MAST30005 Assignment 2

Chengjing Zhang

June 4, 2019

Throughout this assignment, we follow the notations from Artin's book. Notation $R[a, b]$ is defined by sending x_1 and x_2 of the polynomial ring $R[x_1, x_2]$ to a and b respectively. Notation $R(a, b)$ is the smallest field which contains both a and b. In Artin's book, it is proved that $R[a, b] = R(a, b)$ if a and b are both algebraic over R.

1 Question 1

Let $F \subseteq K$ be a field extension. We say that K is algebraic over F if every element of K is algebraic over F. Prove that K is algebraic over F if and only if every subring $R \subseteq K$ containing F is also a field.

Definition 1. Let $F \subseteq K$ be a field extension. We say that K is algebraic over F if every element of K is algebraic over F.

Proposition 2. *Let $F \subseteq K$ be a field extension, then K is algebraic over F if and only if every subring $R \subseteq K$ containing F is also a field.*

Proof. First, we show that if K is algebraic over F, then every subring $R \subseteq K$ containing F is also a field.

Condiser an element $\alpha \in R \subseteq F$. If $\alpha \in F$, then $\alpha^{-1} \in F \subseteq R$. If $\alpha \notin F$, since $\alpha \in R \subseteq K$, we have α is algebraic over F, so there exists an irreducible polynomial $p(x)$ of degree $n \in \mathbb{N}$ such that α is a root of $p(x)$, thus $[F(\alpha) : F] = n$ and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis of $F(\alpha)$ over F. The element α is algebraic over F, so $F(\alpha)$ is a field, it follows that $\alpha^{-1} \in F(\alpha)$. Since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis of $F(\alpha)$ over F, there exists $a_0, a_1, \ldots, a_{n-1} \in F$ such that

$$\alpha^{-1} = a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}. \tag{1}$$

We know that R is a ring and $x \in R$, thus $1, x, \ldots, x^{n-1}$ are all in R, hence $\alpha^{-1} \in R$. Therefore, for any $\alpha \in R$, we have $\alpha^{-1} \in R$, hence R is a field.

Next, we show that K is algebraic over F if every subring $R \subseteq K$ containing F is also a field.

Consider an element $\alpha \in K$. If $\alpha \in F$, then α is algebraic over F since it is the root of $x - \alpha \in F[x]$. If $\alpha \notin F$, then $F[\alpha]$ is a subring of K, hence it is a field. Since $\alpha \notin F$, it cannot be 0, hence $\alpha^{-1} \in F[\alpha]$. Therefore, there exists an integer $n \in \mathbb{N}$ and $n + 1$ coefficients $a_0, \ldots, a_n \in F$ such that

$$\alpha^{-1} = a_0 + a_1\alpha + \cdots a_n\alpha^n. \tag{2}$$

Multiplying the two sides of Equation (2) by α gives

$$1 = a_0\alpha + a_1\alpha^2 + \cdots + a_n\alpha^{n+1}, \tag{3}$$

i.e.

$$a_n\alpha^{n+1} + \cdots + a_0\alpha - 1 = 0. \tag{4}$$

Hence α is a root of polynomial $p(x) = a_n\alpha^{n+1} + \cdots + a_0\alpha - 1$, thus α is algebraic over F. Therefore, any element $\alpha \in K$ is algebraic over F, so K is algebraic over F. □

2 Question 2

Assume that $e \in \mathbb{R}$ is transcendental over $\mathbb{Q}$, and let $K \subset \mathbb{R}$ be an algebraic extension of $\mathbb{Q}$. Prove that e is transcendental over K.

Lemma 3. *If $e \in \mathbb{R}$ is transcendental over $\mathbb{Q}$, and $K \subset \mathbb{R}$ is an algebraic extension of $\mathbb{Q}$, then e is transcendental over K.*

Proof. We prove the lemma by contradiction.

Assume e is algebraic over K, then there exists an irreducible polynomial $p(x) = a_n x^n + \cdots a_1 x + a_0 \in K[x]$ such that e is a root of $p(x)$, where $a_0, \ldots, a_n \in K$.

