2021 秋: 代数学一 (实验班) 期末考试

时间：120 分钟　　满分：110 分，最高得分不超过 100 分

所有的环都有乘法单位元, 且与其加法单位元不相等; 所有环同态把 1 映到 1.

All rings contains 1_R and $1_R \neq 0_R$; all ring homomorphism takes 1 to 1.

判断题 (10 分)

1	2	3	4	5	6	7	8	9	10
F	T	F	F	F	T	F	F	T	T

1. 群 G 忠实作用在集合 X 上. 若 $g_1, g_2 \in G$ 和 $x \in X$ 满足 $g_1 \cdot x = g_2 \cdot x$，则 $g_1 = g_2$.

A group G acts faithfully on a set X. If $g_1, g_2 \in G$ and $x \in X$, then $g_1 \cdot x = g_2 \cdot x$ implies $g_1 = g_2$.

False. Even with the faithful condition, it is still possible that the stabilizer group at $x \in X$ is nontrivial, e.g. G may act on $G \sqcup \{x\}$ so that G acts on G by left translation but fixes x. Thus, if g_1 and g_2 are two distinct elements from the stabilizer, $g_1 \cdot x = g_2 \cdot x = x$ yet $g_1 \neq g_2$.

2. 设 H 是群 G 的正规子群. 假设 H 中元素的最大阶 $\leq m$, G/H 中元素的最大阶 $\leq n$. 则 G 中元素的最大阶 $\leq mn$.

Let H be a normal subgroup of a group G. Suppose that the maximal order of elements in H is $\leq m$, and the maximal order of elements in G/H is $\leq n$. Then the maximal order of elements in G is $\leq mn$.

True. Let $g \in G$; denote $\bar{g}$ its image in G/H. Then there exists positive integer $n' \leq n$ such that $\bar{g}^{n'} = 1_{G/H}$. This means that $g^{n'} \in H$. So $(g^{n'})^{m'} = 1_G$ for some $m' \leq m$. This means that the order of g in G is $\leq m'n' \leq mn$.

3. 设 $\varphi : R \to R'$ 为一交换环之间的满同态. 若 R 为整环, 则 $\varphi(R) = R'$ 也为整环.

Let $\varphi : R \to R'$ be a surjective homomorphism of commutative rings. If R is an integral domain, then $\varphi(R) = R'$ is an integral domain.

False. Typically, the property of being an integral domain does not propagate through quotient. For example, $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ is a surjective homomorphism with $\mathbb{Z}$ an integer domain, yet $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

4. 给定环 R 和 R-左模 M, N. 则 $\mathrm{Hom}_R(M, N)$ 也有自然的 R-左模结构.

Let R be a ring and M and N be left R-modules. Then $\mathrm{Hom}_R(M, N)$ is a left R-module.

False. Typically, if R is not commutative, the Hom space $\mathrm{Hom}_R(M,N)$ is merely an abelian group.

5. 在一个唯一分解整环中, 每个非零元都可以唯一的写成素元的乘积.

In a UFD, every nonzero element can be uniquely written as products of prime elements.

False. In a UFD, every nonzero *nonunit* element can be written as products of prime elements *up to associates*. Here "*up to associates*" means that the prime element factorization can be modified by units; and thus not literally unique.

6. 设域 L 是域 F 的扩张, K_1 和 K_2 为中间域. 若 K_1/F 是正规扩张, 则 K_1K_2/K_2 也是正规扩张.

Let L be a field extension of a field F with intermediate fields K_1 and K_2. Suppose that K_1/F is normal, then K_1K_2 is normal over K_2.

True. It is enough to check the case when K_1/F is finite (the general case follows from taking union of the finite cases). As K_1/F is assumed to be normal, it is the splitting field of a polynomial $f(x) \in F[x]$ over F. Then K_1K_2 is the splitting field of the same polynomial $f(x)$ over K_2.

7. 任一指数为 n 的循环扩张 K/F 一定形如 $K = F(\sqrt[n]{a})$ $(a \in F)$.

