代数学基础作业

中国科学技术大学

2024 秋　杨金榜

陈鉴 & 王子涵 & 辛雨 & 张煜星

第一次作业

9/10　第二周/星期二

1. *(习题 1.1)* 对任意集合 X，我们用 $\mathrm{id_X}$ 表示 X 到自身的恒等映射。设 $f: A \to B$ 是集合间的映射，A 是非空集合。试证：

   (a) f 为单射当且仅当存在 $g: B \to A$，使得 $g \circ f = \mathrm{id_A}$;

   (b) f 为满射当且仅当存在 $h: B \to A$，使得 $f \circ h = \mathrm{id_B}$;

   (c) f 为双射当且仅当存在唯一的 $g: B \to A$，使得 $f \circ g = \mathrm{id_B}, \mathrm{g \circ f = id_A}$。

   这里的 g 称为 f 的逆映射，通常也记为 f^{-1}。证明双射的逆映射也是双射，并讨论逆映射与映射的原像集合之间的关系。

2. *(习题 1.2)* 如果 $f: A \to B, g: B \to C$ 均是一一对应，则 $g \circ f: A \to C$ 也是一一对应，且 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。

3. *(习题 1.5)* 设 X 是无限集，Y 是 X 的有限子集。证明存在双射 $X - Y \to X$。

4. *(习题 1.8)* 设 A，B 是两个有限集合。

   (a) A 到 B 的不同映射共有多少个？

5. *(习题 1.9)* 证明容斥原理（定理 *1.24*）。

6. *(课堂练习 1)* 若 $|A| = |B| < \infty, \forall f: A \to B$，$f$ 单 $\iff$ f 双 $\iff$ f 满。

7. *(课堂练习 2)* 若 $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$，证明 $h \circ (g \circ f) = (h \circ g) \circ f$。

代数学基础作业

中国科学技术大学

2024 秋　杨金榜

陈鉴 & 王子涵 & 辛雨 & 张煜星

第二次作业

9/12　第二周/星期四

8. 回顾：设 $\varphi\colon K\times K\to K$ 为集合 K 上的二元运算。若对任意 $x,y,z\in K$ 都有 $\varphi(\varphi(x,y),z)=\varphi(x,\varphi(y,z))$，则称 φ 满足结合律。若存在 $e\in K$ 使得对任意 $x\in K$ 都有 $\varphi(e,x)=x=\varphi(x,e)$, 则称 e 为 φ 的单位元。若对任意 $x,y\in K$ 都有 $\varphi(x,y)=\varphi(y,x)$, 则称 φ 满足交换律。

   设 $K=\{A,B\}$ 为两个元素组成的集合, 请

   (a) 在集合 K 上找出所有的二元运算 *(*用表格表示, 共 16 个*)*

   (b) 哪几个运算存在单位元

   (c) 那几个满足交换律

   (d) 共有 8 个满足结合律, 尽可能多的找出它们.*(*不需要证明*)*

9. ①验证：$\mathbb{Q}[i]$ 为域（在通常复数域上的 $+,\cdot$ 运算下）;
   ②说明 $K=\mathbb{Q}+\mathbb{Q}\sqrt[3]{2}=\{a+b\sqrt[3]{2}|a,b\in\mathbb{Q}\}$ 在通常 $+,\times$ 下不为域;
   ③请试着构造 K 上两个二元运算 $\oplus,\odot$，使得 $(K,\oplus,\odot)$ 构成域（说明想法即可，无需证明）。

10. 回顾*:* 设 $(K,+,\cdot)$ 为域. 任意元素 $a\in K$ 存在负元, 我们将其记为 $-a$. 并将加法 $b-a$ 定义为 $b+(-a)$. 任意非零元 $a\in K\setminus 0$ 存在逆元, 我们将其记为 a^{-1}. 并将除法 $\frac{b}{a}$ 定义为 $b\cdot a^{-1}$. 请从域的公理体系出发证明:

$$\frac{b}{a}-\frac{d}{c}=\frac{bc-ad}{ac}.$$

11. 证明数集 $R=\left\{\frac{x+y\sqrt{-3}}{2}\middle|x\text{与}y\text{为同奇偶的整数}\right\}$ 在通常的加法和乘法下构成环.

12. 记 $\mathbb{R}[X]$ 为实系数多项式组成的集合, 即

$$\mathbb{R}[X]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n\mid\ n\in\mathbb{N}\text{ 以及 }a_0,a_1,\cdots,a_n\in\mathbb{R}\}.$$

在这个集合上定义通常的多项式加法与乘法. 即, 对任意多项式 $f(x) = \sum_{i=0}^{n} a_i x^i$ 和 $g(x) = \sum_{i=0}^{m} b_i x^i$,

$$f(x) + g(x) = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i$$

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} \left(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j \right) x^k$$

其中, 若 $i > n$, 记 $a_i = 0$; 若 $j > m$, 记 $b_j = 0$. 则 $(\mathbb{R}[X], +, \cdot)$ 构成环, 称为实系数多项式环, 简记为 $\mathbb{R}[X]$.

(a) 请写出实系数多项式环中的零元, 幺元以及负元.

(b) 请证明实系数多项式环是交换环.

(c) (附加，不写不影响作业评分) 请问实系数多项式环是否为域, 为什么? 如果不是，能不能将集合 $\mathbf{R}[X]$ 扩大, 使得其在通常加法和乘法下构成域.

第三次作业

9/19　第三周/星期四

13. 回顾: 实数域上的二阶矩阵组成的集合为

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}.$$

这个集合上可以定义如下加法和乘法运算:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

则 $(M_2(\mathbb{R}), +, \cdot)$ 构成环, 称为实数域上的二阶矩阵代数.

(a) 证明矩阵代数上的乘法结合律.

(b) 举例说明矩阵代数上, 乘法不满足消去律. 即由 $ac = bc$ 以及 $c \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 推不出 $a = b$. 提示: 求 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2$.

14. 回顾: 复数域上的二阶矩阵组成的集合为

$$M_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{C} \right\}.$$

这个集合上可以定义如下加法和乘法运算:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

则 $(M_2(\mathbb{C}),+,\cdot)$ 构成环. 此外, 我们对任意 $e\in\mathbb{C}$ 我们定义如下记号:

$$e\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} ea & eb\\ ec & ed\end{pmatrix}.$$

环 $(M_2(\mathbb{C}),+,\cdot)$ 称为复数域上的二阶矩阵代数. 记

$$i=\begin{pmatrix} \sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{pmatrix},\quad j=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix},\quad \text{以及}\quad k=\begin{pmatrix} 0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{pmatrix}.$$

证明:

(a) $i^2=j^2=k^2=ijk=\begin{pmatrix} -1 & 0\\ 0 & -1\end{pmatrix}$;

(b) $ij=-ji=k$; $jk=-kj=i$; $ki=-ik=j$;

(c) $M_2(\mathbb{C})$ 的子集 $\mathbb{H}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}\}\subset M_2(\mathbb{C})$(这里的 a 视为 aI_2，其中 $I_2=\begin{pmatrix} 1 & 0\\ 0 & 1\end{pmatrix}$) 关于乘法封闭;

注: 实际上, $\mathbb{H}$ 构成 $M_2(\mathbb{C})$ 的子环, 且其中任意非零元都有乘法逆元.

15. 给定集合 M, 令 S_M 为 M 到自身的双射的集合. 证明若以映射的复合 $\circ$ 作为 S_M 上的乘法, 则 $(S_M,\circ)$ 构成一个群.

16. 设集合 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$, 验证它在实数加法和乘法意义下构成环.

17. 设 A 为含幺非交换环，$a,b\in A$. 如果 $ba=1$, 则称 b 为 a 的左逆, a 为 b 的右逆. 如果并思考以下几个问题:

(a) 如果 a 的左逆与右逆同时存在，则左逆等于右逆;

(b) 如果 a 的左逆存在且唯一, 则 a 有右逆; (提示: 若 b 为 a 的左逆, 则 $ab+b-1$ 也为 a 的左逆.)

(c) 如果 a 的左逆不止一个，则必有无数个左逆. (提示: 采用反证法. 考察由 a 的全体左逆组成的集合 $Inv_a:=\{x\in A\mid xa=1\}$. 假若 Inv_a 有限且个数大于 1, 不妨设 $x_1\in Inv_a$, 则 $\{1-ax+x_1\mid x\in Inv_a\}=Inv_a$).

(d) (选做) 请构造一个环 A 使得，里面存在元素 a，其仅有左逆而没有右逆;

注意：9.19 和 9.24 作业应于 9.26-9.30 期间提交

第四次作业

9/24　第四周/星期二

18. 令集合 $G=\{A,B\}$. 用表格的形式列出全部 G 上的运算 φ, 使得 (G,φ) 构成

    1) 半群;

    2) 含幺半群;

    3) 群;

    4) 交换群.

