中国科学技术大学数学科学学院

2022～2023 学年第2 学期期末考试试卷

□ A卷■　　B卷

课程名称 近世代数　　课程编号 001010

考试时间 2023年7月12日　　考试形式 闭卷

姓 名 _____　　学 号 _____　　学 院 _____

如果空间不够, 可以写在试卷(也是答题纸)的背面, 但是请务必用醒目的形式标识.

1. 判断题(30分) 如果结论正确请写"Y", 否则请写"N".

(1) 在一个群中两个正规子群的乘积是一个正规子群. Y

(2) 循环群的商群还是循环群. Y

(3) 如果一个群由有限个元素生成, 而且这些生成元都是有限阶的, 那么这个群一定是有限群. N

(4) 正交群$O(n,\mathbb{R})$(实数域上n阶正交矩阵集合)是一般线性群$GL(n,\mathbb{R})$(实数域上n阶可逆矩阵集合)的正规子群. N

(5) 12阶群一定是交换群. N

(6) 设R是区间$(0,1)$上的连续可积函数集合, 这个集合在函数的乘法和加法运算下构成一个环. Y or N. Riemann, Lesbegue..

(7) 在一个环中两个理想的交是一个理想. Y

(8) 设L/K是一个域扩张, $\alpha \in L$是K上的代数元, $f(x) \in K[x]$, 那么$f(\alpha)$是K上的代数元. Y

(9) 包含无穷多个元素的域特征为0. N

(10) 域的代数扩张一定是有限扩张. N

2. (30分) 简答题.

(1) 设R是唯一因式分解整环, 陈述判定$R[x]$中一个本原多项式不可约的Eisenstein (爱森斯坦因) 判别法.

设 $f = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$.

若存在 $p \in R$ 为素元, 且

$$\begin{cases} p \mid a_i & 1 \le i \le n \\ p^2 \nmid a_n \end{cases}$$

则 f 不可约.

(2) 构造有理数域$\mathbb{Q}$的一个5次扩域, 并简要解释其为什么符合要求.

令 $K = \mathbb{Q}[x]/(x^5-2)$

由 Eisenstein 判别法, x^5-2 在 $\mathbb{Q}$ 上不可约. (及 Gauss 引理)

进而 K 为 $\mathbb{Q}$ 的5次扩域 ($1, x, x^2, x^3, x^4$ 为基).

(3) 写出S_5中两个6阶子群, 一个是交换的, 一个是非交换的.

交换的: $\langle (12), (345) \rangle$

非交换的: $\{\sigma \in S_5, \sigma(4)=4, \sigma(5)=5\} \cong S_3$.

(4) 写出$\sqrt{2}+\sqrt{3}$分别在域$\mathbb{Q}$上和域$\mathbb{Q}[\sqrt{6}]$上的极小多项式.

$\mathbb{Q}$上：$X^4-10X^2+1=0$

$\mathbb{Q}[\sqrt{6}]$上：$X^2-5-2\sqrt{6}=0$

(5) 求正整数$k<17$使得$20^{17}\equiv k \pmod{17}$, 并用群的观点简要解释.

$k=3$. $(\mathbb{F}_{17})^\times$是16阶循环群, 故 $\overline{20}^{17}=\overline{20}=\overline{3}$

(6) 设K是域, x是一个未定元, 视$K(x^2+x+1)$为$K(x)$的子域. 请问$K(x)/K(x^2+x+1)$是否是代数扩张? 如果是, 请问扩张次数次数为多少.

注意到 x满足方程 $T^2+T-(x^2+x)=0$. 需证不约

而后者在$K(x^2+x+1)$上无非因进而不可约(计算次数即可)

故 $K(x)/K(x^2+x+1)$是2次代数扩张.

方法二：只需证明 $x\in K(x^2+x+1)$.

若 $x=\frac{P(x^2+x+1)}{Q(x^2+x+1)}$,

比较次数得到矛盾.

设 $\frac{P(x^2+x+1)}{Q(x^2+x+1)}$ 满足方程, $P,Q\in K[T]$ 互素.

代入 $\frac{P(Y)}{Q(Y)}$ 满足 $T^2+T-(Y-1)=0$.

$\Rightarrow Q(Y)\mid 1,\ P(Y)\mid Y-1$. $\Rightarrow \frac{P(x^2+x+1)}{Q(x^2+x+1)}\in K[x^2+x+1]$.

