近世代数月考

2011年10月10日

1. 设$G = \mathrm{GL}_2(\mathbb{R})$, B为其中上三角阵构成的子群, $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. 证明: G是BwB与B的不交并.

2. 给出$\mathrm{GL}_n(\mathbb{F}_p)$的一个Sylow p子群.

3. 证明$\mathrm{GL}_2(\mathbb{C})$中不含指数有限的真子群.

4. 已知四元数$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$中的乘法如下给出:

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

(1) 证明$\mathbb{H}^\times = \mathbb{H} - \{0\}$在乘法意义下构成群.

(2) 对于$\alpha = a + bi + cj + dk$, 定义其共轭为$\bar{\alpha} = a - bi - cj - dk$. 证明$N : \alpha \mapsto \alpha \cdot \bar{\alpha} = a^2 + b^2 + c^2 + d^2$ 是$\mathbb{H}^\times$到$\mathbb{R}^\times$的群同态.

(3) 证明$\ker N$同构于

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 \\ -\bar{\alpha}_2 & \bar{\alpha}_1 \end{pmatrix} :\ \alpha_1, \alpha_2 \in \mathbb{C},\ |\alpha_1|^2 + \alpha_2|^2 = 1 \right\},$$

其中复数$\alpha = x + yi$ 的共轭是$x - yi$.

5. (1) 若$G/C(G)$是循环群, 证明G为阿贝尔群, 故非交换有限群G的中心$C(G)$的指数≥ 4.

(2) 如G为n阶有限群, t为G中共轭类的个数, $c = \frac{t}{n}$. 证明$c = 1$或者$c \leq \frac{5}{8}$.

6. 设H, K是G的正规子群，且$HK = G$, $H \cap K = \{1\}$. 证明G 同构于$H \times K$.

7. 设群G是24阶群且其中心平凡, 证明G同构于S_4.

近世代数月考

2011年11月14日

1. (10分) 设$f(x) \in \mathbb{Z}[x]$在$\mathbb{Q}[x]$上可约, 证明其在$\mathbb{Z}[x]$上可约.

2. (15分) 设$I_1, \cdots, I_n$是环R中的理想, 且素理想$P = \bigcap\limits_{i=1}^{n} I_i$. 证明: P必等于其中某个I_i.

3. (20分) 设$A = \mathbb{Z}[\sqrt{-2}]$.
(1) 证明A是欧几里得整环.
(2) 给出素数p在A中的因式分解.

4. (25分) 设A是有限阿贝尔群, S^1为单位圆. 定义$A^* = \{$群同态$f : A \to S^1\}$, 并在其中定义乘法为:

$$(f \cdot g)(x) = f(x)g(x).$$

(1) 证明A^*是有限阿贝尔群.
(2) 证明A 同构于A^*.
(3) 如果B是A的子群, 则映射$\varphi : A^* \to B^*$, $f \mapsto f|_B$是满同态, 其中$f|_B$是同态$f : A \to S^1$在B上的限制(提示: 可以先考虑A/B是p阶循环群的情形).

5. (30分) 设D为整环, K是D的商域. 设集合$S \subseteq D$ 满足条件
(i) $0 \notin S$, $1 \in S$;
(ii) 对$x, y \in S$, 则$xy \in S$.
定义

$$S^{-1}D = \left\{ \frac{m}{n} \mid m \in D,\ n \in S \right\} \subseteq K.$$

证明:
(1) $S^{-1}D$ 是K中包含D的子环.
(2) $S^{-1}D$中的素理想必有$S^{-1}\mathfrak{p} = \{\frac{m}{n} \mid m \in \mathfrak{p},\ n \in S\}$的形式, 其中$\mathfrak{p}$是$D$的素理想.
(3) $\operatorname{Spec} S^{-1}D$与集合$\{\mathfrak{p} \in \operatorname{Spec} D \mid \mathfrak{p} \cap S = \emptyset\}$ 一一对应.
(4) 设$D = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$, $S = \mathbb{Z} - \mathfrak{p}$, 则$\mathbb{Z}/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$ 同构于$S^{-1}\mathbb{Z}/S^{-1}\mathfrak{p}$.

