2023–2024 学年《代数学基础》期末考试

考试时间：2024 年 1 月 15 日 14:30–16:30，本卷共 100 分。

一、(10 分) 设 $f(x) = x^7 - x^5 + x^4 + x^2 + 1 \in \mathbb{F}_3[x]$，$g(x) = x^6 - x^3 - x^2 + 1 \in \mathbb{F}_3[x]$，求 $(f(x), g(x))$。

二、(15 分) 判断下面的说法是否正确，并简述理由或给出反例。

(a) 对于素数 p 和正整数 m，$(\mathbb{Z}/p^m\mathbb{Z})^*$ 是循环群。

(b) 对于素数 p，分圆多项式 $\Phi_p(x) = (x^p - 1)/(x - 1)$ 在 $\mathbb{Z}[x]$ 上不可约。

(c) 设 R 为含幺交换环，$f(x) \in R[x]$，且 $\deg(f(x)) = n$ 为正整数，则 $f(x)$ 在 R 上的零点个数小于等于 n。

三、(15 分) 设 $\sigma_1 = (137)(2465) \in S_7$，$\sigma_2 = (145)(2736) \in S_7$。

(a) 求 $\sigma = \sigma_1\sigma_2$ 的不相交轮换表示，并求 σ 的交错数。

(b) 求 σ_2, σ 的阶。

(c) σ_1, σ_2 是否共轭？为什么？

四、(10 分)

(a) 求模 121 的最小原根。

(b) 模 121 意义下有多少个两两互不同余的原根？

五、(10 分) 设 $f(x) = x^4 - x^3 - x^2 + 2x - 1$。

(a) 在 $\mathbb{Z}[x]$ 中对 $f(x)$ 作因式分解。

(b) 设 $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ 为 $f(x)$ 的四个根，求 $\sum_{i=1}^{4} \alpha_i^2$ 和 $\sum_{i=1}^{4} \alpha_i^{-1}$。

六、(10 分)

(a) 证明：$x^4 + x^3 + 1$ 在 $\mathbb{Z}[x]$ 中不可约。

(b) 是否存在 16 元有限域？若存在，给出一个构造。

七、(15 分)

(a) 计算勒让德记号 $\left(\dfrac{-654}{1823}\right)$。

(b) 求所有素数 p，使得 $x^2 + 15$ 在 $\mathbb{F}_p[x]$ 中不可约。

(c) 设素数 p 满足 $p \equiv 3 \pmod 4$。证明：$2p + 1$ 是素数当且仅当 $2^p \equiv 1 \pmod{2p+1}$。

八、(15 分) 设 R 为含幺交换环，$P \neq R$ 为一个真理想。称 P 为一个素理想，当且仅当对于任意的 a, b，若 $ab \in P$，则有 $a \in P$ 或 $b \in P$。

(a) 证明：P 是 R 的素理想当且仅当 R/P 是整环。

(b) 求 $\mathbb{Z}$ 的所有素理想。

(c) 设 p 为一个奇素数，是否 (x, p) 总是 $\mathbb{Z}[x]$ 中的一个素理想？

中国科学技术大学期中试卷 2023-2024年第一学期代数学基础 001356

W.Yang

2024 年 1 月 15 日

考试形式为闭卷。时间是2023年1月15日 14:30-16:30。授课教师为马立明/杨金榜。
第一部分我在考试之后整理重排的LaTeX试卷版本，第二部分是我自己撰写的答案。

1 考试试卷

Problem 1.1. （*10*分）设$f(x) = x^7 - x^5 + x^4 + x^2 + 1 \in \mathbb{F}_3[x]$ 和 $g(x) = x^6 - x^3 - x^2 + 1 \in \mathbb{F}_3[x]$. 求$f(x)$与$g(x)$的最大公因式$(f(x), g(x))$.[1]

Problem 1.2. （*15*分）判断下面的说法是否成立。正确，简要说明理由；错误，举出反例。

1. 设p为素数，m为正整数，则$(\mathbb{Z}/p^m\mathbb{Z})^*$为循环群。
2. 设p为素数，则分圆多项式$\Phi_p(x) = (x^p - 1)/(x - 1)$为$\mathbb{Z}[x]$中不可约多项式
3. 设R为含幺交换环，令$f(x) \in R[x]$，$\deg(f(x)) = n$为正整数，则$f(x)$在环R中的零点个数小于或等于n。