Every cyclic extension K over F of degree n is of the form $K = F(\sqrt[n]{a})$ for some $a \in F$.

False. On needs F to contain nth roots of unity for this to be true.

8. 设域 L 是域 F 的扩张, K_1 和 K_2 为中间域. 若 K_1 和 K_2 为 F 上的 Galois 扩张, 则 $[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F]$.

Let L be a field extension of a field F with intermediate fields K_1 and K_2. Suppose that K_1 and K_2 are Galois over F. Then $[K_1K_2 : F] = [K_1 : F] \cdot [K_2 : F]$.

False. It is a theorem that $[K_1K_2 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2] \cdot [K_2 : K_1 \cap K_2]$. So the statement holds if and only if $K_1 \cap K_2 = F$.

9. 对任一有限域 F 和正整数 n, (在同构意义下) F 恰有一个次数为 n 的循环扩张.

For any finite field F and any positive integer n, there exists a unique (up to isomorphism) cyclic extension of F of degree n.

True. If $F = \mathbb{F}_q$ for q a power of a prime, then the cyclic extension of F of degree n is $\mathbb{F}_{q^n}$.

10. 若 $f(x) \in F[x]$ 是一个不可约多项式且在一个 F 的扩域中存在单根 α, 则 $f(x)$ 在 F 上的正规闭包在 F 上是 Galois 的.

If $f(x) \in F[x]$ is an irreducible polynomial and there exists a simple zero α of $f(x)$ in some field extension of F, then the normal closure of $f(x)$ over F is Galois over F.

True. If an irreducible polynomial is not separable, all of its zeros have the same multiplicity. So the condition implies that $f(x)$ is separable, and thus its normal closure over F is Galois over F.

解答题一 (12 分) 令 R 是一个交换环. 若所有 R 自由模的子模都是自由的, 则 R 是一个主理想整环.

Let R be a commutative ring. If all submodules of finitely generated free modules over R are free over R, then R is a PID.

证明. First prove that R is an integral domain. Suppose that $a, b \in R\backslash\{0\}$ with $ab = 0$. Consider $aR \subseteq R$; it is a submodule of free module; so aR is a free R-module. However, we know that b kills all of aR because $ab = 0$; this contradicts that aR is a free R-module.

Let $I \subseteq R$ be an ideal; it is then a free R-submodule of R. We claim that I is a free module of rank 1 over R. Suppose not, then there exist $(\alpha_j)_{j\in J}$ forming an R-basis of I. But if $\#J \geq 2$, we know that $\alpha_j \cdot (\alpha_i) + \alpha_i \cdot (-\alpha_j) = 0$, contradiction! This says that I is free of rank one, i.e. I is generated by one element $\alpha \in I$ so that $I = (\alpha)$ is a principal ideal. Thus R is a PID. $\square$

解答题二 (12 分) 是否存在一个有限群 G 使得 $G/Z(G)$ 恰有 143 个元素? (这里 $Z(G)$ 是 G 的中心.)

Is there a finite group G such that $G/Z(G)$ has 143 elements? ($Z(G)$ is the center of G.)

证明. There is no such finite group. Suppose not.

We first study $G/Z(G)$: it is easy to see that the numbers of 11-Sylow subgroups H_{11} and 13-Sylow subgroups H_{13} are $n_{11} = n_{13} = 1$. In particular, both H_{11} and H_{13} are normal. As $H_{11} \cap H_{13} = \{1\}$ and $\#G/Z(G) = 143$. Thus $G/Z(G) \cong H_{11} \times H_{13}$. From this, we deduce that $G/Z(G) \cong Z_{143}$, which is a cyclic group.

Let τ be a generator of $G/Z(G) \cong Z_{143}$. Pick a generator $\tilde{\tau} \in G$ that lies in the coset $\tau Z(G)$. But $\tilde{\tau}$ commutes with all elements in $Z(G)$. Moreover $\tilde{\tau}$ commutes with all powers of $\tilde{\tau}$. So $\tilde{\tau}$ commutes with all elements of G. So $\tilde{\tau}$ commutes with all elements in G; thus $\tilde{\tau} \in Z(G)$. But this contradicts with τ being a generator of $G/Z(G)$. Thus such G does not exist. $\square$

解答题三 (13 分)

设 k 为一有 q 个元素的有限域.