近世代数月考

2011年12月12日

1. (30分) (1) 证明对于$n \geq 3$, $x^{2^n}+x+1$在$\mathbb{F}_2[x]$上是可约多项式.

(2) 设p, l 为素数, n 为正整数, 试求$F_p[x]$中l^n次首一不可约多项式的个数.

2. (20分) 设p是素数, $\zeta_p = \exp(2\pi i/p)$是p次本单位根, $(\frac{a}{p})$为Legendre符号. 设

$$G = \sum_{a \in \mathbb{F}_p} \zeta_p^a \Big(\frac{a}{p}\Big).$$

证明:

(1) $\sum\limits_{a \in \mathbb{F}_p} \zeta_p^a = 0$.

(2) $G \cdot \overline{G} = p$, 其中$\overline{G}$ 是G的复共轭.

(3) $G = \pm\sqrt{(-1)^{(p-1)/2}p}$.

3. (25分) 设$F \supseteq \mathbb{Q}$是数域, K/F是域的n次有限扩张. 设$\alpha \in K$. 令T_α为K上的F-线性变换$T_\alpha(x) = \alpha x$.

(1) 设α在F上的最小多项式为$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. 试求$\mathrm{Tr}\, T_\alpha$和$\det T_\alpha$.

(2) 定义$\mathrm{Tr}(\alpha) = \mathrm{Tr}(T_\alpha)$. 证明$B : K \times K \to F$, $(x, y) \mapsto \mathrm{Tr}(xy)$是$F$上的双线性形, 且是非退化的(即若$x \in K$, $B(x, y) = 0$对所有y成立. 则$x = 0$).

4. (25分) (1) 证明$\mathbb{R}[x]$中的不可约多项式一定是1次或者2次的(注: 只知道代数基本定理).

(2) 证明$\mathbb{Z}[x]$上的极大理想必有$(p, f(x))$的形式, 其中p是素数, $f(x) \bmod p$是$\mathbb{F}_p[x]$上的不可约多项式.

近世代数期末考试试卷

2012年1月3日

注意: 试卷共12题, 每题30分, 总分300分. 答卷人可以选作其中任何10题. 多做按最优10题给分. 题目难度和次序无确定关系. **答题纸上必须注明题号**.

1. (1) 设a, b为群G的元素, a的阶是5, 且$a^3b = ab^3$. 证明: $ab = ba$.
   (2) 试求S_6中2阶元的个数.

2. 证明$\mathrm{SL}_n(\mathbb{R})$ 由第一类初等矩阵$I + aE_{ij}$生成, 其中E_{ij}的第(i, j)-元为1, 其他元为0.

3. 设G, A, B 为有限阿贝尔群. 如果$G \oplus A \cong G \oplus B$, 证明$A$ 同构于B.

4. 说明对角线为1的上三角阵集合是$\mathrm{GL}_n(\mathbb{F}_p)$的一个Sylow p子群, 并求$\mathrm{GL}_n(\mathbb{F}_p)$所有Sylow p子群的个数.

5. 设R为交换环. 称$x \in R$为幂零元, 如果存在$n \in \mathbb{N}$. $x^n = 0$. 求证:
   (1) R中所有幂零元构成的集合N是R的一个理想.
   (2) R中所有素理想均包含N.

6. (1) 试求$11 + 7i$与$18 - i$在$\mathbb{Z}[i]$上的最大公因子.
   (2) 若m, n为整数, 则m, n在$\mathbb{Z}$上的最大公因子等于它们在$\mathbb{Z}[i]$上的最大公因子.

7. 设p为素数, A为n阶整方阵, $A^p = I$且$A \neq I$, 证明$n \geq p - 1$.

8. 回忆$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$的判别式是

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

设p为素数.
   (1) 计算$f(x) = x^{p-1} + x^{p-2} + \cdots + 1$的判别式.
   (2) 证明$\mathbb{Q}(\zeta_p)/\mathbb{Q}$中唯一的二次子扩张是$\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$.

9. 构作一个8元域, 并写出其加法表和乘法表.

10. 设K是$f(x) = x^4 - 2$在$\mathbb{Q}$上的分裂域, 试求$K/\mathbb{Q}$的Galois群和全部子域.

