无解. 如果 $c=\pm 1, d=\pm 5$, $5b^2-24b-20=0$ 或 $5b^2+24b+22=0$, 无解! 因此 f 不可约.

9.8. (1) 设 $f(x)=x^{p-1}+\cdots+x+1$, 则 $(x-1)f(x)=x^p-1$. 设 $y=x-1$, 则

$$yf(y+1)=(y+1)^p-1=y^p+\sum_{i=1}^{p-1}\binom{p}{i}y^i,$$

$$f(y+1)=y^{p-1}+\sum_{i=1}^{p-1}\binom{p}{i}y^{i-1},$$

由Eisenstein判别法知其不可约.

(2) 如果 $n=ab$ 不是素数, $a,b>1$, 则

$$(x-1)f(x)=x^n-1=(x^a-1)\sum_{i=0}^{b-1}x^{ai},$$

$$f(x)=(\sum_{j=0}^{a-1}x^j)(\sum_{i=0}^{b-1}x^{ai})$$

可约.

9.9. 假设 $f(x)=(x-a_1)\cdots(x-a_n)-1$ 可约,由于 f 首一, 存在首一的非常数整系数多项式 $g(x),h(x)$, $f(x)=g(x)h(x)$. 于是 $g(a_i)=\pm 1$. 不妨设 $g(a_1)=\cdots=g(a_t)=1, g(a_{t+1})=\cdots=g(a_n)=-1$, 则 $\deg g\geq\max\{t,n-t\}$, 同理 $\deg h\geq\max\{t,n-t\}$. 因此 $t=n-t=\deg g=\deg h$,

$$g(x)=(x-a_1)\cdots(x-a_t)+1,\ h(x)=(x-a_1)\cdots(x-a_t)-1,$$

$$f(x)=g(x)h(x)=(x-a_1)^2\cdots(x-a_t)^2-1,$$

矛盾!

9.10. f 的常数项模长大于等于1, 因此存在根 x_0, $|x_0| \geq 1$. 设

$$g(x) = \frac{f(x)}{x - x_0} = x^{n-1} + \sum_{i=0}^{n-2} b_i x^i,$$

则

$$a_0 = -x_0 b_0,$$

$$a_i = -x_0 b_i + b_{i-1}, \quad 1 \leq i \leq n-2,$$

$$a_{n-1} = -x_0 + b_{n-2},$$

于是

$$\begin{aligned} |b_{n-2}| + |x_0| &\geq |b_{n-2} - x_0| = |a_{n-1}| \\ &> 1 + \sum_{i=0}^{n-2} |a_i| \\ &= 1 + \sum_{i=0}^{n-2} |x_0 b_i - b_{i-1}| \\ &\geq 1 + \sum_{i=0}^{n-2} (|x_0 b_i| - |b_{i-1}|) \\ &= (|x_0| - 1) \sum_{i=0}^{n-2} |b_i| + |b_{n-2}| + 1 \end{aligned}$$

$$(|x_0| - 1)(\sum_{i=0}^{n-2} |b_i| - 1) < 0,$$

因此 $|x_0| > 1, \sum_{i=0}^{n-2} |b_i| < 1$.

设 $g(x) = (x - y_0)(x^{n-2} + \sum_{i=0}^{n-3} c_i x^i)$, 则类似地, 我们有

$$1 > \sum_{i=0}^{n-2} |b_i| \geq (|y_0| - 1) \sum_{i=0}^{n-3} |c_i| + |y_0|,$$

$$(|y_0| - 1)(\sum_{i=0}^{n-3} |c_i| + 1) < 0,$$

$|y_0| < 1$. 因此 f 只有一个根模长大于1, 其余模长均小于1. 如果 $f = gh$ 可约, 则 g, h 的常数项均非零, 均存在模长大于等于1的根, 矛盾! 因此 f 不可约.

实际上, 如果我们利用复变函数中儒歇定理, 可以知道在 S^1 上 $|f - a_{n-1}x^{n-1}| < |a_{n-1}x^{n-1}|$, 从而 f 和 $a_{n-1}x^{n-1}$ 在 S^1 内部有相同多的根, 即 $n-1$ 个.

9.11. (1)

$$\begin{aligned} & x_1^2 x_2 + x_2^2 x_1 + x_1^2 x_3 + x_3^2 x_1 + x_2^2 x_3 + x_3^2 x_2 \\ =& x_1 x_2 (s_1 - x_3) + x_1 x_3 (s_1 - x_2) + x_2 x_3 (s_1 - x_1) \\ =& (x_1 x_2 + x_1 x_3 + x_2 x_3) s_1 - 3 s_3 \\ =& s_1 s_2 - 3 s_3. \end{aligned}$$

(2) 首先 $x_1^2+x_2^2+x_3^2=s_1^2-2s_2$.

$$\begin{aligned}&x_1(x_2^3+x_3^3)+x_2(x_1^3+x_3^3)+x_3(x_1^3+x_2^3)\\=&x_1x_2(x_1^2+x_2^2)+x_1x_3(x_1^2+x_3^2)+x_2x_3(x_2^2+x_3^2)\\=&s_2(x_1^2+x_2^2+x_3^2)-x_1x_2x_3(x_1+x_2+x_3)\\=&s_2(s_1^2-2s_2)-s_3s_1=s_1^2s_2-2s_2^2-s_1s_3.\end{aligned}$$

9.12. 数学归纳法. 设 $t_n=x_1^n+x_2^n+x_3^n$. $n=0,1,2$ 时, $t_0=3,t_1=-a,t_2=a^2-2b$ 是整数. 设 $k\geq 2$, 如果对于 $n\leq k$, $t_n=x_1^n+x_2^n+x_3^n$ 是整数, 则

$$\begin{aligned}t_{k+1}&=-at_k-x_1x_2(x_1^{k-1}+x_2^{k-1})-x_2x_3(x_2^{k-1}+x_3^{k-1})-x_3x_1(x_3^{k-1}+x_1^{k-1})\\&=-at_k-x_1x_2(t_{k-1}-x_3^{k-1})-x_2x_3(t_{k-1}-x_1^{k-1})-x_3x_1(t_{k-1}-x_2^{k-1})\\&=-at_k-bt_{k-1}-ct_{k-2}\end{aligned}$$

是整数.

21. 勘误

习题1.12: "分拆"改为"有序分拆".
习题1.17: z 是纯虚数当且仅当 $\bar{z}=-z$ 且 $z\neq 0$.
习题2.1: "矩阵"改为"2阶方阵".
习题2.4: "方阵"改为"实方阵".
习题2.10: "$\mathbb{Z}(\sqrt{2})$"改为"$\mathbb{Z}[\sqrt{2}]$".
习题2.17: 两处"-30"改为"-3".
习题5.9: $n\geq 2$.
习题8.13: "素数"改为"奇素数".
习题9.11(1) 改为 $x_1^2x_2+x_2^2x_1+x_1^2x_3+x_3^2x_1+x_2^2x_3+x_3^2x_2$.