(1) $k[x]$ 中有多少个首一的不可约多项式次数为 $d = 2, 3, 4, 5, 6$?

(2) 一个 5 次 (不一定不可约) k 上多项式分裂域的 Galois 群可能是什么? 为什么?

Let k be a finite field with q elements.

(1) How many monic irreducible polynomials are there in $k[x]$ of each degree $d = 2, 3, 4, 5, 6$?

(2) What are the possible Galois groups of the splitting field of a (not necessarily irreducible) polynomial of degree 5 over k? Why?

证明. (1) Each irreducible polynomial of degree 2 has exact two zeros in $\mathbb{F}_{q^2} - \mathbb{F}_q$; so there are $\frac{q^2-q}{2}$ irreducible polynomials of degree 2.

Similarly, there are $\frac{q^3-q}{3}$ irreducible polynomials of degree 3, and there are $\frac{q^5-q}{5}$ irreducible polynomials of degree 5.

Each irreducible polynomial of degree 4 corresponds to four elements of $\mathbb{F}_{q^4} - \mathbb{F}_{q^2}$; so there are $\frac{q^4-q^2}{4}$ irreducible polynomials of degree 4.

Each irreducible polynomials of degree 6 corresponds to six elements of $\mathbb{F}_{q^6} - \left(\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3}\right)$; there are $\frac{q^6-q^3-q^2+q}{6}$ such polynomials.

(2) The factorization of f into irreducibles correspond to partitions of 5:

If f is irreducible, the splitting field is $\mathbb{F}_{q^5}$. The associated Galois group is Z_5.

If f factors as the product of a degree 2 and a degree 3 polynomials, the splitting field is $\mathbb{F}_{q^6}$.The associated Galois group is Z_6.

In other cases, we can get similarly $\mathbb{F}_{q^4}$, $\mathbb{F}_{q^3}$, $\mathbb{F}_{q^2}$, and $\mathbb{F}_q$. The associated Galois groups are $Z_4, Z_3, Z_2, \{1\}$, respectively. □

解答题四 (13 分)

记 $\alpha = \sqrt{i+2}$ ($i = \sqrt{-1}$).

(1) 计算 α 在 $\mathbb{Q}$ 上的极小多项式 $f(x)$. (需间接或者直接的证明 $f(x)$ 的不可约性.)

(2) 记 F 为 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域. 确定 F 在 $\mathbb{Q}$ 上的 Galois 群.

(3) 写出所有 $\mathrm{Gal}(F/\mathbb{Q})$ 子群和所有 $F/\mathbb{Q}$ 中间域的一一对应图. (此问无需解释过程, 但子群需要用元素或者生成元标注.)

Let $\alpha = \sqrt{i+2}$ where $i = \sqrt{-1}$.

(1) Compute the minimal polynomial $f(x)$ of α over $\mathbb{Q}$. (Need to show the irreducibility of $f(x)$, directly or indirectly.)

(2) Let F be the splitting field of $f(x)$ over $\mathbb{Q}$. Determine the Galois group of F over $\mathbb{Q}$.

(3) Draw the corresponding diagram representing the field extensions of $\mathbb{Q}$ and subgroups of $\mathrm{Gal}(F/\mathbb{Q})$. (No reasoning is needed for (3), but express the subgroups by elements or generators.)

证明. (1) The condition implies that $\alpha^2 = i+2$. Thus $\alpha^2 - 2 = i$, and hence $(\alpha^2-2)^2 = -1$, namely, $\alpha^4 - 4\alpha^2 + 5 = 0$. Write $\alpha = \beta + 1$; we get

$$(\beta+1)^4 - 4(\beta+1)^2 + 5 = 0 \quad \Rightarrow \quad \beta^4 + 4\beta^3 + 2\beta^3 - 4\beta + 2 = 0.$$

This is irreducible by Eisenstein criterion.