Problem 1.3. （*15*分）令置换$\sigma_1 = (137)(2465) \in S_7$和$\sigma_2 = (145)(2736) \in S_7$。计算或证明以下的结果：

1. 求$\sigma = \sigma_1\sigma_2$的不相交轮换表示及$\sigma$的逆序数（交错数）。
2. 求σ_2和σ的阶。
3. 置换σ_1与σ_2共轭呢？为什么？

Problem 1.4. （*10*分）

1. 求出模121最小的正原根。
2. 模121有多少个两两（模121）互不同余的原根？

Problem 1.5. （*10*分）设$f(x) = x^4 - x^3 - x^2 + 2x - 1 \in \mathbb{Z}[x]$，

1. 求$f(x)$在$\mathbb{Z}[x]$中不可约因式分解；
2. 设$\alpha_1, \alpha_2, \alpha_3, \alpha_4$为$f(x)$的四个根，求$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2$以及$\alpha_1^{-1} + \alpha_2^{-1} + \alpha_3^{-1} + \alpha_4^{-1}$。

Problem 1.6. （*10*分）

[1] 这里卷子上本来还有一题要求出Bezóut定理中的系数，后来在考试的时候说不用做此题，故不录入。

1. 证明$f(x)=x^4+x^3+1$是$\mathbb{Z}[x]$中不可约多项式。

2. 16元有限域是否存在？存在的话，请构造一个。

Problem 1.7. 1. 计算*Legendre*符号$(\frac{-654}{1823})$。

2. 求出所有的素数p使得$x^2+15\in F_p[x]$中不可约。

3. 设p为奇素数，$p\equiv 3 \pmod 4$。证明：$2p+1$是素数的充要条件为

$$2^p\equiv 1 \pmod{2p+1}.$$

Problem 1.8. （*15*分）设R为含幺交换环，R的真理想$\mathfrak{p}\neq R$叫做R的素理想，是指：对于任意$a,b\in R$，若$ab\in\mathfrak{p}$，则$a\in\mathfrak{p}$或$b\in\mathfrak{p}$。

1. 证明$\mathfrak{p}$是R的素理想当且仅当$R/\mathfrak{p}$是整环（没有非零零因子）。

2. 求出整数环$\mathbb{Z}$的所有素理想。

3. 整系数多项式环$\mathbb{Z}[x]$中由不定元x和奇素数p生成的理想(x,p)是素理想吗？为什么？

2 试题解答

Solution 2.1. 通过*Euclid*算法（或者你发明的任何有趣的算法）可以得到是$(x-1)$。

Solution 2.2. 1. 错误，取$p=2$，$m=3$，即考虑$(\mathbb{Z}/8\mathbb{Z})^*$，这是一个*Abel*群且含有四个元素$\overline{1},\overline{3},\overline{5},\overline{7}$.它们之间有乘法

$$\overline{1}^2=\overline{3}^2=\overline{5}^2=\overline{7}^2=\overline{1},$$
$$\overline{3}\cdot\overline{5}=\overline{7},\overline{3}\cdot\overline{7}=\overline{5},\overline{5}\cdot\overline{7}=\overline{3},$$

于是同构于*Klein*四元群C_2^2.

2. 正确。令$x=y+1$，得到

$$\Phi_p(y+1)=y^{p-1}+\binom{p}{1}y^{p-2}+\cdots+\binom{p}{p-2}y+\binom{p}{p-1}$$

最后一项的系数就是p，中间除了首项之外的所有系数被p整除，由*Eisenstein*判别法可得到结论。

能使用*Eisenstein*判别法是因为质数p在$\mathbb{Z}[\zeta]$中完全分歧，其中$\zeta^p=1$。我们有p在$\mathbb{Z}[\zeta]$中分解为$(1-\zeta)^{p-1}u$，其中u是一个单位元。

3. 错误。我们需要整环条件，当这个条件失效的时候我们给出两个反例。

   (a) 反例*1*：就选取$R=\mathbb{Z}/8\mathbb{Z}$，$f(x)=x^2-1$，根据第一小问我们知道$\overline{1},\overline{3},\overline{5},\overline{7}$均为零点。

   (b) 反例*2*：我们给出一个极为精彩的反例。选取$R=\widehat{\mathbb{Z}_{(10)}}$，即整数环$\mathbb{Z}$在理想$(10)$处的完备化。考虑$f(x)=x^2-x$。我们知道0和1是零点，但还有两个非平凡的零点分别是$\cdots109376$和$\cdots980625$.这就解释了我们为什么经常看到625的平方还是以625结尾。比如$0625^2=390625$.