19. 若 G 是群, $x,y\in G$, 定义 x,y 的换位子为

$$[x,y]=xyx^{-1}y^{-1}.$$

    证明

    1) $[x,y]^{-1}=[y,x]$;

    2) $[xy,z]=x\,[y,z]\,x^{-1}\,[x,z]$;

    3) $[z,xy]=[z,x]\,x\,[z,y]\,x^{-1}$.

20. 令 μ_∞ 为 $\mathbb{C}$ 里的所有单位根（即 $\mu_\infty=\{a\in\mathbb{C}|$存在正整数 n 使得$a^n=1\}$），证明 μ_∞ 在复数乘法意义下构成群.

21. 设 A 为集合，$P(A)$ 为 A 里的所有子集构成的集合，在 $P(A)$ 上定义二元运算：$X\Delta Y=(X\bigcap Y^c)\bigcup(X^c\bigcap Y)$，证明 $P(A)$ 在此运算下构成群.

22. 我们给定一个乘法群 G 和其子集 M：

    1) 我们定义 $N_G(M)=\{g\in G|gMg^{-1}=M\}$，请证明 $N_G(M)$ 是 G 的子群

    2) 我们定义 $C_G(M)=\{g\in G|gag^{-1}=a,\forall a\in M\}$，请证明 $C_G(M)$ 是 G 的子群

23. 设 G 为二元实数组构成的集合 $\{(a,b)|a\neq 0\}$,我们定义 G 上的乘法为 $(a,b)(c,d)=(ac,ad+b)$，求证 G 在此运算下是群.

以下三题至少选做一题

24. 试着求出 S_3 的所有子群.
    试着求出 D_4 的所有子群.

25. 设 G 是半群，若对任意的 $a, b \in G$，方程 $xa = b$ 和 $ay = b$ 都在 G 里面有解，证明 G 是群.(提示: 若 $ea = a$, 则 $eb = b$.)

26. 设 G 是一个有限半群, 如果在 G 内均有左右消去律成立, 即由 $ax = ay$ 或 $xa = ya$ 都可以推得 $x = y$，证明 G 是群. (提示:$G = \{ag \mid g \in G\}$.)

注意：9.19 和 9.24 作业应于 9.26-9.30 期间提交

第五次作业

9/26　第四周/星期四

27. (习题 2.14) 群 G 到自身的同构称为 G 的自同构。

    1) 证明群 G 的所有自同构在复合映射作为乘法下构成群。这个群称为 G 的自同构群，记为 $AutG$;
    2) 如 $\varphi : G \xrightarrow{\sim} H$ 为群同构，证明 G 到 H 的所有同构构成集合 $\varphi AutG := \{\varphi \circ f | f \in AutG\}$。

28. 设 G 是群。试问映射 $x \to x^2$ 何时是群同态？并分别举例说明：这一映射可能是单同态但不是满同态，可能是满同态但不是单同态，也可能是同构。

29. (习题 2.16) 设 G 是群。证明映射 $x \to x^{-1}$ 是群同构当且仅当 G 为阿贝尔群。

30. (习题 2.18) 证明乘法群 $\mathbb{C}^\times \cong \mathbb{R}_+^\times \times S^1$，其中 $\mathbb{R}_+^\times$ 是正实数构成的乘法群。

31. (习题 2.25) 如果 I, J 均是交换环 R 的理想，证明

$$I + J = \{x + y | x \in I, y \in J\}$$

与 $I \cap J$ 都是 R 的理想。举例说明 $I \cup J$ 不一定为 R 的理想。

32. 回顾：正交群 $O_2(\mathbb{R})$ 为：

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} cos\theta & \mp sin\theta \\ sin\theta & \pm cos\theta \end{pmatrix} \middle| \theta \in \mathbb{R} \right\}.$$

证明：

$$O_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a, b, c, d \in \mathbb{R} \right\}.$$

33. 设 $(R,+,\cdot)$ 为环，$\varphi: R \to T$ 为双射。定义 T 上的二元运算 $\oplus, \odot$：

$$t_1 \oplus t_2 := \varphi(\varphi^{-1}(t_1) + \varphi^{-1}(t_2))$$

$$t_1 \odot t_2 := \varphi(\varphi^{-1}(t_1) \cdot \varphi^{-1}(t_2))$$

证明：

1) $(T, \oplus, \odot)$ 构成环;

2) φ 是从 $(R,+,\cdot)$ 到 $(T, \oplus, \odot)$ 的环同构。

34. 求所有从 $\mathbb{Q}[\sqrt{2}]$ 到 $\mathbb{Q}[\sqrt{2}]$ 的环同态。

35. (选做)设 φ 是从 $(\mathbb{R},+,\cdot)$ 到 $(\mathbb{R},+,\cdot)$ 的环同构，试证明：$\varphi = id_{\mathbb{R}}$

注意：9.26 和 9.29 作业应于 9.29-10.8 期间提交

第六次作业

9/29　第四周/星期日

36. 证明映射 $\varphi : \mathbb{C} \to M_2(\mathbb{R}),\ a + b\sqrt{-1} \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ 是环同态。

37. 设 G_1, G_2 为群，在笛卡尔积 $G_1 \times G_2$ 上定义乘法运算 $\cdot$, 对任意 $g_1, g_1' \in G_1$ 和 $g_2, g_2' \in G_2$,
$$(g_1, g_2) \cdot (g_1', g_2') := (g_1 g_1', g_2 g_2').$$
   1）证明 $(G_1 \times G_2, \cdot)$ 构成群，称之为群 G_1 和群 G_2 的**直积**或者**笛卡尔积**;
   2）证明**投影映射**
$$Pr_1 : G_1 \times G_2 \to G_1,\ (g_1, g_2) \mapsto g_1$$
   和
$$Pr_2 : G_1 \times G_2 \to G_2,\ (g_1, g_2) \mapsto g_2$$
   均是群的满同态;
   3）证明映射
$$I_1 : G_1 \to G_1 \times G_2,\ g_1 \mapsto (g_1, 1_{G_2})$$
   和
$$I_2 : G_2 \to G_1 \times G_2,\ g_2 \mapsto (1_{G_1}, g_2)$$
   均是群的单同态。

38. 设 R_1, R_2 为环, 在笛卡尔积 $R_1 \times R_2$ 上定义两个二元运算 $+$ 和 $\cdot$, 对任意 $r_1, r_1' \in R_1$ 和 $r_2, r_2' \in R_2$,
$$(r_1, r_2) + (r_1', r_2') := (r_1 + r_1', r_2 + r_2')$$
$$(r_1, r_2) \cdot (r_1', r_2') := (r_1 r_1', r_2 r_2')$$
   1）证明 $(R_1 \times R_2, +, \cdot)$ 构成环，称之为环 R_1 与环 R_2 的**直积**或者**笛卡尔积**;
   2）证明投影映射
$$Pr_1 : R_1 \times R_2 \to R_1,\ (r_1, r_2) \mapsto r_1$$

和

$$Pr_2: R_1 \times R_2 \to R_2,\ (r_1, r_2) \mapsto r_2$$

均是环的满同态;

3) 设 R_1 与 R_2 都不为零环，证明映射

$$I_1: R_1 \to R_1 \times R_2,\ r_1 \mapsto (r_1, 0_{R_2})$$

和

$$I_2: R_2 \to R_1 \times R_2,\ r_2 \mapsto (0_{R_1}, r_2)$$

均保持加法和乘法但不是环同态;

4) 证明若 R_1 与 R_2 都不为零环，则 $R_1 \times R_2$ 一定不是整环。

39. 设 R 为交换环，证明:

1) R 为整环 $\iff$ $R[x]$ 为整环;

2) 若 R 为整环，证明 $R^\times = R[x]^\times$。

40. 设 R 为交换环，对任意 $a \in R$，定义 φ_a 为：$\varphi_a: R[x] \to R,\ f(x) \mapsto f(a)$. 证明 φ_a 是环的满同态，称之为**赋值映射**。

41. 设 R 为交换环, $f, g \in R[x]$. 证明:

1) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$;

2) $\deg(fg) \leq \deg(f) + \deg(g)$;

3) 若 R 为整环，则 $\deg(fg) = \deg(f) + \deg(g)$。

42. (选做)证明：有限整环是域。

注意：9.26 和 9.29 作业应于 9.29-10.8 期间提交

代数学基础作业

中国科学技术大学

2024 秋　杨金榜

陈鉴 & 王子涵 & 辛雨 & 张煜星

第七次作业

10/8　第六周/星期二

43. 设 n 为正整数, 证明 $\gcd(n!+1,(n+1)!+1)=1$. 这里 $n!=n(n-1)\cdots 1$ 是 n 的阶乘.