(2) Zeros of $f(x)$ are $\alpha_0 = \alpha$, $\alpha_1 = -\sqrt{i+2}$, $\alpha_2 = \sqrt{-i+2}$, and $\alpha_3 = -\sqrt{-i+2}$. Note that $\alpha_0\alpha_2 = \sqrt{i+2}\cdot\sqrt{-i+2} = \sqrt{5}$ and similarly $\alpha_1\alpha_3 = \sqrt{5}$. So the splitting field K of $f(x)$ is obtained by adjoining $\sqrt{5}$ to $\mathbb{Q}(\alpha)$, which is a degree 8 field over $\mathbb{Q}$.

We now investigate the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. First we make explicit the nontrivial element σ of the $\mathrm{Gal}(K/\mathbb{Q}(\alpha))$. It acts by

$$\sigma(\alpha) = \alpha, \qquad \sigma(\sqrt{5}) = -\sqrt{5}.$$

We need another element τ, that is in $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-5}))$ but not in $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{5}, i))$. Then $\tau(\sqrt{5}) = -\sqrt{5}$ and $\tau(i) = -i$. This then forces $\tau(\sqrt{2+i}) = \pm\sqrt{2-i}$. We fix it so that $\tau(\sqrt{2+i}) = \sqrt{2-i}$; then $\sigma\tau\sigma(\sqrt{2+i}) = -\sqrt{2-i}$.

One easily compute

$$\tau\sigma\tau(\sqrt{5}) = -\sqrt{5}, \qquad \tau\sigma\tau(\sqrt{2+i}) = \tau\sigma(\sqrt{2-i}) = \tau\sigma\Big(\frac{\sqrt{5}}{\sqrt{2+i}}\Big) = \tau\Big(\frac{-\sqrt{5}}{\sqrt{2+i}}\Big) = \sqrt{2+i}.$$

$\tau^4 = 1$ and $\tau\sigma\tau = \sigma$. So the group is D_8.

$$\begin{tikzcd}[column sep=small]
 & & K = \mathbb{Q}(\alpha, \sqrt{5}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt{2+i}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2-i}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\sqrt{2+i} + \sqrt{2-i}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2+i} - \sqrt{2-i}) \arrow[dl, dash] \\
 & \mathbb{Q}(i) \arrow[dr, dash] & \mathbb{Q}(\sqrt{-5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
 & & \{1\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \tau^2 \sigma \rangle \arrow[d, dash] & \langle \tau^2 \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle \tau \sigma \rangle \arrow[d, dash] & \langle \tau^3 \sigma \rangle \arrow[dl, dash] \\
 & \langle \sigma, \tau^2 \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \tau\sigma, \tau^2 \rangle \arrow[dl, dash] & \\
 & & D_8 & &
\end{tikzcd}$$

$\square$

解答题五 (10 分) 多项式 $f(x)=\prod_{i=1}^{n}(x-r_i)$ 的判别式为 $\prod_{i<j}(r_i-r_j)^2$. 设 $f(x)\in\mathbb{Q}[x]$ 为一 4 次的首一不可约多项式, 其根为 $\alpha,\beta,\gamma,\delta$.

(1) 证明 $\alpha\beta+\gamma\delta$, $\alpha\gamma+\beta\delta$, $\alpha\delta+\beta\gamma$ 是一个首一三次多项式 $g(x)\in\mathbb{Q}[x]$ 的根, 且它的判别式和 $f(x)$ 的判别式相同.

(2) 简短说明为什么 f 在 $\mathbb{Q}$ 上的 Galois 群是五个群 S_4, A_4, Z_4, D_8, $Z_2\times Z_2$ 之一. (提示: 解答涉及到 S_4 的子群分类, 你需要说明是用什么条件选出的这五个群, 无需证明满足所列条件的群恰好这五个群; 但要说明 $Z_2\times Z_2$ 是具体 S_4 的哪个子群.)

(3) 在哪种上述情况下, 多项式 $g(x)$ 是不可约的?

