姓名________ 密封装订线

学号________ 密封装订线

班级________ 密封装订线

西南交通大学 2019–2020 学年第 (一) 学期期末试卷（A）

课程代码 6000259 **课程名称** 近世代数 A **考试时间** 120 分钟

题 号	1	2	3	4	5	6	7	总成绩
分 数								

阅卷教师签字：________________________________

考试说明：所有解答中用到的结论，如课程没有涉及，引用时需给出证明。

1. (15 分) 设 $\mathbb{R}^*$ 为非零实数集，定义集合 $G=\mathbb{R}^*\times\mathbb{R}$ 上的一个二元运算如下：

$$(a,b)*(c,d)=(ac,ad+b)$$

证明：

(a). $(G,*)$ 是一个群.

(b). $K=\{(1,b)|b\in\mathbb{R}\}$ 是 G 的正规子群.

证：易见在 G 中，二元运算 $*$ 是封闭的. （1 **分**）

(1). 结合性：(3 **分**)
$((a,b)*(a_1,b_1))*(c,d)=(aa_1,ba_1+b_1)*(c,d)=(aa_1c,ba_1c+b_1c+d)$,
$(a,b)*((a_1,b_1)*(c,d))=(a,b)*(a_1c,b_1c+d)=(aa_1c,ba_1c+b_1c+d)$
$\Longrightarrow ((a,b)*(a_1,b_1))*(c,d)=(a,b)*((a_1,b_1)*(c,d))$

(2). $e=(1,0)$ 是单位元. $(a,b)*(1,0)=(a,b)=(1,0)*(a,b)$ （2 **分**）

(3). $\forall\alpha=(a,b)\in G$, 取 $\beta=(\frac{1}{a},-\frac{b}{a})$, 则 $\alpha*\beta=\beta*\alpha=(1,0)\Longrightarrow\alpha^{-1}=\beta$, 即任意元都有逆元. 因此由定义知 $(G,*)$ 是一群. (2 **分**)

(b). 欲证 K 为 G 的正规子群，只需证明：K 为 G 的子群，并且对任意 $g\in G$, 都有 $gKg^{-1}\subset K$, 实际上：

$$(1,b)*(1,b')^{-1}=(1,b)*(1,-b')=(1,b-b')\in K\Longrightarrow K\text{是子群}\quad (3\textbf{分})$$

$$(a,b)(1,c)(a,b)^{-1}=(a,ac+b)(\frac{1}{a},-\frac{b}{a})=(1,ac)\in K\Longrightarrow K\lhd G\quad (4\textbf{分})$$

2. (15 分) 设 $f: G \longrightarrow H$ 是一个群同态，A 是 G 的一子群. 证明:

(a) $f(A)$ 是 H 的子群;

(b) 商群 $G/\mathrm{Ker}f$ 同构于 G 在 f 下的同态像 $\mathrm{Im}f$.

证:

(a) $\forall \alpha, \beta \in f(A)$, 则 $\exists a, b \in A$ 使得 $\alpha = f(a), \beta = f(b)$, 注意到：$\alpha\beta^{-1} = f(a)(f(b))^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(A)$, 所以 $f(A)$ 是 H 的子群.（7 **分**）

(b)（**若直接用同态基本定理证，只给** 2 **分**）定义映射:

$$\bar{f}: G/\mathrm{Ker}f \longrightarrow Imf$$
$$g\mathrm{Ker}f \longmapsto f(g)$$

现我们证明 $\bar{f}$ 满足以下条件:

(a). $\bar{f}$ 是群同态：实际上，

$$\bar{f}(g_1\mathrm{Ker}f g_2\mathrm{Ker}f) = \bar{f}(g_1g_2\mathrm{Ker}f) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1\mathrm{Ker}f)\bar{f}(g_2\mathrm{Ker}f)\ 4\textbf{分}$$

(b). $\bar{f}$ 是双射（单且满）：满射显然，只需证 $\bar{f}$ 是单的，实际上，

$$\bar{f}(g_1\mathrm{Ker}f) = \bar{f}(g_2\mathrm{Ker}f) \Longrightarrow f(g_1) = f(g_2) \Longrightarrow f(g_1g_2^{-1}) = e_H \Longrightarrow g_1g_2^{-1} \in \mathrm{Ker}f$$

$\Longrightarrow g_1\mathrm{Ker}f = g_2\mathrm{Ker}f$. 故 $\bar{f}$ 是群同构, 从而 $G/\mathrm{Ker}f \cong \mathrm{Im}f$ (4**分**).

3. (15 分) 设 p, q 都是素数，证明：p^2q 阶群必有非平凡的正规子群.

解：由 Sylow 定理：我们有以下两种情形：

(1). 当 $q < p$. 由于 Sylow $-$ p 子群在该群中的指标是 q，易见，q 是群的唯一的最小素因子，从而 $Sylow - q$ 子群是正规子群。（由课后习题）(7 **分**)

(2). 当 $q > p$, $Sylow - q$ 子群的个数 $n_q | p^2$ 且 $n_q \equiv 1 \pmod{q}$. 从而 $n_q = 1, p, p^2$. （2 **分**）

(a) 若 $n_q = 1$, 则 $Sylow - q$ 子群是正规子群. （2 **分**）

(b) 若 $n_q = p$，由于 $q > p$，且 $n_q \equiv 1 \quad (modq) \Longrightarrow n_q \neq p$ （2 **分**）

(c) 若 $n_q = p^2$ 且 $n_q \equiv 1 \quad (modp)$, 则 $Sylow - q$ 子群有 p^2 个，它们都是循环群. 于是有 $p^2(q-1)$ 个 q 阶元，剩下的 $p^2q - p^2(q-1) = p^2$ 个元素正好是一个 $Sylow - p$ 子群, 从而是正规子群.（2 **分**）

4. (15 分) 求环 $\mathbb{Z}/(18)$ 的全部理想，指出其中那些是素理想和极大理想, 并解释为什么?