故 $\left(\frac{P}{Q}\right)^2+\left(\frac{P}{Q}\right)$至少为4次(或0次), 不能等于 x^2+x. □

3. (20分) 设$\mathbb{F}_3=\mathbb{Z}/3\mathbb{Z}$为3元域, $\mathbb{F}_3^n$为取值$\mathbb{F}_3$的n元列向量. 考虑一般线性群$GL(2,\mathbb{F}_3)$(2阶可逆矩阵集合)和特殊线性群$SL(2,\mathbb{F}_3)$(行列式为1的矩阵集合)在$\mathbb{F}_3^2$上的左乘作用.

(1) 列举$GL(2,\mathbb{F}_3)$在$\mathbb{F}_3^2$上作用的轨道以及轨道长度.

(2) 列举$SL(2,\mathbb{F}_3)$在$\mathbb{F}_3^2$上作用的轨道以及轨道长度, 计算向量$(1,0)^T$在$SL(2,\mathbb{F}_3)$作用下的固定子群以及阶数.

(3) 计算$SL(2,\mathbb{F}_3)$的阶数.

(4) 可以用上面的思想归纳计算$SL(n,\mathbb{F}_3)$的阶数以及$GL(n,\mathbb{F}_3)$的阶数, 写一个递推公式(不需要过程).

(1). 轨道：$\{0\}$, $\mathbb{F}_3^2\setminus\{0\}$.

长度：1, $3^2-1=8$

(2) 同上. $\mathrm{Stab}_{SL(2,\mathbb{F}_3)}((1,0)^T)=\left\{\begin{pmatrix}1&*\\0&1\end{pmatrix}\right\}$.

阶数为3.

(3). $|SL(2,\mathbb{F}_3)|=|\mathrm{Stab}_{SL(2,\mathbb{F}_3)}((1,0)^T)|\times 8$

$=24$

(4). $\frac{|GL(n,\mathbb{F}_3)|}{|GL(n-1,\mathbb{F}_3)|\cdot 3^{n-1}}=3^n-1$.

① $GL(n,\mathbb{F}_3)$在$\mathbb{F}_3^n\setminus\{0\}$上作用传递

② $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$的固定子群 $H=\left\{\begin{pmatrix}1&a_2\cdots a_n\\0&\\\vdots&B\\0&\end{pmatrix}\middle|\ B\in GL(n,\mathbb{F}_3)\right\}$

①+② $\Rightarrow$ $3^n-1=\frac{|GL(n,\mathbb{F}_3)|}{|H|}$

$|H|=|GL(n-1,\mathbb{F}_3)|\cdot 3^{n-1}$.

4. (25分) 设$R=\mathbb{Z}[\sqrt{2}i]=\{a+b\sqrt{2}i|a,b\in\mathbb{Z}\}$复数域$\mathbb{C}$的子环, 并视$\mathbb{Z}$为$R$的子环, 以下设$p$是一个素数, 记有限域$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

(1) 证明环同构$R\cong\mathbb{Z}[x]/(x^2+2)$和

$$R/(p)\cong\mathbb{Z}[x]/(p,x^2+2)\cong\mathbb{F}_p[x]/(x^2+\bar{2}).$$

(2) 证明R为欧氏整环.

(3) 列举$\mathbb{Z}[\sqrt{2}i]$中的单位, 判断9和7是否是可约的(需要说明理由), 如果可约对其做一个不可约分解(只需结果即可).

(4) 在环$x\in\mathbb{Z}[\sqrt{2}i]$中, 判断同余方程$x\equiv\sqrt{2}i\pmod 9$, $x\equiv 1\pmod 7$ 是否可解, 如果可解请列举所有满足上述同余方程的解.

(5) 证明存在整数a,b使得$p=a^2+2b^2$当且仅当在环$\mathbb{F}_p[x]$中多项式$x^2+\bar{2}$可约.

(6) 由前面的结论已知理想(7)是$R=\mathbb{Z}[\sqrt{2}i]$的极大理想. 记商域$L=R/(7)$, 视$K=\mathbb{F}_7$为L的子域.

(6.1) 求元素$\overline{2\sqrt{2}i}$在K上的极小多项式.

(6.2) 证明$K[x]$上的一个三次不可约多项式$f(x)$在$L[x]$上也是不可约的.