The *discriminant* of a polynomial $f(x)=\prod_{i=1}^{n}(x-r_i)$ is $\prod_{i<j}(r_i-r_j)^2$. Let $f(x)\in\mathbb{Q}[x]$ be a monic irreducible polynomial of degree 4 with roots $\alpha,\beta,\gamma,\delta$.

(1) Prove that $\alpha\beta+\gamma\delta$, $\alpha\gamma+\beta\delta$, and $\alpha\delta+\beta\gamma$ are roots of a monic cubic polynomial $g(x)\in\mathbb{Q}[x]$ whose discriminant is the same as the discriminant of f.

(2) Give a short explanation of why the Galois group of f over $\mathbb{Q}$ is one of the five groups S_4, A_4, Z_4, D_8, or $Z_2\times Z_2$. (Hint: The solution would involve the classification of subgroups of S_4; you need only to specify the condition that allows you to pin down these groups, but do not need to verify that the subgroups exactly satisfying your conditions are these five groups. However, do explain how $Z_2\times Z_2$ is realized as a subgroup of S_4.)

(3) In which of the above case, is the polynomial g irreducible?

证明. (1) Rewrite $\alpha_1=\alpha,\alpha_2=\beta,\alpha_3=\gamma,\alpha_4=\delta$, and set write $f(x)=x^4-a_1x^3+a_2x^2-a_3x+a_4$. Set $g(x)=(x-\alpha\beta-\gamma\delta)(x-\alpha\gamma-\beta\delta)(x-\alpha\delta-\beta\gamma)$. Either, one can verify directly that however permuting $\alpha,\beta,\gamma,\delta$, $g(x)$ is invariant; or one can compute directly that

$$\begin{aligned}g(x)=x^3-&\sum_{\{i,j\}\subset\{1,2,3,4\}}\alpha_i\alpha_jx^2+\sum_{\{i,j,k\}\subset\{1,2,3,4\}}\alpha_i^2\alpha_j\alpha_kx\\&+\Big(\sum_{i=1}^{4}\alpha_i^2\cdot(\alpha_1\cdots\alpha_4)+\sum_{\{i,j,k\}\subset\{1,2,3,4\}}\alpha_i^2\alpha_j^2\alpha_k^2\Big)\\=&x^3-a_2x^2+(a_1a_3-4a_4)x+\big(a_4(a_1^2-2a_2)+a_3^2-2a_2a_4\big)\end{aligned}$$

The discriminant of $g(x)$ is

$$\begin{aligned}\operatorname{disc}(g)&=\big(\alpha\beta+\gamma\delta-\alpha\gamma-\beta\delta\big)^2\big(\alpha\beta+\gamma\delta-\alpha\delta-\beta\gamma\big)^2\big(\alpha\gamma+\beta\delta-\alpha\delta-\beta\gamma\big)^2\\&=\big((\alpha-\delta)(\beta-\gamma)\big)^2\big((\beta-\delta)(\alpha-\gamma)\big)^2\big((\gamma-\delta)(\alpha-\beta)\big)^2=\operatorname{disc}(f).\end{aligned}$$

(2) The Galois permutes all four roots $\alpha, \beta, \gamma, \delta$ and is thus a subgroup of S_4. For f to be irreducible, we need the action on the four elements to be transitive. The only subgroups of S_4 which acts transitively on these four elements (i.e. not contained in an S_3) are there five groups. Here

$$Z_2 \times Z_2 = \{(12)(34), (13)(24), (14)(23)\}.$$

(3) The polynomial $g(x)$ is irreducible if and only if the action of the Galois group on the set $\{\alpha\beta+\gamma\delta, \alpha\gamma+\beta\delta, \alpha\delta+\beta\gamma\}$ is transitive. The stabilizer group of the element $\alpha\beta+\gamma\delta$ is $\langle(12),(34),(13)(24)\rangle$, which is conjugate to D_8 sitting inside S_4, where the rotation is given by (1423).