   关于这个反例值得一提的是，注意到这里问题出在我们相当于想在这个环里面做类似开平方根的操作，但是这里面2是10的因子，所以我们会得到一些不太好的结果。我们也知道如果特征为p那么通常开p次方根不是一个好主意。

Solution 2.3. *1. (1642)(35)*。写开来不难得到逆序数是*8*.

2. 12, 4.

3. 共轭。因为S_n中两个元素共轭当且仅当它们的不相交轮换表示拥有同样的型。

Solution 2.4. *1. 2*，因为

$$2^{10} = 1024 \equiv 56 \pmod{121}.$$

2. 因为$(\mathbb{Z}/121\mathbb{Z})^* \simeq \mathbb{Z}/110\mathbb{Z}$，故原根数量为$\varphi(110) = \varphi(11)\varphi(5)\varphi(2) = 40$.

Solution 2.5. *1.* $f(x) = (x-1)(x^3 - x + 1)$。我们只需要证明$x^3 - x + 1$不可约。而这个方程是三次的，故没有有理根即没有一次因式就不可约。它的有理根只可能是± 1，代入后发现均不是。

2. 直接取$\alpha_4 = 1$.

根据*Vieta*定理，我们知道$\alpha_1 + \alpha_2 + \alpha_3 = 0, \alpha_1 \cdot \alpha_2 + \alpha_2 \cdot \alpha_3 + \alpha_1 \cdot \alpha_3 = -1, \alpha_1 \cdot \alpha_2 \cdot \alpha_3 = -1$.于是

$$\begin{aligned}\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2 \cdot (\alpha_1 \cdot \alpha_2 + \alpha_2 \cdot \alpha_3 + \alpha_1 \cdot \alpha_3) + 1 \\ &= 0 + 2 + 1 = 3. \\ \alpha_1^{-1} + \alpha_2^{-1} + \alpha_3^{-1} + \alpha_4^{-1} &= \frac{\alpha_1 \cdot \alpha_2 + \alpha_2 \cdot \alpha_3 + \alpha_1 \cdot \alpha_3}{\alpha_1 \cdot \alpha_2 \cdot \alpha_3} + 1 \\ &= 2.\end{aligned}$$

Solution 2.6. *1.* 模*2*约化，证明其在$\mathbb{F}_2[x]$上的不可约性（我们省略$\mathbb{F}_2$中上划线[2]）。我们知道这个四次方程要可约要么其有一次因式，要么为两个二次不可约因式值之积。但$f(0) = f(1) = 1 \in \mathbb{F}_2$，且$\mathbb{F}_2[x]$中唯一的二次不可约多项式为$x^2 + x + 1$，而其平方为$x^4 + x^2 + 1 \neq x^4 + x^3 + 1$，故得证。

2. 存在，就取$\mathbb{F}_{16} = \mathbb{F}_2[x]/(x^4 + x^3 + 1)$。

当然我们也可以用*Artin-Schreier*多项式$x^4 + x + 1$（这个多项式还跟*Hilbert 90*和一些特征p理论有关[3]），取$\mathbb{F}_{16} = \mathbb{F}_2[y]/(y^4 + y + 1)$。

这样得到的两个域（不典范地）同构。

为什么得到的是域呢？因为$\mathbb{F}_2[x]$是*PID*，所以其中的不可约多项式生成的理想均为极大的，商掉之后得到的就是一个域，并且是一个*4*维的$\mathbb{F}_2$-线性空间，故是一个16元域。

Solution 2.7. *1.* 给出两种做法。

[2]我本人不是很喜欢用上划线（上一题用只是为了区分原来的整数环和商环）。

[3]也正因如此，选取这类多项式在$\mathbb{F}_{p^p}$这一类域的构造中更为标准（因为简单）。

(a) 使用二次互反律。

$$\begin{aligned}(\frac{-654}{1823}) &= (\frac{-1}{1823})(\frac{2}{1823})(\frac{327}{1823})\\ &= (\frac{2150}{1823})(\frac{-1}{1823})(\frac{2}{1823})\\ &= (\frac{5}{1823})^2(\frac{2}{1823})^2(-1)(\frac{43}{1823})\\ &= (\frac{17}{43})\\ &= (\frac{60}{43})\\ &= (\frac{2}{43})^2(\frac{3}{43})(\frac{5}{43})\\ &= (\frac{43}{5})(\frac{43}{3})(-1)\\ &= (\frac{3}{5})(-1)\\ &= 1.\end{aligned}$$