44. 设 n 为正整数, m 为正奇数. 证明: $\gcd(2^m-1,2^n+1)=1$.

45. 求 $\gcd(1573,-1859),\gcd(-121,-169),\gcd(76501,9719)$.

46. 设 n 为正整数. 证明: n 至多有 $2\lfloor\sqrt{n}\rfloor$ 个正因子. 这里 $\lfloor\cdot\rfloor$ 表示向下取整.

47. 设 n 为正整数. 证明: $n^2|(n+1)^n-1$.

48. (选做) 记 $X=\{m+\frac{n}{n+1}|n,m\in\mathbb{N}\}$. 证明: X 的任意非空子集均有最小元, 即 X 为良序集. (注: 这里的序关系是继承自 $(\mathbb{R},\leq)$ 的)

注意：10.8 和 10.10 作业应于 10.10-10.15 期间提交

第八次作业

10/10　第六周/星期四

49. 设 n 为正整数，a,b 为正整数，证明：
(1) $\gcd(a^n,b^n)=\gcd(a,b)^n$;
(2) 设 a,b 是互素的正整数，c 为正整数，$ab=c^n$，则 a,b 都是某个正整数的 n 次方幂。

50. 用欧几里得算法求 963 和 657 的最大公约数，并求出方程 $963x+657y=\gcd(963,657)$ 的一组特解，以及所有整数解。

51. 设 a,b 为正整数且 $\gcd(a,b)=1$。证明：当整数 $n>ab-a-b$ 时，方程 $ax+by=n$ 有非负的整数解；但当 $n=ab-a-b$ 时，该方程没有非负整数解。

52. 求 $\operatorname{lcm}(1573,-1859)$，$\operatorname{lcm}(-121,-169)$，$\operatorname{lcm}(76501,9719)$.

53. (选做) 设 $p(x)=a_0+a_1x+\cdots+a_nx^n$ 为整系数多项式，$a_0,a_n\neq 0$。证明：$p(x)$ 的有理数根 $x_0=\frac{p}{q}$ 满足 $p\mid a_0, q\mid a_n$，其中 p,q 为互素的整数。

54. (选做) 求所有的正整数列 $\{a_i\}$ 满足 $\forall i\neq j, \gcd(i,j)=\gcd(a_i,a_j)$.（提示：Don't spend too much time on this question）

注意：10.8 和 10.10 作业应于 10.10-10.15 期间提交

第九次作业

10/15　第七周/星期二

55. 设 $\varphi : R_1 \to R_2$ 为环同态，证明：
   (1) 若 $J \lhd R_2$，则 $\varphi^{-1}(J) := \{r_1 \in R_1 | \varphi(r_1) \in J\}$ 为 R_1 的理想;
   (2) 若 $I \lhd R_1$ 且 φ 为满射，则 $\varphi(I) \lhd R_2$;
   (3) 给出反例说明若 φ 不为满射则 (2) 不一定成立。

56. 设 I 为 R 的理想，证明：

$$M_2(I) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in I \right\}$$

   为 R 上矩阵代数 $M_2(R)$ 的理想。

57. 设 R 为环（不一定交换），证明：

$$(a) = \left\{ \sum_{i=1}^{n} x_i a y_i \middle| x_i . y_i \in R, n \in \mathbb{N} \right\},$$

   其中左边为由 a 生成的理想, 即定义为包含 a 的最小理想。

58. 设 R 为含幺交换环. 设 $I_1, I_2 \lhd R$ 是两个理想, 若 $I_1 + I_2 = R$, 则称 I_1, I_2 **互素**.
   (1) 若 I_1, I_2 互素, 证明 $I_1 \cap I_2 = I_1 I_2$;
   (2) 若 $I_1, \cdots, I_n$ 两两互素, 证明:
      (a) I_1 与 $I_2 \cdots I_n$ 互素;
      (b) $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

注意：10.15 和 10.17 作业应于 10.17-10.22 期间提交

代数学基础作业

中国科学技术大学

2024 秋　杨金榜

陈鉴 & 王子涵 & 辛雨 & 张煜星

第十次作业

10/17　第七周/星期四

59. 设 f 为 $\mathbb{Z}_{>0}$ 上的函数

 (1) 若对所有互素的正整数 m,n, 有 $f(mn)=f(m)f(n)$, 则称 f 为积性函数;

 (2) 若对任意的正整数 m,n, 有 $f(mn)=f(m)f(n)$, 则称 f 为完全积性函数;

 设正整数 n 的因式分解为 $n=p_1^{v_{p_1}(n)}\cdots p_s^{v_{p_s}(n)}$, 定义

$$\sigma_k(n)=\sum_{d|n,d\geq 1}d^k$$

 证明:

 (1)

$$\sigma_k(n)=\prod_{i=1}^{s}\frac{p_i^{(v_{p_i}(n)+1)k}-1}{p_i^k-1},(k\geq 1);$$

 (2) $\sigma_k(n)$ 为积性函数但不是完全积性函数.

60. (习题 3.7) 设 $n>1$ 为整数，如果对于任何整数 m, 或者 $n\mid m$ 或者 $(n,m)=1$, 则 n 必是素数.

61. (习题 3.8) 设整数 $n>2$, 证明：n 和 $n!$ 之间必有素数. 由此证明素数有无穷多个.

62. (习题 3.11) 设 a,b 是整数，$a\neq b,n$ 是正整数. 如果 $n\mid(a^n-b^n)$, 则 $n\mid\frac{a^n-b^n}{a-b}$.

63. (习题 3.12) 设 $n\geqslant 1$. 证明：

 (1) n 为完全平方数的充要条件是 $\sigma_0(n)$ 为奇数，

 (2) $\sigma_0(n)\leqslant 2\sqrt{n}+1$;

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

64. (习题 3.13) 设 $m\in\mathbb{Z}_+$ 的因式分解为 $m=\prod_i p_i^{\alpha_i}$. 若 f 为积性函数，证明

$$f(m)=\prod_i f(p_i^{\alpha_i}).$$

65. (选做) (习题 3.9)

(1) 设 m 为正整数，证明：如果 2^m+1 为素数，则 m 为 2 的方幂。

(2) 对 $n \geqslant 0$, 记 $F_n = 2^{2^n}+1$, 这称为费马数. 证明: 如果 $m > n$, 则 $F_n \mid (F_m - 2)$;

(3) 证明：如果 $m \neq n$, 则 $(F_m, F_n) = 1$. 由此证明素数有无穷多个.

66. (选做) (习题 3.10)

(1) 设 m, n 都是大于 1 的整数，证明：如果 $m^n - 1$ 是素数，则 $m = 2$ 并且 n 是素数.

(2) 设 p 是素数，记 $M_p = 2^p - 1$, 这称为梅森数. 证明：如果 p, q 是不同的素数，则 $(M_p, M_q) = 1$.

67. (选做) (习题 3.14) 对于 $n = p_1^{e_1} \cdots p_s^{e_s} \in \mathbb{Z}_+$, 令

$$\mu(n) = \begin{cases} 1, & \text{如果} n = 1, \\ (-1)^s, & \text{如果} e_1 = \cdots = e_s = 1, \\ 0, & \text{其他情况}. \end{cases}$$

$\mu(n)$ 称为默比乌斯 (Möbius) 函数，证明:

$$\sum_{1 \leqslant d \mid n} \mu(d) = \begin{cases} 1, & \text{如果} n = 1, \\ 0, & \text{如果} n > 1. \end{cases}$$

68. (选做) (习题 3.15) 设 $f(x)$ 和 $g(x)$ 为两个定义在正整数集合 $\mathbb{Z}_+$ 上的函数 (值域可以为任何数域). 证明:

(1) $g(n) = \sum_{1 \leqslant d \mid n} f(d)$ 当且仅当 $f(n) = \sum_{1 \leqslant d \mid n} \mu(d) g(\frac{n}{d})$.

(2) 如果 $g(x) \neq 0$, 则 $g(n) = \prod_{1 \leqslant d \mid n} f(d)$ 当且仅当 $f(n) = \prod_{1 \leqslant d \mid n} g(\frac{n}{d})^{\mu(d)}$.

其中 μ 为上题的默比乌斯函数。上面两个等价关系习惯上称为默比乌斯反演公式 (Möbius inversion formula).

69. (选做) 证明 ED（欧几里得整环）$\Rightarrow$ PID（主理想整环）。

注意：10.15 和 10.17 作业应于 10.17-10.22 期间提交

第十一次作业

10/22　第八周/星期二

70. 证明：连续 n 个整数中恰有一个被 n 整除.

71. (1) 证明：完全平方数模 3 同余于 0 或 1，模 4 同余于 0 或 1，模 5 同余于 0,1 或 4;

    (2) 证明：完全立方数模 9 同余于 0 或 ±1; 整数的四次幂模 16 同余于 0 或 1.