So if the Galois group is contained in Z_4, D_8 or $Z_2 \times Z_2$, (after considering conjugations), there exists one element in $\{\alpha\beta+\gamma\delta, \alpha\gamma+\beta\delta, \alpha\delta+\beta\gamma\}$ fixed by this group. In this case, $g(x)$ is reducible. Otherwise, if the Galois group is A_4 or S_4, $g(x)$ is irreducible. $\square$

解答题六 (10 分)

令 p 为一素数. 假设域 F 的每一个有限扩张的次数都被 p 整除. 证明所有 F 的有限扩张的次数都是 p 的幂次.

Let p be a prime integer. Suppose that the degree of every finite extension of a field F is divisible by p. Prove that the degree of every finite extension of F is a power of p.

证明. Let E be a finite separable extension of F and K its Galois closure; write $G := \mathrm{Gal}(K/F)$. Take H to be the p-Sylow subgroup of G, then K^H is an extension of F of degree $[G : H]$, which is prime to p, unless $G = H$. But we have assumed that the degree of every finite extension of F is divisible by p. So $G = H$, and thus any finite separable extension of F has degree a power of p.

If F is perfect, the above already proved the problem. Otherwise, F has an extension of degree $\ell = \mathrm{char}(k)$ given by $F(\sqrt[\ell]{a})$ for some $a \in F \backslash F^\ell$. Thus $\ell = p$. Then all finite extensions of F have degree a power of p.

$\square$

解答题七 (10 分)

设 R 为一唯一分解整环, 其中所有非零素理想皆为极大理想. 证明 R 是一个主理想整环.

Suppose that R is a unique factorization domain (UFD) for which every nonzero prime ideal is maximal. Show that R is a principal ideal domain (PID).

证明. We first prove that for two prime elements p and q, either they are associates, or there exists $a, b \in R$ such that $ap + bq = 1$. Indeed, if p and q are not associates, the ideals (p) and (q) cannot have containment relations (otherwise, say $(p) \subseteq (q)$, we must have $q|p$; which would immediately forces p and q to be associates). Now as nonzero prime ideals (such as (p) and (q)) are maximal, the ideal (p, q) must be the unit ideal, i.e. there exists $a, b \in R$ such that $ap + bq = 1$.

Next, we show that if, in the factorization of two elements $c, d \in R$, no prime factors of c are associates of prime factors of d, then there exists $a, b \in R$ such that $ac + bd = 1$. By induction, it suffices to prove that: if $(p_1, q) = (p_2, q) = (1)$, then $(p_1p_2, q) = (1)$. Indeed, write $\lambda_1 p_1 + \mu_1 q = 1$ and $\lambda_2 p_2 + \mu_2 q = 1$ for $\lambda_1, \lambda_2, \mu_1, \mu_2 \in R$, then

$$\lambda_1\lambda_2 p_1 p_2 = (1 - \mu_1 q)(1 - \mu_2 q) = 1 - (\mu_1 + \mu_2 - \mu_1\mu_2 q)q$$

This implies that $(p_1p_2, q) = (1)$.

We finally prove that R is a PID. Let I be a nonzero ideal. Pick an element $x \in I$ with minimal number of prime factors. We show that $I = (x)$. If $y \in I \backslash (x)$, then write $d = \gcd(x, y)$ and $x = dx_d$ and $y = dy_d$ with $x_d, y_d \in R$, and x_d, y_d have distinct prime factors. By the discussion above, there exist $a, b \in R$ such that $ax_d + by_d = 1$. This implies that $d \in I$, contradicting with the minimality of prime factors of $x \in I$. Thus I is a principal ideal. $\square$

解答题八 (10 分)

设群 G 由两个元素生成.

(1) 证明 G 至多有 17 个指数为 3 的子群. (提示: 考虑从 G 到 S_3 的同态.)

(2) 证明 G 至多有 13 个指数为 3 的子群.

注: 你可以直接证明 (2). 事实上, 存在这样的群 G 恰有 13 个指数为 3 的子群, 但你不需要证明这个.

Let G be a group which is generated by two elements.

(1) Prove that G has at most 17 subgroups of index 3. (Hint: think about homomorphisms from G to S_3.)

(2) Prove that G has at most 13 subgroups of index 3.