(b) 使用广义二次互反律（*Jacobi*符号），避免大数分解的麻烦。

$$\begin{aligned}(\frac{-654}{1823}) &= (\frac{-1}{1823})(\frac{2}{1823})(\frac{327}{1823})\\ &= (\frac{1823}{327})\\ &= (\frac{188}{327})\\ &= (\frac{2}{327})^2(\frac{47}{327})\\ &= (\frac{327}{47})(-1)\\ &= (\frac{-1}{47})(\frac{2}{47})(-1)\\ &= 1.\end{aligned}$$

2. 首先排除$p = 2, 3, 5$的情形，下面假设$p \geq 7$.于是只需要-15不是二次剩余。即$(\frac{-1}{p})(\frac{3}{p})(\frac{5}{p}) = -1$. 然后进行**恶心**的分类讨论。

若$p \equiv 1 \pmod 4$，则$(\frac{-1}{p})(\frac{3}{p})(\frac{5}{p}) = (\frac{p}{3})(\frac{p}{5})$。若$p \equiv 3 \pmod 4$，则$(\frac{-1}{p})(\frac{3}{p})(\frac{5}{p}) = (\frac{p}{3})(\frac{p}{5})$。二者没有区别。

若$p \equiv 1, 4 \pmod 5$，那么$(\frac{p}{5}) = 1$.若$p \equiv 2, 3 \pmod 5$，那么$(\frac{p}{5}) = -1$.若$p \equiv 1 \pmod 3$，那么$(\frac{p}{3}) = 1$.若$p \equiv 2 \pmod 3$，那么$(\frac{p}{3}) = -1$.

最后使用中国剩余定理化简**更为恶心**，作者在此略去留给读者。

3. 若$2p+1$为素数，由*Euler*准则与二次互反律，并且$2p+1 \equiv 7 \pmod 8$，

$$2^p \equiv (\frac{2}{2p+1}) = 1 \pmod{2p+1}.$$

反过来，若$2p+1$不为素数，则存在奇素数q整除$2p+1$且q小于$2p+1$，于是$q < p$.

由*Fermat*小定理我们知道$2^{q-1} \equiv 1 \pmod{q}$，而$2^p \equiv 1 \pmod{q}$，故$2^{(q-1,p)} \equiv 1 \pmod{q}$，然而$p$为奇素数，所以$(q-1,p)$或者为1或者为$p$。而这不能是$p$否则与$q < p$矛盾。故为1，即$2 \equiv 1 \pmod{q}$，矛盾。故$2p+1$为素数。

或者注意到2的阶一定要整除$\varphi(2p+1)$和p，因此必须是p，为$\varphi(2p+1)$必须是偶数且小于等于$2p$，所以只能是$2p$，这就意味着$2p+1$为素数。

Solution 2.8. *1.* $\mathfrak{p}$是R的素理想 $\Leftrightarrow (xy \notin \mathfrak{p} \Rightarrow \overline{x} \notin \mathfrak{p}, \overline{y} \notin \mathfrak{p}) \Leftrightarrow (\overline{xy} \neq 0 \in R/\mathfrak{p} \Rightarrow \overline{x} \neq 0 \in R/\mathfrak{p}, \overline{y} \neq 0 \in R/\mathfrak{p}) \Leftrightarrow R/\mathfrak{p}$是整环。

2. 由于$\mathbb{Z}$为*PID*，且± 1为单位，所有理想形如(n)，$n \in \mathbb{Z}_{\geq 0}$.

$n = 0$时，$\mathbb{Z}/(0) = \mathbb{Z}$为整环，故为素理想。

$n = 1$时，(1)为单位理想为整个环，舍去。

$n \geq 2$时，若$n = pq$为非平凡分解，则$\overline{p} \cdot \overline{q} = \overline{0}$意味着$\mathbb{Z}/n\mathbb{Z}$不是整环。若$n$为素数$p$，那么$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$为域自然也是整环，实际上这些是极大理想。

综上，全部素理想为$(0), (p)$，其中p为$\mathbb{Z}$中的素数。（这也被称为环的素谱空间）

3. 事实上这甚至是一个极大理想。

$$\frac{\mathbb{Z}[x]}{(x,p)} = \frac{\mathbb{Z}}{(p)} = \mathbb{F}_p.$$

我们用到了第二同构定理，商两次可以分开进行。