11. 设$\alpha_1^2 = 2$, $\alpha_2^2 = 3$. 求$\alpha_1 + \alpha_2$在$\mathbb{Q}$, $\mathbb{F}_5$, $\mathbb{F}_7$上的不可约多项式.

12. 设K是$f(x) = x^4 - 2$在$\mathbb{F}_5$上的分裂域, 试求$K/\mathbb{F}_5$的Galois群和全部子域.

近世代数月考

2013年3月27日

1. 设 A, B 是群 G 的两个子群. 试证 AB 是 G 的子群当且仅当 $AB = BA$.

2. 回答下列问题：
  (1) 设 p 是素数, p 方幂阶群是否一定含有 p 阶元?
  (2) 35阶群是否一定同时含有5阶和7阶元素?
  (3) 若有限群 G 同时含有10阶元 x 和6阶元 y, 那么群 G 的阶应该满足什么条件?

3. 试计算:
  (1) S_6 中2阶元的个数.
  (2) A_8 中阶最大的元素个数.

4. 设群 G 作用在集合 Σ 上. 令 t 表示 Σ 在 G 作用下的轨道个数, 对任意 $g \in G$, $f(g)$ 表示 Σ 在 g 作用下的不动点个数. 试证

$$\sum_{g\in G} f(g) = t|G|.$$

5. (1) 若 $G/Z(G)$ 是循环群, 证明 G 为阿贝尔群, 故非交换有限群 G 的中心 $Z(G)$ 的指数 $\geqslant 4$.
  (2) 如果 G 为 n 阶有限群, t 为 G 中共轭类的个数, $c = \frac{t}{n}$. 证明 $c = 1$ 或者 $c \leqslant \frac{5}{8}$.

6. 设群 $\mathrm{SL}_2(\mathbb{R})$ 在上半平面 $\mathcal{H}$ 上的作用即: 对 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma(z) = \dfrac{az+b}{cz+d}$. 试证明微分形式 $\dfrac{dx \wedge dy}{y^2}$ 在 γ 作用下不变, 即若 $z = x + yi$, $\gamma(z) = x' + y'i$, 则

$$\frac{dx \wedge dy}{y^2} = \frac{dx' \wedge dy'}{y'^2}.$$

7. (1) 设 p 是素数, $n \geqslant 1$. 证明映射

$$\varphi : \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{F}_p),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \mod p & b \mod p \\ c \mod p & d \mod p \end{pmatrix}$$

为群的满同态.
  (2) 试求群 $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ 的阶.
  (3) 设正整数 m, n 互素. 试证明:

$$\mathrm{GL}_2(\mathbb{Z}/mn\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

近世代数月考

2013年4月27日

1. 证明复数域 $\mathbb{C}$ 可嵌入到环 $M_2(\mathbb{R})$ 中.

2. 令 $G = G_1 \times G_2 \times \cdots \times G_n$, 且对任意 $i \neq j$, $|G_i|$ 和 $|G_j|$ 互素. 证明 G 的任意子群 H 都是它的子群 $H \cap G_i$ $(i = 1, 2, \cdots, n)$ 的直积.

3. 设 R 是环, $\mathfrak{m}$ 是 R 的一个理想. 假设 R 的每个不属于 $\mathfrak{m}$ 的元素是 R 中 的单位. 证明 $\mathfrak{m}$ 是 R 的唯一极大理想.

4. 设 F 是域, 多项式环 $F[x]$ 的分式域记为 K. 对于 $a \in F$, 称 $f(x) \in K$ 在点 a 处正则是指存在 $p_1(x), p_2(x) \in F[x]$, $p_2(a) \neq 0$ 且 $f(x) = \dfrac{p_1(x)}{p_2(x)}$. 定义 f 在 a 点的值为 $f(a) = p_1(a)/p_2(a)$.

(1) 证明 $f(a)$ 的定义是良好的.

记 O 为所有在 a 点正则的 $f(x)$ 构成的环.

(2) 求 O 的单位群.

(3) 证明 O 中真理想 I 均是由 $(x-a)^n (n \in \mathbb{N})$ 生产的主理想.

5. 证明150阶群不是单群.