For conevience, we write $\mathbb{Q}(a_0, \ldots, a_i)$ as E_i for i between 0 and n. Since K is an algebraic field extension of $\mathbb{Q}$, the coefficients $a_0, \ldots, a_n \in K$ are all algebraic over $\mathbb{Q}$, so for any i between 1 and n, there exists a polynomial $p_i(x) \in \mathbb{Q}[x]$ of degree n_i such that a_i is a root of $p(x)$. Since $p_i(x) \in \mathbb{Q}[x]$, it follows that $p_i(x) \in E_{i-1}[x]$, so the degree of a_i over E_{i-1} is also finite, hence $[E_i : E_{i-1}] < \infty$ for all i between 1 and n. Considering the field extension chain $\mathbb{Q} \subset E_0 \subset \cdots \subset E_n$, we have

$$[E_n : \mathbb{Q}] = [E_0 : \mathbb{Q}] \cdot [E_1 : E_0] \cdots [E_n : E_{n-1}] < \infty.$$

Since $a_0, \ldots, a_n \in E_n$, we have $p(x) \in E_n[x]$.

By assumption, e is a root of $p(x)$, hence e is algebraic over E_n. The degree of $p(x)$ over E_n is n, and e is a root of $p(x)$, hence $[E_n(e) : E_n] \leq n$, therefore

$$[E_n(e) : \mathbb{Q}] = [E_n : \mathbb{Q}] \cdot [E_n(e) : E_n] < \infty.$$

Since $\mathbb{Q} \subset \mathbb{Q}(e) \subset E_n(e)$, hence $[\mathbb{Q}(e) : \mathbb{Q}] < \infty$, i.e. the degree of e over $\mathbb{Q}$ is also finite, thus e is algebraic over $\mathbb{Q}$, which contradicts to the given condition that e is transcendental over $\mathbb{Q}$. Therefore, e is transcendental over K. □

3 Question 3

Let $K = \mathbb{Q}[i, \sqrt[4]{2}]$.

3.1 Part A

Show that K is a splitting field of $X^4 - 2$ over $\mathbb{Q}$.

Lemma 4. *The field K is a splitting field of $X^4 - 2$ over $\mathbb{Q}$.*

Proof. Since i is a root of $X^2+1 \in \mathbb{Q}[x]$, and $\sqrt[4]{2}$ is a root of $X^4-2 \in \mathbb{Q}[x]$, both i and $\sqrt[4]{2}$ are algebraic over $\mathbb{Q}$, hence $\mathbb{Q}[i, \sqrt[4]{2}] = \mathbb{Q}(i, \sqrt[4]{2})$.

Since

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2}),$$

and $-\sqrt[4]{2}, \sqrt[4]{2}, -i\sqrt[4]{2}, i\sqrt[4]{2} \in \mathbb{Q}(i, \sqrt[4]{2})$, the polynomial X^4-2 can be facterized into linear factors in $\mathbb{Q}(i, \sqrt[4]{2})$.

Any field L where X^4-2 can be facterized into linear factors must contain $\sqrt[4]{2}$ and $i\sqrt[4]{2}$, and therefore must contain $i\sqrt[4]{2}/\sqrt[4]{2} = i$. By the definition of $\mathbb{Q}(i, \sqrt[4]{2})$, we have $\mathbb{Q}(i, \sqrt[4]{2}) \subseteq L$. Therefore, $\mathbb{Q}(i, \sqrt[4]{2}) = \mathbb{Q}[i, \sqrt[4]{2}]$ is a splitting field of X^4-2 over $\mathbb{Q}$. □

3.2 Part B

Find a $\mathbb{Q}$-basis of K.

Lemma 5. *The set* $\mathcal{P} = \{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{8}\}$ *forms a* $\mathbb{Q}$*-basis of* K*.*

Proof. We know that $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[x]/(x^4-2)$, so $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Since i is a root of $x^2+1 \in \mathbb{Q}(\sqrt[4]{2})[x]$, the degree of i over $\mathbb{Q}(\sqrt[4]{2})$ is at most 2. We also know that $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, and $i \notin \mathbb{R}$, thus $i \notin \mathbb{Q}(\sqrt[4]{2})$, so the degree of i over $\mathbb{Q}(\sqrt[4]{2})$ is not 1. Therefore, the degree of i over $\mathbb{Q}(\sqrt[4]{2}) = 2$, so $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$.