72. 设 a 是奇数，n 是正整数，证明：$a^{2^n} \equiv 1\ mod\ 2^{n+2}$.

73. 设 m, n 都是正整数且有 $m = nt$，则模 n 的任何一个同余类

$$\{x \in \mathbb{Z} | x \equiv r\ mod\ n\}$$

可表示为 t 个模 m 的 (两两不同的) 同余类

$$\{x \in \mathbb{Z} | x \equiv r + in\ mod\ m\}(i = 0, 1, ..., t-1)$$

之并.

74. 计算如下同余方程 (注: 需要有计算过程):

    (a) $5x \equiv 11 \mod 13$

    (b) $29x \equiv 7 \mod 17$

    (c) $26x \equiv 34 \mod 43$

75. 设 p 为奇素数，证明：
(1) $\binom{p-1}{i-1} \equiv (-1)^{i-1} \mod p$;
(选做)(2) $\sum_{i=1}^{p-1} 2^i \cdot i^{p-2} \equiv \sum_{i=1}^{\frac{p-1}{2}} i^{p-2} \mod p$。(提示: 利用 (1)，以及证明 (2) 两边在模 p 意义下等于 $-\frac{1}{p}(2^p - 2)$)

注意：10.22 和 10.24 作业应于 10.24-10.29 期间提交

第十二次作业

10/24　第八周/星期四

76. 判定如下同余方程组是否有解, 如果有解求出解集:

(a) $$\begin{cases} x \equiv 4321 \mod 440533, \\ x \equiv 138344 \mod 563137, \end{cases}$$

(b) $$\begin{cases} x \equiv 4321 \mod 266243, \\ x \equiv 13834 \mod 478997. \end{cases}$$

注: 这题的目的是让大家感受一下, 当 m_i 比较大时, 不同方法的效率. 课堂上有部分同学没有按照辗转相除法来求解同余方程组, 大家可以先试试用自己的方法解这一道题. 比较一下, 辗转相除法和自己的方法那个更高效. 这一题允许大家用计算器做加减乘.

77. 利用中国剩余定理求解下列同余方程组:

$$\begin{cases} 2x \equiv 7 \mod 11, \\ 3x \equiv 12 \mod 17, \\ 5x \equiv 3 \mod 19. \end{cases}$$

78. 求解下列同余方程组:

$$\begin{cases} x \equiv 11 \mod 40, \\ x \equiv 31 \mod 100, \\ x \equiv 45 \mod 98. \end{cases}$$

79. (a). 设 p 为素数, r 为正整数. 求 $\varphi(p^r)$. (其中 φ 为欧拉函数.)
(b). 设 p, q 为不同的素数. 求 $\varphi(pq)$.

80. 证明：设 p 为素数，则有 $(p-1)! \equiv -1 \mod p$ (威尔逊定理). (提示: $1, \cdots, p-1$ 中除了 1 和 -1 外, 其它元素可两两配对使得它们乘积模 p 同余于 1.)

81. 设 p 为奇素数, 如果 $r_1, \cdots, r_{p-1}$ 与 $r_1', \cdots, r_{p-1}'$ 都过模 p 的非零同余类 $\{[1], [2], \cdots, [p-1]\}$，证明：$r_1r_1', \cdots, r_{p-1}r_{p-1}'$ 不过模 p 的非零同余类 $\{[1], [2], \cdots, [p-1]\}$，即证明存在 $i \neq j$，使得 $r_ir_i' \equiv r_jr_j' \mod p$. (提示: 威尔逊定理.)

以下题目选做. 以后想学数论的同学必做.

82. 证明：对于任意正整数 n，都存在 n 个连续正整数，使得它们其中每个数都不是素数的幂次 (即不为 p^α，其中 p 为素数，α 为正整数).

83. 设 m 为正整数，n 为整数，证明：数 2n 可以表示为两个与 m 互素的整数之和 (提示：我们先证明一个引理：对于 m 为正整数，n 为整数，存在整数 a, b 且满足 $(a, m) = 1, (b, m) = 1$，使得 $2n \equiv a + b \mod m$)

84. 给定素数 $p > 5$，对于 $k \in \{1, \cdots, p-1\}$，我们在模 $q = p^n$ 意义下定义 $\frac{1}{k} \equiv [x_k] \mod q$, 其中$x_k$满足$x_k \cdot k \equiv 1 \mod q$，证明下列式子成立：

(1) $\sum\limits_{k=1}^{p-1} \frac{1}{k^4} \equiv 0 \mod p$;

(2) $\sum\limits_{k=1}^{p-1} \frac{1}{k^3} \equiv 0 \mod p^2$.

注意：10.22 和 10.24 作业应于 10.24-10.29 期间提交

第十三次作业

10/29　第九周/星期二

85. 计算 $\varphi(360), \varphi(429)$.

86. (1) 证明: 当 $n \geq 3$ 时, $\varphi(n)$ 是偶数;
(2) 证明: 当 $n \geq 2$ 时, 不超过 n 且与 n 互素的正整数之和是 $\frac{n\varphi(n)}{2}$.

87. (1) 求 3^{421} 十进制表示中的末两位数码.
(2) 求 18^{1001} 十进制表示中的末两位数码.

88. 设 $\gcd(a, 10) = 1$，证明：$a^{20} \equiv 1 \mod 100$.

89. 设 m,n 为正整数，$\gcd(m, n) = 1$. 证明：$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \mod mn$.

90. 设 a 与 m 为正整数. 记群同态 $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \overline{x} \mapsto \overline{ax}$ 为 φ_a. 证明: 对于任意 $b \in \mathbb{Z}$, 若 $\varphi_a^{-1}(\bar{b}) \neq \emptyset$, 则 $|\varphi_a^{-1}(\bar{b})| = |\ker(\varphi_a)| = \gcd(a, m)$.

91. 设 q 为素数, k 为域. 证明:
(1) $\varphi \colon \mathbb{Z} \to k, n \mapsto n \cdot 1_k$ 为环同态. (注: 此处 $\cdot$ 不是 k 中乘法, 是取 1_k 的倍数.)
(2) 若 φ 不是单同态，则理想 $\ker(\varphi)$ 的正生成元为素数, 记为 p.
(3) 若 k 为有限域, 则 $p \mid |k|$. (提示: k 可写为形如 $\{a + n \cdot 1_k \mid n \in \mathbb{Z}\}$ 的子集的无交并, 这些子集的元素个数均为 p.)
(4) 若 k 为 q 元域, 则 k 与 $\mathbb{F}_q := \mathbb{Z}/q\mathbb{Z}$ 同构. (提示: 记 $n_k := n \cdot 1_k$, 则 $k = \{0_k, 1_k, \cdots, (q-1)_k\}$.)

注意：10.29 和 10.31 作业应于 10.31-11.5 期间提交

第十四次作业

10/31　第九周/星期四

92. (习题 6.1) 证明在群中
   (1) 元素 x 与它的逆的阶相同.
   (2) 元素 x 与它的共轭的阶相同.(x 与 y 在 G 中共轭 $\iff \exists g \in G, s.t. g^{-1}xg = y$)
   (3) 元素 xy 与 yx 的阶相同.
   (4) 元素 xyz 与 zyx 的阶不一定相同.

93. (习题 6.2) 证明 $\frac{3}{5} + \frac{4}{5}i \in \mathbb{C}^\times$ 的阶为无穷.

94. (习题 6.3) 设
$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$
   试求 A，B，AB 和 BA 在 $GL_2(\mathbb{R})$ 中的阶.

95. (习题 6.4) 证明群中元素 a 的阶 ≤ 2 当且仅当 $a = a^{-1}$.

96. (习题 6.5) 证明如果群 G 中任何元素的阶 ≤ 2，则 G 是阿贝尔群.

97. (习题 6.6) 设 x 在群中的阶是 n，求 $x^k (k \in \mathbb{Z})$ 的阶.

98. (选做) 设 p 是素数，试求 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ 有多少个 p 阶元？有多少个 p 阶子群？

99. (选做) 给出 $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$ 为循环群的充要条件.

注意：10.29 和 10.31 作业应于 10.31-11.5 期间提交

第十五次作业

11/5　第十周/星期二

100. (1) 记 $G = \left\langle \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Q})$. 求群 G 所有子群.

(2) 记 $G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{Q})$. 求群 G 所有子群.

101. (习题 6.10) 设 p 为奇素数, X 为 2 阶整系数矩阵，而 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. 如果 $I + pX \in \mathrm{SL}_2(\mathbb{Z})$ 的阶有限, 证明 $X = 0$.

102. (习题 6.12) 设 $G = \langle g \rangle$ 为 n 阶循环群. 证明: 元素 g^k 与 g^l 有相同的阶当且仅当 $\gcd(k, n) = \gcd(l, n)$.

