抽象代数期末考试

2018年1月2日，星期二

1 [15分]. 设R是交换幺环，$M = R$是秩为1的自由模。证明：非空子集$S \subset M$是一组基当且仅当$S = \{a\}$，a是R中的一个可逆元素。

2 [15分]. 找出1800阶交换群的所有可能的同构类型（不需要证明）。

3 [15分]. 记$K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$。

(1) [5分]，证明K在$\mathbb{Q}$上的次数等于4。

(2) [5分]，设$\alpha \in K - \mathbb{Q}$，证明$\alpha$在$\mathbb{Q}$上的次数等于2或者4。

(3) [5分]，找出一个元素$\alpha \in K - \mathbb{Q}$，它在$\mathbb{Q}$上的次数是4（不需要证明）。

4 [10分]. 设$R = \mathbb{Z}$，$M = R^{(2)}$是R上秩为2的自由模。在$M^* = M - \{0\}$上定义一个关系$\sim$：对于$v, v' \in M^*$，$v \sim v'$当且仅当存在R-模自同构$\eta : M \to M$，使得$\eta(v) = v'$。

(1) [5分]，证明$\sim$是一个等价关系。

(2) [5分]，找出一些两两互不等价的M^*中的元素，其代表所有的等价类（不需要证明）。

5 [10分]. 设R是交换幺环，$M = R^{(n)}$是R上秩为n的自由模，$f : M \to M$是一个R-模同态。记$A \in M_n(R)$为f 在M的标准基$\{e_1, \ldots, e_n\}$下对应的矩阵。

(1) [5分]，证明f是满同态当且仅当$\det A$是R中的可逆元素。

(2) [5分]，假设$\det A$不是R中的零因子，证明f是单同态。

6 [10分]. 设域F的特征为素数p，假设$a \in F$且$a \notin F^p = \{b^p : b \in F\}$。证明：对于任意的整数$e \geq 1$，$x^{p^e} - a \in F[x]$是不可约多项式。

7 [10分]. 设d是不含任何非平凡平方因子的整数，且$d \neq 0, 1$。记R_d是二次数域$\mathbb{Q}_d = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$的代数整数环，$R_d^\times$为$R_d$的单位群。

(1) [5分]，设$d < 0$，证明$R_d^\times$是有限群，并就d的不同取值具体描叙$R_d^\times$。

(2) [5分]，设$d = 10$，找出$R_{10}^\times$（作为一个Abel群）的生成元并描叙$R_{10}^\times$的结构。

说明：如果套用Pell方程的结果，需给出完整证明，否则视为无效。

8 [5分]. 设$n > 6$。证明：不存在群G，满足$G^{(1)} \cong S_n$。

Proof. Suppose there is such a group G.

Lemma 1: for $n > 6$, if $\sigma \in S_n$ satisfies $\sigma^2 = 1$ and the conjugacy class containing $\sigma \in S_n$ has the same number of elements as the class of (12), then $\sigma \sim (12)$.

Under the assumption, σ is a product of k 2-cycles ($1 \leq k \leq \frac{n}{/}2$). Prove by counting the numbers of conjugacy classes containing σ and (12) respectively.

Lemma 2: $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$.

The group S_n is generated by 2-cycles $\{(k, k+1) : 1 \leq k \leq n-1\}$. By Lemma 1, each $f \in \mathrm{Aut}(S_n)$ maps any $(k, k+1)$ to a 2-cycle. Note that, the product of two different 2-cycles has order 2 if and only if they are disjoint, otherwise the order is 3. From this, by an inductive arguement one can find a permutation $\tau \in S_n$ such that

$$f((k, k+1)) = (\tau(k), \tau(k+1)),\ \forall k, 1 \leq k \leq n-1.$$

Then, $f = \mathrm{Ad}(\tau)$.

As $G^{(1)}$ is a normal subgroup, by conjugation we have a natural homomorphism $\phi : G \to \mathrm{Aut}(G^{(1)})$. Write $N = \ker \phi$. By Lemma 2,

$$\phi|_{G^{(1)}} : G^{(1)} \to \mathrm{Aut}(G^{(1)})$$

is an isomorphism. Hence, $G = N \rtimes G^{(1)}$. On the other hand, $N = Z_G(G^{(1)})$ commutes with $G^{(1)}$. Thus, $G = N \times G^{(1)}$. Moreover, $N \cong G/G^{(1)}$ is commutative. Therefore, $G^{(1)} = N^{(1)} \times (G^{(1)})^{(1)} = (G^{(1)})^{(1)}$. As $G^{(1)} \cong S_n$, we get $S_n = S_n^{(1)} = A_n$. By counting order, we get a contradiction. □

9 [5分]. 设p是素数，n是正整数。记$k = \mathbb{Z}/p\mathbb{Z}$，它是含有$p$个元素的域。令$G$是$GL_n(k)$的一个子群，则$G$有一个在$V = k^n$ 上的自然作用。假设G是有限p-群，证明G在V上有一个非零的不变向量，也即：存在$0 \neq v \in V$使得

$$g \cdot v = v,\ \forall g \in G.$$

10 [5分]. 设p是奇素数，G是$GL_n(\mathbb{Z})$的子群。假设G是有限p-群，证明G的阶$< p^{\frac{pn}{(p-1)^2}}$。

Proof. Write $p^l = |G|$, $l \in \mathbb{Z}_{\geq 0}$.

Take a primitive root a ($\in \{1, 2, ..., p^2\}$) modulo p^2. By Dirichlet theorem, there exists a prime $q \equiv a \pmod{p^2}$.

Modulo q, there is a natural homomorphism $\phi : G \to \mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$. We show that ϕ is injective. For any $I \neq A \in G$, suppose that $A \in \ker \phi$. Then, there exists $k \geq 1$, $Y \in M_n(\mathbb{Z}) - qM_n(\mathbb{Z})$ such that $A = I + q^k Y$. Then,

$$I = A^{p^l} = (I + q^k Y)^{p^l} \equiv I + q^k p^l Y \pmod{q^{k+1}}.$$

Hence, $p^l Y \in qM_n(\mathbb{Z})$. Due to $(p, q) = 1$ and $Y \in M_n(\mathbb{Z}) - qM_n(\mathbb{Z})$, thus $p^l Y \in M_n(\mathbb{Z}) - qM_n$. This is a contraction.

As ϕ is injective, $G \cong \phi(G) \subset \mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$. Counting order, we get

$$p^l | \prod_{0 \leq j \leq n-1} (q^n - q^j).$$

As $q \equiv a \pmod{p^2}$ is a primitive root modulo p^2, it is a primitive root module p^k for any $k \geq 1$. Therefore, the order of p-power in $\prod_{0 \leq j \leq n-1} (q^n - q^j)$ is equal to

$$\sum_{k \geq 0} [\frac{n}{(p-1)p^k}].$$

Thus,

$$l \leq \sum_{k \geq 0} [\frac{n}{(p-1)p^k}] \leq \sum_{k \geq 0} \frac{n}{(p-1)p^k} = \frac{np}{(p-1)^2}.$$

This is the conclusion we want to show. $\square$