6. 设有限阿贝尔群 $A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}$, 其中 p_i 是素数, $\alpha_i \geq 1$ 为正整数. 证明 A 的任意子群 B 均同构于 $\mathbb{Z}/p_1^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\beta_s}\mathbb{Z}$, 其中 $0 \leq \beta_i \leq \alpha_i$ 为整数.

7. 设 R 是正整数集合到域 K 的函数全体. 在 R 上定义加法为一般函数的加法, 乘法定义为卷积: 对于 $f, g \in R$, 卷积 $f * g$ 即

$$(f * g)(m) = \sum_{xy=m} f(x)g(y).$$

其中求和过所有正整数对 (x, y) 使得 $xy = m$.

(1) 证明 R 在上述加法和乘法意义下构成交换环, 其单位元为函数 δ, 其中 $\delta(1) = 1$, $\delta(x) = 0$ 如 $x \neq 1$.

(2) 证明常值函数 $\varphi_1 : x \mapsto 1$ 的逆元为 Möbius函数

$$\mu(x) = \begin{cases} 1, & x = 1; \\ (-1)^r, & x\text{是}r\text{ 个不同素数的乘积}; \\ 0, & \text{其他情况}. \end{cases}$$

(3) 由(2), 你能给出 Möbius 公式并给出理由吗?

近世代数月考

2013年5月26日

1.(1) 求 $\zeta_7 = e^{2\pi i/7}$ 在 $\mathbb{Q}$ 上的最小多项式.
(2) 求 $\cos\frac{2\pi}{7}$ 在 $\mathbb{Q}$ 上的最小多项式.

2. 设域 F 的特征不是 2. 证明 F 上任意 2 次扩张 K 均可写为 $K = F(\sqrt{a})$, 其中 $a \in F - F^2$. 如果 F 的特征为 2, 结论是否成立?

3. 设 $p \equiv 3 \mod 4$ 是素数. 证明商环 $\mathbb{Z}[i]/(p)$ 同构于 $\mathbb{F}_{p^2}$.

4. 设 D 是整环但不是域, 证明 $D[x]$ 不是主理想整环.

5. 设 α, β 分别是有限域 $\mathbb{F}_p$ (p 是素数)的代数闭包 $\bar{\mathbb{F}}_p$ 中的多项式 x^2-2 和 x^2-3 的根. 令 $E = \mathbb{F}_p(\alpha, \beta)$. 讨论 $E/\mathbb{F}_p$ 的扩张次数.

6. 证明两个整多项式在 $\mathbb{Q}[x]$ 中互素当且仅当它们在 $\mathbb{Z}[x]$ 中生成的理想含有一个非零整数.

7. 设 F 是域, R 是 F 上的所有 x 项系数为 0 的多项式构成的集合. 证明 R 是环但不是 UFD.

8. 证明当 $n \geq 3$ 时, $x^{2^n} + x + 1$ 是 $\mathbb{F}_2[x]$ 上的可约多项式.

近世代数期末考试试卷

2013年6月17日

注意: 试卷共12题, 每题30分, 总分300分. 答卷人可以选作其中任何10题. 多做按最优10题给分. 题目难度和次序无确定关系. **答题纸上必须注明题号**.

1. 证明或者给出反例:
   (1) 如果正整数 m 整除 阿贝尔群 G 的阶 n, 则 G 有 m 阶子群.
   (2) 如果正整数 m 整除 G 的阶 n, 则 G 有 m 阶子群.

2. 给出群 S_6 中元素可能的型, 并求出每个型中元素的个数.

3. 证明 $\mathbb{Q}$ 不是循环群, 但它的任意有限生成子群都是循环群.

4. 试给出一个9元域并给出它的乘法表.

5. 设a, b 是群G中的两个元素, 证明 a与 a^{-1} 有相同阶, ab 与 ba 有相同阶.

6. 试求出 (同构意义下) 所有 6 阶群.

7. 试求出 (同构意义下) 所有 8 阶群.

8. 设 p 是素数.
   (1) 证明 p^2 阶群都是阿贝尔群.
   (2) 求$\mathrm{GL}_3(F_p)$ 中Sylow p-群的阶.
   (3) 给出$\mathrm{GL}_3(F_p)$ 中Sylow p-群的具体例子, 并说明它不是阿贝尔群.