Since $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[x]/(x^4-2)$, the set $\mathcal{B} = \{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt[4]{2})$. Also from $\mathbb{Q}(i, \sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2})(i) \cong \mathbb{Q}(\sqrt[4]{2})/(x^2+1)$, we know that $\mathcal{C} = \{1, i\}$ forms a $\mathbb{Q}(\sqrt[4]{2})$-basis of $\mathbb{Q}(i, \sqrt[4]{2})$.

In the proof of degree theorem, we have shown that the set of products of one element from $\mathcal{B}$ and one element from $\mathcal{C}$ forms a $\mathbb{Q}$-basis of K, which is exactly $\mathcal{P}$. □

3.3 Part C

Find an automorphism of order four of K over $\mathbb{Q}[i]$.

Solution: First, we know that both $\sqrt[4]{2}$ and $i\sqrt[4]{2}$ are algebraic over $\mathbb{Q}[i]$ since they are both roots of $x^4-2 \in \mathbb{Q}[i]$. Therefore, $\mathbb{Q}[i][\sqrt[4]{2}] = \mathbb{Q}[i](\sqrt[4]{2})$ and $\mathbb{Q}[i][i\sqrt[4]{2}] = \mathbb{Q}[i](i\sqrt[4]{2})$. Then since $\sqrt[4]{2} = -i(i\sqrt[4]{2}) \in \mathbb{Q}[i][i\sqrt[4]{2}]$, hence $\mathbb{Q}[i](\sqrt[4]{2}) \subset \mathbb{Q}[i][i\sqrt[4]{2}]$. Similarly, since $i\sqrt[4]{2} = i\sqrt[4]{2} \in \mathbb{Q}[i][\sqrt[4]{2}]$, we also have $\mathbb{Q}[i](i\sqrt[4]{2}) \subset \mathbb{Q}[i][\sqrt[4]{2}]$. Therefore, $\mathbb{Q}[i][\sqrt[4]{2}] = \mathbb{Q}[i][i\sqrt[4]{2}]$. By definition of polynomial ring, we have $K = \mathbb{Q}[i][\sqrt[4]{2}] = \mathbb{Q}[i][i\sqrt[4]{2}]$.

Since there exists a homomorphism $f_1 : \mathbb{Q}[i][x] \to \mathbb{Q}[i][\sqrt[4]{2}]$, which sends x to $\sqrt[4]{2}$, by universal property of polynomial rings and quotient rings, there exists a homomorphism $\phi_1 : \mathbb{Q}[i][x]/(x^4-2) \to \mathbb{Q}[i][\sqrt[4]{2}]$, which sends the coset of x to $\sqrt[4]{2}$. Also, $(\sqrt[4]{2})^4 - 2 = 0$, so $(x^4-2) \subseteq \ker(f)$. Since polynomial rings are PID, and (x^4-2) is irreducible, (x^4-2) is therefore maximal. We know that $\ker(f)$ is also an ideal, and clearly $\ker(f) \neq \mathbb{Q}[i][x]$, so $\ker(f) = (x^4-2)$. By first isomorphism theorem, ϕ_1 is therefore an isomorphism, which sends the coset of x to $\sqrt[4]{2}$. Similarly, there exists a isomorphism $\phi_2 : \mathbb{Q}[i][x]/(x^4-2) \to \mathbb{Q}[i][i\sqrt[4]{2}]$, which sends the coset of x to $i\sqrt[4]{2}$.