证明: 由环同态基本定理，$\mathbb{Z}_{18}$ 的理想都是形如: $I/(18)$, 其中 I 是 $\mathbb{Z}$ 的包含理想 (18) 的 $\mathbb{Z}$ 的理想，故 $\mathbb{Z}_{18}$ 的全部理想是:

$$\mathbb{Z}_{18},\quad (2)/(18),\quad (3)/(18),\quad (6)/(18),\quad (9)/(18),\quad (0) \qquad\qquad (7\ \text{分})$$

同理，$\mathbb{Z}_{18}$ 的极大理想都形如: $I/(18)$, 其中 I 满足: $(18) \subset I$, I 是 $\mathbb{Z}$ 的极大理想。由环同态第三定理: $\mathbb{Z}/28/I/(28) \cong \mathbb{Z}/I$. 从而，$I/(28)$ 是极大理想 $\Longleftrightarrow$ $\mathbb{Z}/I$ 是域. 但 $\mathbb{Z}/I$ 是域 $\Longleftrightarrow$ $I = (p)$, p 是素数，只需找 18 的素因子: $2, 3$, 那么由其生成的理想 I 就满足: $(18) \subset I$, I 是 $\mathbb{Z}$ 的极大理想，综上所述，

$$(2)/(18),\quad (3)/(18)$$

为 $\mathbb{Z}_{18}$ 的极大理想. (8 **分**）

5. (15 分) 设 $\mathbb{F}[x]$ 为域 $\mathbb{F}$ 上的多项式环，证明: $\mathbb{F}[x]$ 为主理想整环.

证: 设 $I \neq 0$ 为 $\mathbb{F}[x]$ 的任意一个理想，取 $p(x)$ 为 I 中次数最小的非零次多项式. $\forall f(x) \in I$, 则由多项式带余除法，则存在 $r(x) \in \mathbb{F}[x]$，使得:

$$f(x) = p(x)q(x) + r(x), \quad 0 \leq degr(x) < deg(p(x)) \qquad ((7\ \text{分})$$

$\Longrightarrow r(x) = f(x) - p(x)q(x) \in I$, 从而 $r(x)$ 必须为零多项式. 否则 $r(x) < deg(p(x))$, 这与 $p(x)$ 为 I 中次数最小的非零次多项式相矛盾. 从而，$f(x) = p(x)q(x) \Longrightarrow I = (p(x))$, 即 I 为主理想环. 此外, 若 $f(x)g(x) = 0 \Longrightarrow f(x) = 0$或$g(x) = 0$, 从而 $\mathbb{F}[x]$ 是整环. 总之，$\mathbb{F}[x]$ 是主理想整环. (8 **分**）

6. (10 分) 构造一个有 27 个元的有限域.

解： 由于 $3^3 = 27$, 所以我们考虑多项式环 $\mathbb{Z}_3[x]$, 要构造 27 个元的有限域，只需找一个在域 $\mathbb{Z}_3$ 上一个 3 次不可约多项式 $f(x)$ 即可. 因为

$$\mathbb{Z}_3[x]/(f(x)) \cong \mathbb{Z}_3[\alpha]$$

而 $\mathbb{Z}_3[\alpha]$ 是一个有 27 个元的域。其中 $f(x)$ 为 α 的极小多项式. 为此我们考虑 $f(x) = x^3+2x+1$, 易见，$f(x)$ 是 $\mathbb{Z}_3$ 上的不可约多项式。从而域 $\mathbb{Z}_3[x]/(f(x))$ 即为一个有 27 个元的有限域.

7. (15 分) 设 α 是多项式 $f(x) = x^3 - 6x^2 + 9x + 3$ 的一个实根.

(a) 证明：$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

(b) 求: $(1+\alpha)^{-1}$

证明： （1）由 Eisenstein 判别法知多项式 $f(x) = x^3 - 6x^2 + 9x + 3$ 在 $\mathbb{Q}$ 上不可约，从而 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. （6 **分**）
(2) 设 $(1+\alpha)^{-1} = a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q}$, 则:

$$\begin{aligned} 1 &= (1+\alpha)(a + b\alpha + c\alpha^2) = a + b\alpha + c\alpha^2 + a\alpha + b\alpha^2 + c\alpha^3 \\ &= a + (a+b)\alpha + (b+c)\alpha^2 + c(6\alpha^2 - 9\alpha - 3) \\ &= (a-3c) + (a+b-9c)\alpha + (b+7c)\alpha^2 \qquad (3\ \textbf{分}) \end{aligned}$$

从而我们有以下方程组:

$$\begin{aligned} a - 3c &= 1 \\ a + b - 9c &= 0 \\ b + 7c &= 0 \end{aligned}$$

所以我们得到：$(1+\alpha)^{-1} = \frac{1}{13}(\alpha^2 - 7\alpha + 16)$ （6 **分**）