Remark: Clearly, you can choose to prove (2) directly. In fact, there exists a such group G with exactly 13 *subgroups of index* 3*; but you do not need to prove that.*

证明. For each such group H of G of index 3, write the set of cosets by $\{H, aH, bH\}$. Then we can associate *two* homomorphisms $\varphi_{H,1}, \varphi_{H,2} : G \to S_3$ given by the left multiplication on $\{H, aH, bH\}$. (Here, we identify H with 1, and these are two ways to identify aH and bH with 2 and 3; hence the two homomorphisms.) So these two homomorphisms are conjugate by (23).

We may recover H from $\varphi_{H,1}$ and $\varphi_{H,2}$ by taking the preimage of $\{1, (23)\}$ under either $\varphi_{H,1}$ and $\varphi_{H,2}$, namely the subgroup of S_3 that fixes 1. In other words,

$$\{\text{subgroups of } G \text{ of index } 3\} \hookrightarrow \{\text{homomorphisms } \varphi : G \to S_3\}/\text{conjugation}$$

As G is generated by two elements $x, y \in G$, the homomorphism $\varphi : G \to S_3$ is determined by $\varphi(x), \varphi(y) \in S_3$. Moreover, since G acts transitively on $\{H, aH, bH\}$, the images of $\varphi(x), \varphi(y)$ in S_3 cannot be contained in a proper subgroup of S_3. All such possible pairs $(\varphi(x), \varphi(y)) \in (S_3)^2$ have

$$6^2 - 3 \cdot 2^2 + 2 = 26$$

possibilities. Modulo the conjugation action, there are 13 possible pairs of homomorphisms. Thus, there are at most 13 subgroups H of G of index 3. $\square$

解答题九 (5 分)

令 k 为一特征为 $p>0$ 的完美域. 设 $F=k(t)$ 为 k 上单变元的函数域. 证明 F 的任一有限扩张 E 都是单扩张, 即存在 $\alpha\in E$ 使得 $E=F(\alpha)$.

Let k be a perfect field of characteristic $p>0$. Let $F=k(t)$ be the field of rational functions in one variable over k. Show that every finite extension E of F can be generated by one element, that is, there exists $\alpha\in E$ such that $E=F(\alpha)$.

证明. We first remark that by the proof of primitive element theorem, a finite separable extension can be generated by one element.

Let E be a finite extension of $F=k(t)$, we need to show that E is generated by one element over F. We prove by induction on $[E:F]$. We will show that

(1) either E/F is separable,

(2) or $k(t^{1/p})\subseteq E$.

Suppose that we have proved this. Then in case (1), the separable extension E/F is generated by one element. In case (2), E is a finite extension of $k(t^{1/p})$. Write $u=t^{1/p}$; then E is a finite extension of $k(u)$. By inductive hypothesis, $E=k(u)(\alpha)$. Let $f(x)\in k(u)[x]$ be the minimal polynomial of α over $k(u)$; write $f(x)=x^n+a_{n-1}(u)x^{n-1}+\cdots+a_0(u)$. Then $(f(x))^p=x^{pn}+a_{n-1}(u)^p x^{p(n-1)}+\cdots+a_0(u)^p\in F[x]$ is the minimal polynomial of α over $k(t)$. (This can be seen as follows: clearly, $f(\alpha)^p=0$; if $(f(x))^p$ factors nontrivially as $g(x)h(x)\in F[x]$, then viewing $g(x),h(x)\in k(u)[x]$, we see that they must be powers of $f(x)$. Contradiction.)