Since ϕ_1 and ϕ_2 are both isomorphism, $\psi = \phi_1^{-1}\phi_2 : \mathbb{Q}[i][\sqrt[4]{2}] \to \mathbb{Q}[i][i\sqrt[4]{2}]$ is also an isomorphism. We have shown that $K = \mathbb{Q}[i][\sqrt[4]{2}] = \mathbb{Q}[i][i\sqrt[4]{2}]$, so ψ is an automorphism of K. Since the construction of K comes from a polynomial

ring $\mathbb{Q}[i][x]$, the elements of $\mathbb{Q}[i]$ in K are from the monomials of degree 0 and $4k$, where $k \in \mathbb{N}$, which are not influenced by ψ, so ψ fixes $\mathbb{Q}[i]$.

Then we check the order of ψ. Applying ψ once sends $\sqrt[4]{2}$ to $i\sqrt[4]{2}$. Applying ψ twice sends $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. Applying ψ thrice sends $\sqrt[4]{2}$ to $-i\sqrt[4]{2}$. Applying ψ four times sends $\sqrt[4]{2}$ to $\sqrt[4]{2}$ back. Therefore, ψ is an automorphism of order four of K over $\mathbb{Q}[i]$.

3.4 Part D

Determine all the automorphisms of K over $\mathbb{Q}$.

Solution: From main theorem of Galois theory, we know that $|G(K|\mathbb{Q})| = 8$. We also know that $G(K|\mathbb{Q}) \subset S_4$, so it is a Sylow 2-subgroup of S_4. By Sylow's theorem, all Sylow 2-subgroups are isomorphic. We also know that dihedral group D_4 is a Sylow 2-subgroup of order 8, therefore $G(K|\mathbb{Q}) \cong D_4$.

All the roots of $X^2 - 4$ are of the form $\alpha_j = i^j \sqrt[4]{2}$, where $1 \leq j \leq 4$, this gives an automorphism of order 4:

$$\begin{aligned} \sigma : i &\longmapsto i \\ \sqrt[4]{2} &\longmapsto i\sqrt[4]{2}. \end{aligned}$$

We also have an automorphism of order 2:

$$\begin{aligned} \tau : i &\longmapsto -i \\ \sqrt[4]{2} &\longmapsto \sqrt[4]{2}. \end{aligned}$$

So far, we have got the generators of $G(K|\mathbb{Q})$, which are σ and τ, then we have $G(K|\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$, where 1 is the identity automorphism.

Moreover, we can also clarify how these elements permute the roots, written with the exponent j: $1 = (1)$, $\sigma = (1234)$, $\sigma^2 = (13)(24)$, $\sigma^3 = (1432)$, $\tau = (13)$, $\tau\sigma = (12)(34)$, $\tau\sigma^2 = (24)$, $\tau\sigma^3 = (14)(23)$.

3.5 Part E

The zeros of $X^4 - 2$ form the set $S = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Describe the action of $\mathrm{Aut}(K|\mathbb{Q})$ on S.

Solution: In part d, we have shown that $G(K|\mathbb{Q}) = \mathrm{Aut}(K|\mathbb{Q}) \cong D_4$. We also know that the four elements of S forms a square on the complex plane. Therefore, the action of $\mathrm{Aut}(K|\mathbb{Q})$ is actually applying rotations or reflections on the square whose vertices are the elements of S.

3.6 Part F

Find all subgroups of $\mathrm{Aut}(K|\mathbb{Q})$.

Solutions: We have shown that $\mathrm{Aut}(K|\mathbb{Q}) \cong D_4$. By Lagrange's theorem, all the subgroups of D_4 are of order 1, 2, 4, or 8. First, we have the trivial subgroups 1 and $\mathrm{Aut}(K|\mathbb{Q})$. There are five subgroups of D_4 of order 2, so the subgroups of order 2 of $\mathrm{Aut}(K|\mathbb{Q})$ are $H_1^{(2)} = \{1, \tau\}$, $H_2^{(2)} = \{1, \tau\sigma\}$, $H_3^{(2)} = \{1, \tau\sigma^2\}$, $H_4^{(2)} = \{1, \tau\sigma^3\}$ $H_5^{(2)} = \{1, \sigma^2\}$. There are three subgroups of D_4 of order 4, so the subgroups of order 4 of $\mathrm{Aut}(K|\mathbb{Q})$ are $H_1^{(4)} = \{1, \sigma, \sigma^2, \sigma^3\}$, $H_2^{(4)} = \{1, \sigma^2, \tau, \tau\sigma^2\}$ and $H_3^{(4)} = \{1, \sigma^2, \tau\sigma, \tau\sigma^3\}$.