103. (习题 6.13) 设 $G = \langle g \rangle$ 为 100 阶循环群. 试求

(1)　所有满足 $a^{20} = 1$ 的元素 a.

(2)　所有阶为 20 的元素 a.

104. (习题 6.21) $S^1 = (\{z \in \mathbb{C} \mid |z| = 1\}, \cdot)$ 的任意有限子群均为循环群.

105. 设 G_1 和 G_2 为两群. 设 $\varphi_i \colon G_i \to G_i$ 为 G_i 的自同构 $(i = 1, 2)$. 证明

$$\varphi_1 \times \varphi_2 \colon G_1 \times G_2 \to G_1 \times G_2, \quad (g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))$$

为群 $G_1 \times G_2$ 的自同构, 且

$$\psi \colon \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \to \mathrm{Aut}(G_1 \times G_2), \quad (\varphi_1, \varphi_2) \mapsto \varphi_1 \times \varphi_2 \qquad (*)$$

为群的单同态.

106. 设 p, q 为两不同的素数. 令 $G_1 = \mathbb{Z}/p\mathbb{Z}$, $G_2 = \mathbb{Z}/q\mathbb{Z}$.

(1)　求 $G = G_1 \times G_2$ 所有生成元.

(2)　写出 G 的所有子群.

(3)　证明此时, $(*)$ 中定义的 ψ 为同构.

107. (选做) 设 p 为素数. 令 $G_1 = G_2 = \mathbb{Z}/p\mathbb{Z}$.

(1) 写出 $G = G_1 \times G_2$ 的所有子群.

(2) 证明此时, $(*)$ 中定义的 ψ 为不是同构.

108. (选做) (习题 6.9) 设 m 是奇正整数且不是素数幂次.

(1) 求 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中 2 阶元的个数.

(2) 证明

$$\prod_{g \in (\mathbb{Z}/m\mathbb{Z})^\times} g = 1$$

(提示: 习题 6.7,6.8)

注意: 11.5 和 11.7 作业应于 11.7-11.12 期间提交

第十六次作业

11/7　第十周/星期四

109. 已知 $(\mathbb{Z}/17\mathbb{Z})^*$ 为循环群, $\overline{3}$ 为其生成元:

(1) 写出对数表:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^k	$\overline{1}$	$\overline{3}$														

(2) 利用对数表求解同余方程: $10^x \equiv 5 (\mathrm{mod}\ 17)$.

(3) 利用对数表求解同余方程: $x^6 \equiv 2 (\mathrm{mod}\ 17)$.

110. 利用中国剩余定理将

$$(\mathbb{Z}/(2^3 \times 5 \times 7)\mathbb{Z}) \times (\mathbb{Z}/(2 \times 7^2)\mathbb{Z}) \times (\mathbb{Z}/(5 \times 11)\mathbb{Z})$$

化为标准形式.

以下题目选做. 按如下的步骤证明有限交换群的结构定理

111. 设 G 为有限交换群. p 为素数.

(1) $G(p) := \{g \in G \mid \exists k \in \mathbb{N}, \text{s.t. } g^{p^k} = 1_G\}$ 为 G 的子群.

(2) 集合 $\{\text{素数 } p \mid \exists g \in G, \text{s.t. } p \mid \mathrm{ord}(g)\}$ 为有限集. 记为 $\{p_1, p_2, \cdots, p_s\}$.

(3) 映射

$$\begin{aligned} \varphi : G(p_1) \times G(p_2) \times \cdots \times G(p_s) &\longrightarrow G \\ (g_1, g_2, \cdots, g_s) &\longmapsto g_1 g_2 \cdots g_s \end{aligned}$$

为群同态.

(4) φ 为单同态 (提示: 设 $\varphi(g_1, \cdots, g_s) = 1$, 其中 $g_i^{p_i^{\alpha_i}} = 1_G$, 取 M_i 满足 $M_i \equiv 1 (\mathrm{mod}\ p_i^{\alpha_i}), M_i \equiv 0 (\mathrm{mod}\ p_j^{\alpha_j}) (\forall j \neq i)$, 则 $1_G = \varphi((g_1 \cdots g_s)^{M_i} = g_i)$

(5) φ 为满同态. (提示: 设 $g \in G$, $n = \mathrm{ord}(g) = p_1^{\alpha_1} \cdots p_s^{\alpha_s} (\alpha_i \geq 0)$, $n_i := n/p_i^{\alpha_i}$, 则 $\gcd(n_1, \cdots, n_s) = 1 \Longrightarrow \exists x_1, \cdots, x_s, \text{s.t. } \sum_i n_i x_i = 1, g = \prod_i (g^{n_i})^{x_i})$

112. 设 G 为有限交换群, p 为素数, 若 $G=G(p)$, 设 g_0 为 G 中一个阶数最大的元素, 即 $p^\alpha=\operatorname{ord}(g_0)=\max_{g\in G}\operatorname{ord}(g)$. 则存在 $H_0\leq G$ 使得映射

$$\begin{aligned}\varphi:\langle g_0\rangle\times H_0&\longrightarrow G\\(g_0^i,h)&\longmapsto g_0^ih\end{aligned}$$

为群同构. 请按如下步骤完成证明:

取 H_0 为 $\Sigma:=\{H\leq G\mid\langle g_0\rangle\cap H=\{1_G\}\}$ 中阶数最大的一个子群, 并如上面构造映射 φ.

(1) 验证 φ 为群的单同态.

(2) $\forall g\in G,g^{p^\alpha}=1_G$.

(3) 若 $g^p\in\operatorname{Im}\varphi$, 则存在 $i\in\mathbb{Z}$, s.t. $(gg_0^i)^p\in H_0$. (提示: 若 $g^p=g_0^kh_0$, 则 $p\mid k$,$(gg_0^{-\frac{k}{p}})^p=h_0\in H)$

(4) 若 $((gg_0)^i)^p\in H_0$, 则 $g\in\operatorname{Im}\varphi$.(提示: 否则 $\langle gg_0^i\rangle\cdot H_0\notin\Sigma\implies\exists h\in H_0,j,l,\text{s.t. }g_0^j=(gg_0^i)^l\cdot h\neq 1_G\implies p\nmid l\implies g=g_0^{-i}(g_0^jh^{-1})^{l'}\in\operatorname{Im}\varphi$, 其中 $ll'\equiv 1(\operatorname{mod}p^\alpha)$)

(5) 结合 (2)(3)(4), 说明 φ 为满射.

注意：11.5 和 11.7 作业应于 11.7-11.12 期间提交

代数学基础作业

中国科学技术大学
2024 秋　杨金榜
陈鉴 & 王子涵 & 辛雨 & 张煜星

第十七次作业

11/19　第十二周/星期二

113. 证明阶 ≤ 5 的群都是阿贝尔群.

114. 在同构意义下确定所有的 4 阶群.

115. 设 g_1, g_2 是群 G 的元素，H_1, H_2 是 G 的子群，证明下列两条等价：

   1) $g_1H_1 \subseteq g_2H_2$;

   2) $H_1 \subseteq H_2$ 且 $g_2^{-1}g_1 \in H_2$.

116. 设 g_1, g_2 是群 G 的元素，H_1, H_2 是 G 的子群。证明如果 $g_1H_1 \cap g_2H_2 \neq \varnothing$, 则它是关于子群 $H_1 \cap H_2$ 的左陪集.

117. 如果 H 与 K 是 G 的子群且阶互素，证明 $H \cap K = \{1\}$.

118. 设 $G = \bigsqcup_{i\in I} a_iH$, 对每个 i, 取 $s_i \in a_iH$. 证明:$S = \{s_i | i \in I\}$ 为左陪集代表元系，即 $G = \bigsqcup_{i\in I} s_iH$.

119. 若 $aH = Hb$, 则 $aH = Ha = bH = Hb$.

120. (选做) $A = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$, 其中 $2 \leq m_1 \mid m_2 \cdots \mid m_n$,
$A[d] := \{a \in A | da = 0\}$, 证明：

   (1) $A[d]$ 为 A 的子群;

   (2) $\#A[d] = \prod_{i=1}^{n} gcd(d, m_i)$;

   (3) 若 $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \cong \mathbb{Z}/m_1'\mathbb{Z} \times \cdots \times \mathbb{Z}/m_{n'}'\mathbb{Z}$, 其中 $2 \leq m_1 \mid m_2 \cdots \mid m_n, 2 \leq m_1' \mid m_2' \cdots \mid m_{n'}'$. 则 $n = n'$ 且 $m_i = m_i'(\forall i = 1, \cdots, n)$.
   (提示: $A \cong A' \Rightarrow \#A[d] = \#A'[d](\forall d)$)

注意：11.19 和 11.21 作业应于 11.21-11.26 期间提交

第十八次作业

11/21　第十二周/星期四

121. 设 $\varphi : G \to G'$ 为群同态:, 若 $N' \lhd G'$, 则 $\varphi^{-1}(N') \lhd G$.

