2020 — 2021 秋学期抽象代数期末考试

1. (20 分, 每小题 2 分) 判断下列断言是否为真 (**不需证明**).

   (a) 对于固定的正整数 n, 只有有限个互不同构的 n 阶有限群. **对**

   (b) 15 阶群一定是循环群. **对**

   (c) 对任何正整数 n, 环 $\mathbf{Z}/(n)$ 的可逆元的全体在乘法下构成一个有限循环群. **错**

   (d) 表现矩阵
   $$\begin{bmatrix} 1 & x+y-1 \\ x & x^2 \\ y & y^2-x \end{bmatrix}$$
   决定了 $\mathbf{C}[x,y]$ 上的一个自由模. **错**

   (e) 诺特环的子环仍然是诺特环. **错**

   (f) 实数 $\sqrt[3]{2+\sqrt{5}}$ 可以用尺规构造出来. **错**

   (g) $\mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ 是唯一分解整环. **对**

   (h) $\mathbf{Z}[\sqrt{-3}]$ 是唯一分解整环. **错**

   (i) 元素个数相同的有限域一定同构. **对**

   (j) 特征 0 的环一定是无限的. **对**

2. (15 分) 分类一切阶数小于等于 7 的群 (只需写下所有的同构类, **不需证明**).

   答案: $\{1\}, C_2, C_3, C_2\times C_2, C_4, C_5, C_6, \mathfrak{S}_3, C_7.$

3. (20 分, 每小题 10 分) 令 $A=\mathbf{Z}[\sqrt{2}]=\left\{a+b\sqrt{2}\in\mathbf{R} : a,b\in\mathbf{Z}\right\}$.

   令 $\mathfrak{m}=(5)=\left\{a+b\sqrt{2}\in A : 5\mid a, 5\mid b\right\}$.

   (a) 证明 $\mathfrak{m}$ 是 A 的极大理想.

   证 我们有
   $$A/\mathfrak{m}\cong\mathbf{Z}[X]/(X^2-2,5)\cong\mathbf{F}_5[X]/(X^2-2).$$
   由于 $(2/5)=-1$, X^2-2 不可约, 又 $\mathbf{F}_2[X]$ 是主理想整环, 任何不可约元生成之非零理想为极大.

   (b) 域 $A/\mathfrak{m}$ 的元素个数是多少?

   答案: 25.

4. (10 分) 令 G 是一个奇数阶的有限群. 设 H 是 G 的一个 5 阶正规子群. 证明 H 被包含于 G 的中心.

   证 令 G 共轭作用于 H 上. 我们得到同态 $G\to\mathrm{Aut}(H)$. 由于 H 是 5 阶群, $\mathrm{Aut}(H)\cong\mathbf{Z}/(4)$. 由于 G 奇数阶, 其像必然为奇数阶. 但 $\mathbf{Z}/(4)$ 之奇数阶子群只有平凡群. 因此 G 在 H 上之作用必然为平凡. 即 $H\subset \mathrm{Z}(G)$.

5. (10 分) 设域 F 具有特征 0. 设 K/F 是一个以 $\mathbf{Z}/(2)\times\mathbf{Z}/(2)$ 为 Galois 群的 Galois 扩张. 证明存在 $\alpha,\beta\in K$, 使得 $\alpha^2\in F,\beta^2\in F, K=F(\alpha,\beta)$.

证 令 K_i 分别为 $\mathbf{Z}/(2)^2$ 的第 i 个分量对应的子群的对应中间域. 则 K_i/F 为二次扩张, 故而相当于添入 $\alpha_i,\alpha_i^2\in F$. 包含 α_i 的 K 的子域也包括了 $\alpha_1\alpha_2$. 因此至少是 4 维 F-线性空间, 因此 $K=F(\alpha_1,\alpha_2)$.

6. (20 分) 设 R 为整环, 以 K 为分式域, 满足如下性质:

- $R\neq K$,
- $[x\in K-R]\implies[x^{-1}\in R]$.

(a) (5 分) 若 p 是素数, 证明

$$\mathbf{Z}_{(p)}=\left\{\frac{a}{b}\in\mathbf{Q}:\frac{a}{b}\text{ 是既约分数, 且 } p\nmid b\right\}$$

满足题设中关于 R 的条件.

证 显然 $\mathbf{Z}_{(p)}$ 是以 $\mathbf{Q}$ 为分式域的整环. 若 $a/b\notin\mathbf{Z}_{(p)}$, 则 $a\neq 0, p\mid b, p\nmid a$. 故 $b/a\in\mathbf{Z}_{(p)}$.

(b) (8 分) 证明 $\mathfrak{m}=\{r\in R:r^{-1}\notin R\}$ 是 R 的唯一极大理想.

证 若 $I\subsetneq R$ 是真理想, 则任意 $r\in I$, r^{-1} 必然不在 R 中, 不然 $1\in I, I=R$. 因此只需证明 $\mathfrak{m}$ 是理想. 为此, 设 $a-\{0\}\in R, x\in\mathfrak{m}-\{0\}$. 若 $ax\notin\mathfrak{m}$, 则 $a^{-1}x^{-1}\in R$, 则 $aa^{-1}x^{-1}=x^{-1}\in R$, 矛盾.