(5). 存在 $a,b\in\mathbb{Z}$ 使 $p=a^2+2b^2$

$\Leftrightarrow$ p 在 R 中可约.

("$\Rightarrow$": 显然; "$\Leftarrow$": 若 $p=\alpha\cdot\beta$, $\alpha,\beta\notin R^\times$

则 $p^2=N(\alpha)N(\beta)$

$\Rightarrow N(\alpha)=N(\beta)=p$

$\alpha=a+b\sqrt{2}i$

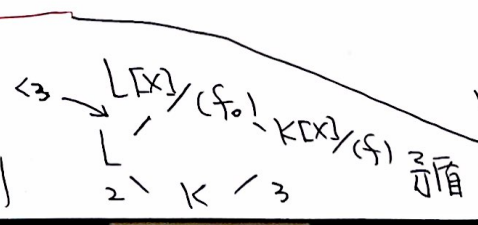
$\Rightarrow p=a^2+2b^2$)

(6.1). 由 $\sqrt{2}i$ 极小多项式为 x^2+2

故 $2\sqrt{2}i$ 极小多项式为 x^2+1.

(6.2也可取证: 若 f 在 L 上可约, 则有根 $u\in L$. u 在 K 上三次不可)

(6.2). 假设 f 在 L 上可约, 取 f 的不可约因子 $f_0\in L[x]$, 则



$3\mid[L:K]=[L:\mathbb{F}_7]\Rightarrow\deg f_0\geq 3$) □

(1) 易知 x^2+2 是 $\sqrt{2}i$ 的零化多项式, 且在 $\mathbb{Q}$ 上不可约 (Eisenstein)

故 $\varphi:\mathbb{Z}[x]\longrightarrow R$ 的 Kernel 为 (x^2+2). 易知 φ 满, $x\mapsto\sqrt{2}i$

由同态基本定理知 $R\cong\mathbb{Z}[x]/(x^2+2)$

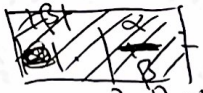
$$R/(p)=\frac{\mathbb{Z}[x]/(x^2+2)}{(p,x^2+2)/(x^2+2)}\cong\mathbb{Z}[x]/(p,x^2+2)\cong\mathbb{F}_p[x]/(x^2+2).$$ □

(2) 只需证明 $N:a+b\sqrt{2}i\mapsto a^2+2b^2$ 是欧氏赋值.

易知 $\forall\gamma\in\mathbb{C}$, $\exists s\in R$ 使得 $|\gamma-s|<1$

进而 $\forall\alpha,\beta\in R$, 取 $s\in R$ 使得 $\left|\frac{\alpha}{\beta}-s\right|<1$, 令 $\tau=\alpha-s\beta$

$\beta\neq 0$.

则 $|\tau|=$  $|\beta|\cdot\left|\frac{\alpha}{\beta}-s\right|<|\beta|$. □

进而 $N(\cdot)=|\cdot|^2$ 是欧氏赋值

(3). $a+b\sqrt{2}i\in R^\times\Leftrightarrow N(a+b\sqrt{2}i)=1$

$\Leftrightarrow a^2+2b^2=1$

$\Leftrightarrow a+b\sqrt{2}i=\pm 1$.

易得 $9=(1+\sqrt{2}i)^2(1-\sqrt{2}i)^2$ 从而可约.

而 $R/(7)\cong\mathbb{F}_7[x]/(x^2+2)$. 由于 $\left(\frac{-2}{7}\right)=\left(\frac{-1}{7}\right)\cdot\left(\frac{2}{7}\right)=-1\cdot 1=-1$

后者为整环. 故 $7\in R$ 不可约. □

(4). 易得 $\begin{cases}28\equiv 1\ [9]\\28\equiv 0\ [7]\end{cases}$ $\begin{cases}36\equiv 0\ [9]\\36\equiv 1\ [7]\end{cases}$.

故 $\alpha=28\sqrt{2}i+36$ 为一解. 若 $\beta\in R$ 也为解

$\Leftrightarrow\alpha-\beta\equiv 0\ [9],[7]$

$\overset{(3)}{\Leftrightarrow}\alpha-\beta\equiv 0\ [63]$.

R中倒互素.

$\Leftrightarrow\beta=\alpha+63\gamma$, $\gamma\in R$. □