Now we prove that one of (1) and (2) happens. Suppose that (2) does not hold; we prove (1). It suffices to show that each $\alpha\in E$ is separable over F. Suppose some α is not separable over F; let $f(x)$ be the minimal polynomial. By a theorem from the class, $f(x)=g(x^p)$ for some $g(x)=x^n+a_{n-1}(t)x^{n-1}+\cdots+a_0(t)\in F[x]$. As k is perfect, there exists $b_i(t^{1/p})\in k(t^{1/p})$ such that $b_i(t^{1/p})^p=a_i(t)$. So the minimal polynomial of α over $k(t^{1/p})$ divides $x^n+b_{n-1}(t^{1/p})x^{n-1}+\cdots+b_0(t^{1/p})$. Note that

$$p\cdot\deg g\geq [k(t^{1/p})(\alpha):k(t^{1/p})][k(t^{1/p}):k(t)]=[k(t^{1/p})(\alpha):F(\alpha)]\cdot[F(\alpha):F]=[k(t^{1/p})(\alpha):F(\alpha)]\cdot\deg f.$$

It follows that $k(t^{1/p})(\alpha)=F(\alpha)$; thus $F(\alpha)$ contains $k(t^{1/p})$, proving (2). $\square$

解答题十 (5 分)

设域 F 满足 $\mathbb{Q} \subseteq F \subset \mathbb{C}$, 是一个 $\mathbb{Q}$ 上的有限交换 Galois 扩张. 设 $\alpha \in F$ 的极小多项式为 $f(x) \in \mathbb{Q}[x]$, 且满足 $|\alpha| = 1$.

(1) 证明 F 在复共轭下保持稳定.
(2) 证明 $f(x)$ 的任一复根 β 满足 $|\beta| = 1$.
(3) 记 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, 证明对所有 $0 \leq i < n$, $|a_i| \leq 2^n$.
(4) 证明 F 只包含有限多个绝对值为 1 的代数整数 (即满足极小多项式的系数为整数的 F 中的元素).
(5) 证明 (4) 中的这些代数整数都是单位根.

Let F be a field with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, where $F/\mathbb{Q}$ is a finite *abelian* Galois extension. Let $\alpha \in F$ and let $f(x) \in \mathbb{Q}[x]$ be its minimal monic polynomial. Assume that $|\alpha| = 1$.

(1) Show that F is closed under complex conjugation.
(2) Prove that $|\beta| = 1$ for every complex root β of $f(x)$.
(3) Writing $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, show that $|a_i| \leq 2^n$ for all i with $0 \leq i < n$.
(4) Prove that F contains only finitely many algebraic integers (i.e. elements in F whose minimal polynomial over $\mathbb{Q}$ have coefficients in $\mathbb{Z}$) having absolute value 1.
(5) Deduce that each of the algebraic integers in (4) is a root of unity.

证明. (1) As F is Galois over $\mathbb{Q}$, the Kronecker–Weber theorem implies that F is contained in $\mathbb{Q}(\zeta_N)$ for some N. The complex conjugation belongs to $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ must stabilize any Galois extension of $\mathbb{Q}$. So F is stable under complex conjugation.

In particular, this means that the complex conjugation c may be viewed as an element in $\mathrm{Gal}(F/\mathbb{Q})$.

(2) As $f(x)$ is irreducible, there exists $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ that takes α to β. Moreover, since $\mathrm{Gal}(F/\mathbb{Q})$ is abelian, c and σ commutes. So

$$|\alpha| = 1 \quad \Rightarrow \quad \alpha c(\alpha) = 1 \quad \Rightarrow \quad \sigma(\alpha)\sigma(c(\alpha)) = 1 \quad \Rightarrow \quad \sigma(\alpha)c(\sigma(\alpha)) = 1.$$

This shows that $|\beta| = 1$.

(3) As $f(x) = \prod_{i=1}^n (x - \alpha_i)$ with each $|\alpha_i| \leq 1$. Expand this out, it is easy to see that each $|a_i| \leq 2^n$.

(4) If $\alpha \in F$ is an algebraic integer with absolute value 1, its minimal polynomial must be of the form above (with degree $n \leq [F : \mathbb{Q}]$; so the coefficients have absolute value $\leq 2^n$. So there are finitely many such polynomials, and hence finitely many such α's.

(5) For each α above, consider $1, \alpha, \alpha^2, \ldots$. They are all algebraic integers with absolute value 1. But there are only finitely many such elements. We must have $\alpha^i = \alpha^j$ for some $i \neq j$. Thus $\alpha^{j-i} = 1$ and α is a root of unity.

$\square$