9. 设 p, l 为互不相同的素数, n 为正整数. 求 $\mathbb{F}_p[x]$ 中首一不可约 l^n 次多项式的个数.

10. 设域 $F = \mathbb{F}_5$ 或者 $\mathbb{Q}$. 证明 $f(x) = x^3 + x + 1$ 为 F 上的不可约多项式. 求 $f(x)$ 在 F 上的 Galois群.

11. 证明 $\mathbb{Q}(\sqrt[4]{2}(1+\sqrt{-1})/\mathbb{Q}$ 是四次扩张; 并求出它的 Galois群.

12. (1) 证明 $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ 是 Galois 扩张, 并求出 Galois 群;
   (2) 求元素 $\sqrt{6} + \sqrt{10} + \sqrt{15}$ 在 Q 上的极小多项式.

13. 设 E/F 为有限 Galois 扩张, N 和 M 为中间域, $E \supseteq N \supseteq M \supseteq F$, 并且 N 是 M 在 F 上的正规闭包. 证明

$$\mathrm{Gal}(E/N) = \bigcap_{\sigma \in \mathrm{Gal}(E/F)} \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}.$$

14. 设 E 为 $x^4 - 2$ 在 $\mathbb{Q}$ 上的分裂域.
   (1) 试求出 $E/\mathbb{Q}$ 的全部中间域.
   (2) 试问哪些中间域是 $\mathbb{Q}$ 的 Galois 扩张?

15. 设 $E = \mathbb{Q}(\alpha)$, 其中 $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$. 证明

(1) α^2-2 也是多项式 $x^3+x^2-2x-1=0$ 的根.
(2) $E/\mathbb{Q}$ 是正规扩张.
(3) 试求 $\mathrm{Gal}(E/\mathbb{Q})$.

16. 试确定 $\mathbb{Z}[x]$ 中所有的素理想和极大理想.

17. 设 u 是多项式 $x^3-6x^2+9x+3=0$ 的根.
(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$.
(2) 试将 u^4 和 $(u^2-6u+8)^{-1}$ 表示为 1, u, u^2 的线性组合.

18. 设 p 是素数.
(1) 证明 $f(x^p)=f(x)^p$ 对于任意 $f(x)\in\mathbb{F}_p[x]$ 成立.
(2) 设整数 $m\geq n\geq 0$. 证明: $\binom{pm}{pn}\equiv\binom{m}{n} \bmod p$.

19. 设 p 是$\mathbb{Z}$ 上的奇素数, n为正整数. 证明 x^n-p 是 $\mathbb{Z}[i]$ 上的不可约多项式.

20. 证明 x^3+nx+2 对所有 $n\neq 1,-3,-5$ 是$\mathbb{Z}$ 上的不可约多项式.

21. 设 $d\geq 3$ 为无平方因子的整数, $K=\mathbb{Q}(\sqrt{d})$.
(1) 证明 K 中任意元素在$\mathbb{Q}$ 上的最小多项式的次数等于 1或者 2.
(2) 设 $\mathcal{O}$ 是 K 中所有在 $\mathbb{Q}$上的最小多项式为首一整系数多项式的元素的集合. 证明 $\mathcal{O}$ 是秩 2 自由阿贝尔加法群.

22. 设 $n\geq 3$ 为无平方因子的整数, $R=\mathbb{Z}[\sqrt{-n})$.
(1) 证明 2, $\sqrt{-n}$ 和 $1+\sqrt{-n}$ 在 R 上为不可约元.
(2) 证明 $\sqrt{-n}$ 和 $1+\sqrt{-n}$ 在 R 上不能同时为素元.

23. 证明若整环R 中的素理想都是主理想, 则 R 是PID (提示: 反证法. 利用Zorn引理, 考虑对所有非主理想按包含关系排序获得的极大元).

24. 设 $\mathfrak{p}$ 是含幺交换环 R 的素理想, $I_1,\ldots,I_n$ 是 R 的理想. 如果 $\mathfrak{p}=\bigcap\limits_{i=1}^{n} I_i$, 则 $\mathfrak{p}$ 必等于某个 I_i.