122. 设 $H \leq G, N \lhd G$, 则 $HN := \{hn|h \in H, n \in N\}$ 为 G 的子群.

123. 请给出 $X = \{A, B, C\}$ 上的所有等价关系.

124. 请证明等价关系中的 3 条公理相互独立, 即

   1) 存在关系满足自反性、对称性，但不满足传递性；
   2) 存在关系满足自反性、传递性，但不满足对称性；
   3) 存在关系满足对称性、传递性，但不满足自反性.

125. (1) 设 $f : X \to Y$ 为集合之间的映射, 则 $\mathcal{R}_f := \{(x_1, x_2)|f(x_1) = f(x_2)\}$ 为 X 上的等价关系.

   (2) 若 $\mathcal{R}$ 为 X 上等价关系, 则存在映射 $g : X \to Y$ 使得 $\mathcal{R} = \mathcal{R}_g$.

126. (选做) 若 $H \lhd G$, 则

   (a) $(G/H, \cdot)$ 构成群;
   (b) $\varphi : G \to G/H, g \mapsto gH$ 为群的满同态;
   (c) $\ker \varphi = H$.

127. (选做) 若 $\varphi : G \to G'$ 为群同态，则 $\mathrm{im}\, \varphi \cong G/\ker \varphi$.

128. (选做) 设 R 为环，$I \lhd R$ 为理想，则

   (a) $(R/I, +, \cdot)$ 构成环;
   (b) $\varphi : R \to R/I, r \mapsto r + I$ 为环的满同态;
   (c) $\ker \varphi = I$.

129. (选做) 若 $\varphi : R \to R'$ 为环同态，则 $\mathrm{im}\, \varphi \cong R/\ker \varphi$.

130. (选做)设 R 为整环, 在

$$R\times R\backslash\{0\}=\{(p,q)|p\in R,q\in R\backslash\{0\}\}$$

上定义关系

$$(p,q)\sim(s.t)\overset{def}{\Leftrightarrow}pt=sq$$

(a) 证明"$\sim$" 为 $R\times R\backslash\{0\}$ 上的等价关系.

(b) 记

$$\frac{p}{q}:=\{(s,t)|(s,t)\sim(p,q)\}$$

$$Frac(R):=\{\frac{p}{q}|p\in R,q\in R\backslash\{0\}\}$$

证明: $\begin{cases}\frac{p}{q}+\frac{s}{t}:=\frac{pt+sq}{qt}\\ \frac{p}{q}\cdot\frac{s}{t}:=\frac{ps}{qt}\end{cases}$ 是良定义的.

(c) 证明: $(Frac(R),+,\cdot)$ 构成域.

(d) 证明: $\varphi:R\to Frac(R),r\mapsto\frac{r}{1}$ 为环的单同态.

注意: 11.19 和 11.21 作业应于 11.21-11.26 期间提交

第十九次作业

11/26　第十三周/星期二

定义　若 $(\mathbb{Z}/m\mathbb{Z})^\times$ 循环，且 $g \bmod m$ 生成 $(\mathbb{Z}/m\mathbb{Z})^\times$, 则称 g 为模 m 的一个原根.

131. 设 p 是奇素数. 证明：模 p 的任意两个原根之积不是模 p 的原根.

132. 设 p 是奇素数，对于任意的 $0 \le i \le p-2$，证明都有 $\sum\limits_{x=1}^{p} x^i \equiv 0 \mod p$ 成立

133. 设 n, a 都是正整数且 $a > 1$, 试求 a 在群 $(\mathbb{Z}/(a^n-1)\mathbb{Z})^\times$ 的阶, 并证明:$n \mid \varphi(a^n-1)$.

134. 设 m 是正整数. 整数 a 和 b 对于模 m 的阶分别是 s 及 t, 且 $(s,t)=1$. 证明:ab 模 m 的阶是 st.

135. (1) 对 $p = 3, 5, 7, 11, 13, 17, 19, 23$, 求模 p 的最小正原根（直接给出答案即可）;

     (2) 求模 11 的所有原根（需要计算过程）

136. 设 $\varphi : G \twoheadrightarrow H$ 为群的满同态. 证明: 若 G 为循环群, 则 H 也为循环群.

137. 设 G 是一个 n 阶有限群，若对任一 n 的正因子 m，G 中至多只有一个 m 阶子群，证明 G 是循环群

138. （选做）设 G 为有限阿贝尔群，取正整数 d 满足 $d||G|$，证明 G 中有一个 d 阶子群

注意：11.26 和 11.28 作业应于 11.28-12.3 期间提交

第二十次作业

11/28　第十三周/星期四

139. (1) 求模 11^{101} 的一个原根（要求计算过程）

(2) 求模 18 的所有原根（要求计算过程）

140. 设 p 是奇素数, 假设存在数 $a, p \nmid a$, 使得对 $p-1$ 的所有素因子 q, 有 $a^{(p-1)/q} \not\equiv 1\ (mod\ p)$, 证明：$a$ 是模 p 的原根.

141. 设 p 与 $q = 2p+1$ 都是素数时. 证明

(1) 当 $p \equiv 1\ (mod\ 4)$ 时，2 是模 q 的原根;

(2) 当 $p \equiv 3\ (mod\ 4)$ 时，-2 是模 q 的原根.

142. 给定义奇素数 p，求所有 $\mathbb{Z} \to \mathbb{Z}$ 的函数 f，满足对任意的整数 m, n 都有 $f(mn) = f(m)f(n)$，以及如果 $m \equiv n \mod p$，则有 $f(m) = f(n)$.

143. 设 $n > 1$ 是正整数，证明下述命题等价：

(1) 对任意的非零自然数 a，都有 $n|(a^n - a)$

(2) 对 n 的任一素因子 p，都有 p 恰好整除 n 且 $(p-1)|(n-1)$

144. (选做) 证明：群 G 是循环群当且仅当 G 的任一子群都形如 $G^m = \{g^m | g \in G\}$，其中 m 是非负整数。
(提示：分 G 中有无限阶元和仅有限阶元的情况讨论，并且可以知道在后者情况下 G 的所有元素的阶构成的集合是有限集)

注意：11.26 和 11.28 作业应于 11.28-12.3 期间提交

第二十一次作业

12/3　第十四周/星期二

145. 计算 $(\frac{17}{23}),(\frac{19}{37}),(\frac{60}{79}),(\frac{92}{101})$.

146. (1) 确定以 -3 为二次剩余的素数;

(2) 确定以 5 为二次剩余的素数.

147. 设 $p=4k+1$ 是素数，a 是 k 的因子，证明 $(\frac{a}{p})=1$.

148. 设 p 是素数，$p\equiv 1\ (mod\ 4)$，证明：

(1) $\sum\limits_{\substack{r=1\\(\frac{r}{p})=1}}^{p-1} r=\frac{p(p-1)}{4}$;

(2) $\sum\limits_{a=1}^{p-1} a(\frac{a}{p})=0$;

(3) $\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{k^2}{p}]=\frac{(p-1)(p-5)}{24}$.

(提示：$(\frac{p-r}{p})=(\frac{-1}{p})(\frac{r}{p})$，然后利用带余除法 $k^2=[\frac{k^2}{p}]p+r_k$)

149. 设 p 是素数，$p\equiv 3\ (mod\ 4)$，且 $p>3$, 证明：

(1) $\sum\limits_{\substack{r=1\\(\frac{r}{p})=1}}^{p-1} r\equiv 0\ (mod\ p)$;

(2) $\sum\limits_{a=1}^{p-1} a(\frac{a}{p})\equiv 0\ (mod\ p)$.

(提示：注意到 $\sum\limits_{\substack{r=1\\(\frac{r}{p})=1}}^{p-1} r\equiv\sum\limits_{k=1}^{\frac{p-1}{2}}k^2\ (mod\ p)$)

150. 设 $n>1$，$p=2^n+1$ 是素数。证明：模 p 的原根集合与模 p 的二次非剩余集合相同；进而证明 $3,7$ 都是模 p 的原根.

151. 设 p 是奇素数,a 是整数.

(1) 证明: 同余方程 $x^2 - y^2 \equiv a \ (mod\ p)$ 必有解;

(2) 若 (x, y) 和 (x', y') 均是上述同余方程的解, 当 $x \equiv x'$ 且 $y \equiv y' \ (mod\ p)$ 时, 我们将 (x, y) 和 (x', y') 看成模 p 的同一个解. 证明: (1) 中同余方程的解数是 $p-1$(如果 $p \nmid a$) 或 $2p-1$(如果 $p \mid a$).