3.7 Part G

Find all intermediate field extensions of $\mathbb{Q} \subset K$.

Solutions: From Galois theory, we know that any intermediate field extension corresponds to a subgroup of $\mathrm{Aut}(K|\mathbb{Q})$. Also, we know that all the degrees of the intermediate field extensions should divides the degree of $\mathbb{Q} \subset K$, therefore the intermediate field extensions can only be of degree 2 or 4.

We know that the trivial subgroup $\{1\}$ corressponds to K itself, since the order of it is 1. The other trivial subgroup $\mathrm{Aut}(K|\mathbb{Q})$ corresponds to $\mathbb{Q}$, since the order of it is exactly $|\mathrm{Aut}(K|\mathbb{Q})|$. These two are not intermediate field extensions.

Then we consider all the subgroups of order four. By main theorem of Galois theory, they corresponds to intermediate field extensions of degree two over $\mathbb{Q}$. Since i, $\sqrt{2}$, $i\sqrt{2}$ are roots of x^2+1, x^2-2, x^2+2 respectively. The three field extensions $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i\sqrt{2}]$ are all field extensions of degree two. By definiton of σ, we can see that $H_1^{(4)}$ fixes $\mathbb{Q}[i]$. By applying the elements of $H_2^{(4)}$ and $H_3^{(4)}$ to $\sqrt{2}$ and $i\sqrt{2}$, we can get that $H_2^{(4)}$ corresponds to $\mathbb{Q}[\sqrt{2}]$ and $H_3^{(4)}$ corresponds to $\mathbb{Q}[i\sqrt{2}]$. By the main theorem of Galois theory, there is no other intermediate field extensions of degree two.

Then we consider the field extension of degree four over $\mathbb{Q}$. From the definition of τ we know that $H_1^{(2)}$ fixes $\mathbb{Q}[\sqrt[4]{2}]$. From the description of the action of $\mathrm{Aut}(K|\mathbb{Q})$ on S in part e, we can also find the field extensions corresponding to $H_2^{(2)}$, $H_4^{(2)}$ and $H_3^{(2)}$ are $\mathbb{Q}[(i-1)\sqrt[4]{2}]$, $\mathbb{Q}[i\sqrt[4]{2}]$ and $\mathbb{Q}[(i+1)\sqrt[4]{2}]$ respectively. Since $H_5^{(2)}$ is a subgroup of all the subgroups of $\mathrm{Aut}(K|\mathbb{Q})$ of order four, the field extension corresponding to it has to be an intermediate extension of all the three field extensions of degree two. We can check that σ^2 fixes $(1+i)\sqrt{2}$, so $H_5^{(2)}$ corresponds to $\mathbb{Q}[(1+i)\sqrt{2}] = \mathbb{Q}[i,\sqrt{2}]$.

So far, we have got all the intermediate field extensions of $\mathbb{Q} \subset K$. The field extensions of degree two are $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[i\sqrt{2}]$. The field extensions of degree four are $\mathbb{Q}[\sqrt[4]{2}]$, $\mathbb{Q}[(i-1)\sqrt[4]{2}]$, $\mathbb{Q}[i\sqrt[4]{2}]$, $\mathbb{Q}[(i+1)\sqrt[4]{2}]$ and $\mathbb{Q}[(1+i)\sqrt{2}]$.

4 Question 4

Prove $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Lemma 6. $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$.