若 $a,b\in\mathfrak{m}-\{0\}$, 但是 $a+b\notin\mathfrak{m}$, 则 $a+b\neq 0$, $(a+b)^{-1}\in\mathfrak{m}$, 因此

$$\frac{a}{a+b},\frac{b}{a+b}\in\mathfrak{m}$$

取倒数, 得到 $b/a, a/b\notin\mathfrak{m}$. 矛盾.

(c) (7 分) 如果 R 不是主理想整环, 证明 R 不是诺特环.

证 只需证明任何 R 的有限生成理想是主理想. 为此, 可对生成元个数归纳. 设 $I=(f_1,\ldots,f_r)$, $f_i\neq 0$. 则 f_r/f_1 或者 f_1/f_r 之一属于 R. 若为前者, 可以在生成元中去掉 f_1, 若为后者, 可以去掉 f_r. 总之可以削减生成元个数.

7. (15 分) **阅读理解题**.

令 R 为一个含幺交换环. 一个 R 上的 (**一维**, **交换**) **形式群律** (1-dimensional commutative formal group law) 是指一个两变元形式幂级数 $F(X,Y)\in R[[X,Y]]$, 满足以下性质:

- 若 $F(X,Y)=\sum_{i,j\geq 0}a_{i,j}X^iY^j$, 则 $a_{0,0}=a_{1,1}=0$, $a_{1,0}=a_{0,1}=1$. 即 F 的次数小于等于 1 的项为 $X+Y$.
- (“结合律”) 在三个变量形式幂级数环 $R[[X,Y,Z]]$ 中, 成立等式

$$F(F(X,Y),Z)=F(X,F(Y,Z)).$$

- (“交换律”) 在 $R[[X,Y]]$ 中, 成立 $F(X,Y)=F(Y,X)$.

设 $F, G \in R[[X,Y]]$ 是两个环 R 上的形式群律. 一个从 F 到 G 的**同态**是指一个单变量幂级数 $u(X) = a_1 X + a_2 X^2 + \cdots \in R[[X]]$, 满足

$$F(u(X), u(Y)) = u(G(X,Y))$$

称同态 $u(X)$ 为环 R 上的形式群律的**同构**, 如果 $u'(0)$ 是 R 中的可逆元.

(a) (5 分) 设 F 是一个 R 上的形式群律. 对自然数 n, 归纳定义幂级数 $\{n\}_F(X) \in R[[X]]$ 如下: $\{1\}_F(X) = X$, $\{2\}_F(X) = F(X,X)$, $\{3\}_F(X) = F(\{2\}_F(X), X)$, $\ldots$, $\{m+1\}_F(X) = F(\{m\}_F(X), X)$, $\ldots$. 证明 $\{n\}_F(X)$ 是 F 到自己的同态.

证 对 n 归纳. 计算

$$\begin{aligned}
F(\{n\}(X), \{n\}(Y)) &= F(F(\{n-1\}(X), X), \{n\}(Y)) \\
&= F(X, F(\{n-1\}(X), \{n\}(Y))) \\
&= F(X, F(\{n-1\}(X), F(\{n-1\}(Y), Y))) \\
&= F(X, F(\{n-1\}(X), \{n-1\}(Y), Y)) \\
&= F(X, F(Y, \{n-1\}F(X,Y))) && \leftarrow \text{归纳假设} \\
&= F(F(X,Y), \{n-1\}(F(X,Y))) \\
&= \{n\}(F(X,Y)).
\end{aligned}$$

今考虑如下幂级数:

- ‘‘形式加法群'': $F_{\mathrm{a}}(X,Y) = X + Y$,
- ‘‘形式乘法群'': $F_{\mathrm{m}} = X + Y + XY = (1+X)\cdot(1+Y) - 1$.

由于这两个幂级数的非零系数只有 1, 我们可以将它们看作任何环 R 上的幂级数. 它们定义了两个 R 上的形式群律.

(b) (5 分) 如果将 $F_{\mathrm{a}}, F_{\mathrm{m}}$ 看作 $\mathbf{Q}$ 上的形式群律, 证明它们是同构的.

证 令 $\phi(X) = \sum_{n=1}^{\infty} X^n/n! = e^X - 1$. 利用指数函数性质即证.

(c) (5 分) 如果将 $F_{\mathrm{a}}, F_{\mathrm{m}}$ 看作 $\mathbf{Z}$ 上的形式群律, 它们是否同构?

[提示: 如果它们在 $\mathbf{Z}$ 上同构, 那么将诸系数模 p, 便能够推出它们在 $\mathbf{F}_p$ 上同构.]

答案 否. 若在 $\mathbf{F}_p$ 上通过 u 同构, 则 $0 = u(\{p\}_{F_{\mathrm{a}}}(X)) = \{p\}_{F_{\mathrm{m}}}(u(X)) = u(X)^p$. 与 $u(0) \neq 0$ 矛盾.