(提示: 考虑集合 $A = \{k^2\} \subset \mathbb{F}_p$ 与集合 $B = \{k^2 + a\} \subset \mathbb{F}_p$; 第二问考虑分解 $x^2 - y^2 = (x+y)(x-y)$ 并利用原根)

注意: 12.3 和 12.5 作业应于 12.5-12.10 期间提交

代数学基础作业

中国科学技术大学
2024 秋　杨金榜
陈鉴 & 王子涵 & 辛雨 & 张煜星

第二十二次作业

12/5　第十四周/星期四

152. 求所有的素数 p 使得 x^2-15 在 $\mathbb{F}_p[x]$ 中可约.

153. 设 a 是奇数，则有：

    (1) $x^2 \equiv a \mod 2$ 对所有 a 都有解；

    (2) $x^2 \equiv a \mod 4$ 有解的充要条件是 $a \equiv 1 \mod 4$，并且在此条件满足时有两个不同的解;

    (3) $x^2 \equiv a \mod 2^k (k \geq 3)$ 有解的充要条件是 $a \equiv 1 \mod 8$，并且在此条件成立时恰有四个解：如果 x_0 是一个解，则 $\pm x_0, \pm x_0 + 2^{k-1}$ 是所有解.

154. 设 p 是奇素数, 证明:$\mathbb{F}_p[x]$ 中形如 $x^2+\alpha x+\beta$ 的二次多项式中, 共有 $\frac{p(p-1)}{2}$ 个不可约多项式. (提示：$x^2+\alpha x+\beta=(x+2^{-1}\alpha)^2+\beta-4^{-1}\alpha^2$，对 $(\frac{\beta}{p})$ 进行分类讨论并运用 151 题结论)

155. 设 p 是奇素数,$f(x)=ax^2+bx+c$ 且 $p \nmid a$. 记

$$D=b^2-4ac.$$

证明

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

156. 设 $\mathbb{F}$ 是域，$a \in \mathbb{F}$，在多项式环 $\mathbb{F}[x]$ 上证明：

    (1) 若 n 是正整数，则 $x-a \mid x^n-a^n$;

    (2) 若 n 是正奇数，则 $x+a \mid x^n+a^n$.

注意：12.3 和 12.5 作业应于 12.5-12.10 期间提交

第二十三次作业

12/10　第十五周/星期二

157. 对于下面的情形, 用欧几里得算法求 $(f(x), g(x))$:

 (1) $F=\mathbb{Q}, f(x)=x^3+x-1, g(x)=x^2+1$;

 (2) $F=\mathbb{F}_2, f(x)=x^7+\overline{1}, g(x)=x^6+x^5+x^4+\overline{1}$;

 (3) $F=\mathbb{F}_3, f(x)=x^8+\overline{2}x^5+x^3+\overline{1}, g(x)=\overline{2}x^6+x^5+\overline{2}x^3+\overline{2}x^2+\overline{2}$.

158. 设 m,n 是正整数, 证明: $F[x]$ 上多项式 x^m-1 和 x^n-1 的最大公因数是 $x^{(m,n)}-1$.

159. 设 $f(x), g(x) \in F[x]$, 且 $f(x)$ 与 $g(x)$ 互素, 则对任意正整数 n, $f(x^n)$ 与 $g(x^n)$ 也互素.

160. (1) 求有理系数多项式 $\alpha(x), \beta(x)$ 使 $x^3\alpha(x)+(1-x)^2\beta(x)=1$;

 (2) 更一般地, 对于正整数 m,n, 求有理系数多项式 $u(x), v(x)$ 使 $x^m u(x)+(1-x)^n v(x)=1$.

161. 设 f 和 g 都是 $F[x]$ 中次数至少为 1 的多项式, 且不存在 $u \in F$, 使得 $f=ug$. 设 $d(x)$ 是 $u(x)$ 与 $V(x)$ 的最大公因子. 证明:

 (1) 存在多项式 $u(x), v(x)$, 使得 $\deg u(x) < \deg g(x) - \deg d(x)$ 且 $d(x) = f(x)u(x)+g(x)v(x)$;

 (2) 此时 $\deg v(x) < \deg f(x) - \deg d(x)$;

 (3) 符合 (a) 中条件的多项式 $u(x), v(x)$ 是唯一确定的.

162. 设 $f(x), g(x) \in F[x]$ 满足 $g(x) \neq 0$. 则 $\frac{f(x)}{g(x)} \in F(x)$, 其中 $F(x)$ 为 F 上有理函数域. 下面对于形式分式的计算都是在分式域上进行. 则:

 (1) 设 $g(x)=a(x)b(x)$, 其中 $a(x)$ 与 $b(x)$ 互素且均非常数; 假设 $\deg f < \deg g$, 则存在唯一确定的 $r(x), s(x) \in F[x]$, $\deg r < \deg a$, $\deg s < \deg b$, 使得 $\frac{f(x)}{g(x)} = \frac{r(x)}{a(x)} + \frac{s(x)}{b(x)}$;

(2) 设 $g(x)$ 为首项系数为 1, 其标准分解是 $g(x)=\prod\limits_{i=1}^{l} p_i^{m_i}(x)$. 假设 $\deg f<\deg g$, 则存在唯一确定的多项式 $h_i(x)\in F[x], \deg h_i<m_i\deg p_i (1\le i\le l)$, 使得 $\frac{f(x)}{g(x)}=\frac{h_1(x)}{p_1^{m_1}(x)}+\cdots+\frac{h_l(x)}{p_l^{m_l}(x)}$;

(3) 设 $p(x)\in F[x]$ 是不可约多项式, m 是正整数. 则对于任意 $h(x)\in F[x]$, 若 $h(x)\neq 0$ 且 $\deg h<m\deg p$, 则存在唯一确定的多项式 $\alpha_i(x)\in F[x](1\le i\le m)$ 使得 $\frac{h(x)}{p^m(x)}=\frac{\alpha_m(x)}{p(x)}+\cdots+\frac{\alpha_1(x)}{p^m(x)}$, 其中 $\deg\alpha_i<\deg p$;

(4) 证明: 每一个分子的次数小于分母的次数, 且分母有标准分解 $f(x)=p_1^{m_1}(x)\cdots p_l^{m_l}(x)$ 的有理分式 $\frac{g(x)}{f(x)}$ 是部分分式的和, 每个部分分式的分母是 $p_i^{k_i}(x)(k_i=1,\cdots,m_i; i=1,\cdots,l)$, 而分子次数小于 $\deg p_i$.

注意：12.10 和 12.12 作业应于 12.12-12.17 期间提交

第二十四次作业

12/12　第十五周/星期四

163. 确定 $\mathbb{F}_2[x]$ 与 $\mathbb{F}_3[x]$ 中所有 2 次及 3 次的首项系数为 1 的不可约多项式.

164. 设直线 $y = ax + b$ 交曲线 $y^2 = x^3 + cx + d$ 于两点 $(x_1, y_1), (x_2, y_2)$. 试用 x_1, y_1, x_2, y_2 表示 a, b, c 和 d.

165. 设 $f(x) \in \mathbb{F}_p[x], \deg f = p - 2$. 若对所有 $\alpha \in \mathbb{F}_p(\alpha \neq 0)$ 有 $f(\alpha) = \alpha^{-1}$, 试确定 $f(x)$.

166. 令分圆多项式 $\Phi_n(x) = \prod_{k=1,(k,n)=1}^{n}(x - \zeta_n^k)$. 证明:
(1) $\prod_{1 \leq d | n} \Phi_d(x) = x^n - 1$.
(2) 如果 n 为大于 1 的奇数, 则 $\Phi_{2n}(x) = \Phi_n(-x)$.
(3) $\Phi_n(x) = \prod_{1 \leq d | n}(x^d - 1)^{\mu(\frac{n}{d})}$, 其中 μ 为莫比乌斯函数.
(注: 关于莫比乌斯函数的定义参考习题 67 和 68, 允许不加证明地使用这两题中的结论)

167. 设 F 为 F' 的子域, $f(x), g(x) \in F[x]$. 证明
1) f 在 $F[x]$ 中整除 g 当且仅当 f 在 $F'[x]$ 中整除 g;
2) f 与 g 在 $F[x]$ 中互素当且仅当 f 与 g 在 $F'[x]$ 中互素.

以下题目选做.

168. 设 p 为素数, n 为正整数, F 为 p^n 元域.
(1) 证明: $F^\times$ 为 $p^n - 1$ 循环群. (提示: 与 $n = 1$ 时相似)
(2) d 为正整数, $d|n$, 则 $E := \{\alpha \in F | \alpha^{p^d} = \alpha\}$ 构成 F 的子域. (提示: 在 F 上 $(\alpha + \beta)^p = \alpha^p + \beta^p$)

169. 设 f 为 $\mathbb{F}_p[x]$ 中 d 次首一不可约多项式, 则 $f | x^{p^n} - x \iff d|n$.
(提示: (右推左) 记 $F' = \mathbb{F}_p[x]/f\mathbb{F}_p[x] \implies \overline{x} \in F'$ 为 $f(x) \in F'[x]$ 的根 $\implies f$ 与 $x^{p^d} - x$ 在 $F'[x]$ 中不互素

(左推右) $d' := \gcd(n,d) \implies f|\gcd(x^{p^n}-x, x^{p^d}-x) = x^{p^{d'}}-x \implies \overline{x} \in E := \{\alpha \in F' | \alpha^{p^{d'}}\} \implies F' \subset E \implies p^d \leq p^{d'}$)

注意：12.10 和 12.12 作业应于 12.12-12.17 期间提交

代数学基础作业
中国科学技术大学
2024 秋　杨金榜
陈鉴 & 王子涵 & 辛雨 & 张煜星

第二十五次作业

12/17　第十六周/星期二

170. (习题 5.8) 设 $f(x)$ 是实系数多项式，$a \in \mathbb{R}$, 试决定 a 在下述多项式的零点重数：

   (a) $f(x) - f(a) - f'(a)(x-a) - \frac{f''(a)}{2}(x-a)^2$;

   (b) $f(x) - f(a) - \frac{x-a}{2}(f'(x) + f'(a))$.

171. (习题 5.9) 证明多项式 $f(x) = \sum_{k=0}^{n} \frac{x^k}{k!}$ 无重根.

172. (习题 5.10) 证明 1 是多项式 $x^{2n} - nx^{n+1} + nx^{n-1} - 1$ 的 3 重零点，其中 $n \geq 2$.

173. (习题 5.11) 设 $f(x) \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上不可约，证明它一定没有多重的复根.

174. 请在 $\mathbb{R}[x]$ 中分解多项式 $x^5 + 1$ 和 $x^5 - 2$.

175. 设 $f(x) \in \mathbb{Z}[x]$，且 $f(0) \equiv f(1) \equiv 1\ (mod\ 2)$，证明：$f(x)$ 没有整数根.

176. (选做) 设 $\mathbb{F} = \mathbb{F}_p, n \geq 1$,

   (a) 证明
   $$x^{p^n} - x = \prod_{P(x):\text{首一不可约},\deg P|n} P(x)$$

   (b) 证明在 $\mathbb{F}[x]$ 中存在 n 次不可约多项式.
   (提示：即证明 n 次不可约多项式个数大于 0)

注意：12.17 和 12.19 作业应于 12.19-12.24 期间提交

第二十六次作业

12/19　第十六周/星期四

177. 在相应的环中判定不可约性

    1) $2x^3 + 3x + 1 \in \mathbb{Z}[x]$

    2) $2x^5 + 30x + 90 \in \mathbb{Q}[x]$

    3) $x^4 - x^3 - 3x^2 + 8x + 1 \in \mathbb{Z}[x]$

178. 设 $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ 为本原多项式. 设 p 为素数, 若 $p \nmid a_0, p|a_1, \cdots, p|a_{n-1}, p||a_n$, 证明 f 在 $\mathbb{Z}[x]$ 中不可约.

179. 证明:

    1) 设 $f \in \mathbb{Z}[x]$ 为本原多项式,p 为素数, 若 f 的首项系数不被 p 整除, 且 $f \ mod\ p$ 在 $\mathbb{F}_p[x]$ 中不可约, 则 f 在 $\mathbb{Z}[x]$ 中不可约.

    2) $x^4 + x + 1$ 在 $\mathbb{F}_2[x]$ 中不可约.

    3) $x^4 + 3x + 5$ 在 $\mathbb{Z}[x]$ 中不可约.

180. 设 $n > 1$ 是正整数, 证明: 如果 $x^{n-1} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约, 则 n 是素数.

181. 设 $a_1, \cdots, a_n$ 是互不相同的整数, 证明:$(x - a_1) \cdots (x - a_n) - 1$ 在 $\mathbb{Q}[x]$ 中不可约. (提示: 若 $(x - a_1) \cdots (x - a_n) - 1 = h(x)g(x)$, 则 $a_1, \cdots, a_n$ 为 $h^2 - 1$ 和 $g^2 - 1$ 的根)

182. 对 $f(x) \in \mathbb{Z}[x]$ 且 $f(x) \neq 0$, 用 $c(f)$ 表示 $f(x)$ 的容度.

    (1) 对任意 $a \in \mathbb{Z}, a \neq 0$, 证明: $|c(af)| = |a \cdot c(f)|$;

    (2) 证明 $|c(fg)| = |c(f) \cdot c(g)|$.

183. 设 $f(x)$ 是本原多项式,$g(x) \in \mathbb{Q}[x]$, 且 $f(x)g(x) \in \mathbb{Z}[x]$, 则 $g(x) \in \mathbb{Z}[x]$.

184. 设 $p(x) \in \mathbb{Z}[x]$ 是本原的不可约多项式, 证明: 对 $f(x), g(x) \in \mathbb{Z}[x]$, 若 $p(x)|f(x)g(x)$, 则 $p(x)|f(x)$ 或 $p(x)|g(x)$.

注意: 12.17 和 12.19 作业应于 12.19-12.24 期间提交

第二十七次作业

12/24　第十七周/星期二

185. 把置换 $\sigma = (456)(567)(761)$ 写成不相交轮换的积

186. 计算置换的乘积，并求乘积的阶：

    (1) $[(135)(2467)]\cdot[(147)(2356)]$

    (2) $[(13)(57)(246)]\cdot[(135)(24)(67)]$

187. 讨论置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$ 的奇偶性

188. 证明 $S_n(n \geq 3)$ 中的偶置换均为 3 轮换之积

189. 证明 S_n 中奇置换的阶一定是偶数

190. 证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $\frac{n!}{\prod_{i=1}^{n}\lambda_i! i^{\lambda_i}}$ 个. 由此来证明：

$$\sum_{\lambda_i \geq 0, \lambda_1+2\lambda_2+\cdots+n\lambda_n=n} \frac{1}{\prod_{i=1}^{n}\lambda_i! i^{\lambda_i}} = 1$$

.

191. 当 $n \geq 2$ 时，证明：(12) 和 $(123\cdots n)$ 是 S_n 的一组生成元.

注意：12.24 和 12.26 作业应于 12.26-12.31 期间提交

第二十八次作业

12/26　第十七周/星期四

192. 设置换 $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ 的交错数为 k，求置换 $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$ 的交错数.

193. 考虑 S_n 中置换 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$，请问何时 σ 的交错数最大.

194. 给定四元多项式 f，令 $G_f = \{\sigma \in S_4 | (\sigma f)(x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4)\}$. 证明 G_f 是 S_4 的子群，并求下列给定 f 的 G_f:

   (1) $f = x_1x_2 + x_3x_4$;

   (2) $f = x_1x_2x_3x_4$.

195. 将下列对称多项式写成初等对称多项式的多项式：

   (1) $x_1^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3^2x_1 + x_2^2x_3 + x_3^2x_2$;

   (2) $x_1(x_2^3 + x_3^3) + x_2(x_1^3 + x_3^3) + x_3(x_1^3 + x_2^3)$.

196. 试求 $s_i(1, \zeta_n, \cdots, \zeta_n^{n-1})$，其中 s_i 为关于 $x_1, \cdots, x_n$ 的 i 次初等对称多项式，ζ_n 为 n 次单位根.

197. 取 $\alpha, \beta \in S_n$，证明：

   (1) $\alpha\beta\alpha^{-1}\beta^{-1} \in A_n$;

   (2) $\alpha\beta\alpha^{-1} \in A_n$ 当且仅当 $\beta \in A_n$.

198. 对于正整数 n，证明 $x^n + x^{-n}$ 是关于 $x + x^{-1}$ 的整系数多项式.

199. 多项式 $3x^3 + 2x^2 - 1$ 的根在 $\mathbb{C}$ 上有三个不同的根，设为 r_1, r_2, r_3. 求多项式 $f(x) \in \mathbb{Q}[x]$，使得它的根恰为 r_1^2, r_2^2, r_3^2.

200. (选做) 我们记 $t_k = \sum_{i=1}^{n} x_i^k (k \geq 1)$，特别地 $t_0 = n$，设 $f(x) = \prod_{i=1}^{n}(x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots + (-1)^n s_n$，证明下列等式：

   (a) 若 $k \leq n-1$，则 $t_k - t_{k-1}s_1 + t_{k-2}s_2 + \cdots + (-1)^{k-1}t_1s_{k-1} + (-1)^k k s_k = 0$;

   (b) 若 $k \geq n$，则 $t_k - t_{k-1}s_1 + t_{k-2}s_2 + \cdots + (-1)^n t_{k-n}s_n = 0$

注意：12.24 和 12.26 作业应于 12.26-12.31 期间提交