Proof. Since $\sqrt{2}$ is a root of $X^2-2=0$, $\sqrt{3}$ is a root of $X^2-3=0$, and $\sqrt{2}+\sqrt{3}$ is a root of $X^4-10X^2+1=0$, they are all algebraic over $\mathbb{Q}$, hence $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Since $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, and any $\alpha \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ can be represented as $\alpha = a_0 + a_1(\sqrt{2}+\sqrt{3}) + \cdots a_n(\sqrt{2}+\sqrt{3})^n$, where $a_0,\ldots,a_n \in \mathbb{Q}$, hence α is also in $\mathbb{Q}[\sqrt{2},\sqrt{3}]$, so $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subseteq \mathbb{Q}[\sqrt{2},\sqrt{3}]$.

Since $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a field, we have $\sqrt{3}-\sqrt{2} = (\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since $\frac{1}{2}(\sqrt{3}-\sqrt{2}) + \frac{1}{2}(\sqrt{2}+\sqrt{3}) = \sqrt{3}$, we have $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Similarly, $\sqrt{2} = \frac{1}{2}(\sqrt{2}+\sqrt{3}) - \frac{1}{2}(\sqrt{3}-\sqrt{2}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. By the definition of $\mathbb{Q}(\sqrt{2},\sqrt{3})$, it follows that $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Therefore $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. □

5 Transcendental numbers

5.1 Part A

Prove that the set of all algebraic numbers over $\mathbb{Q}$ is countable.

Proposition 7. *Let A be the set of all algebraic numbers over $\mathbb{Q}$, then A is countable.*

Proof. If $\alpha \in A$, then there exists a monic irreducible polynomial $p(x) = x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ such that α is a root of $p(x)$.

Since for all $0 \leq i < n$, we have $a_i \in \mathbb{Q}$, i.e. there exists $m_i, n_i \in \mathbb{Z}$ such that $a_i = m_i/n_i$. Multiplying $p(x)$ by $\prod_{i=0}^{n-1} n_i$ gives a new polynomial

$$p'(x) = p(x) \prod_{i=0}^{n-1} n_i = x^n \prod_{i=0}^{n-1} n_i + \cdots + m_0 \prod_{i=1}^{n-1} n_i \in \mathbb{Z}[x].$$

Let a_i' be the coefficient of x_i in $p'(x)$, i.e. write $p'(x)$ as $p'(x) = a_n' x^n + \cdots a_0'$, then $a_i' \in \mathbb{Z}$. Since α is a root of $p(x)$, it is also a root of $p'(x)$.

Sort the roots of $p'(x)$ by absolute value from small to big, and treat multiple roots of $p'(x)$ as a single root, we get a list of at most n numbers, and α is the k-th root in this list, where $1 \leq k \leq n$. Then we can define a function $f : A \to \mathbb{N}$ as

$$f(\alpha) = 2^k \cdot 3^{a_0'} \cdots p_{n+2}^{a_n'},$$

where p_i is the i-th prime number.

If $f(\alpha) = f(\alpha')$, then they must be the roots of the same polynomial with the same index k, i.e. $\alpha = \alpha'$, hence f is injective. By the definition of countable set, A is therefore countable. □

5.2 Part B

Prove that the set of real numbers $\{\log(p) | p \text{ is prime.}\}$ is linearly independent over $\mathbb{Q}$.

Lemma 8. *The set of real numbers $P = \{\log(p) | p \text{ is prime.}\}$ is linearly independent over $\mathbb{Q}$.*

Proof. We prove this lemma by contradiction.

If P is linearly dependent over $\mathbb{Q}$, then there exist different prime numbers $p_1, \ldots, p_n$ and $a_1, \ldots, a_n \in \mathbb{Q}$ such that

$$a_1 \log(p_1) + \cdots + a_n \log(p_n) = 0, \tag{5}$$

for some $a_i \neq 0$. For $1 \leq i \leq n$, since $a_i \in \mathbb{Q}$, there exists $m_i, n_i \in \mathbb{Z}$ such that $a_i = m_i/n_i$, multiplying Equation (5) by $\prod_{i=1}^{n} n_i$ gives

$$\log(p_1) m_1 \prod_{i=2}^{n} n_i + \cdots \log(p_n) m_n \prod_{i=1}^{n-1} n_i = 0. \tag{6}$$

Write the coefficient of $\log(p_i)$ as a_i', clearly $a_i' \in \mathbb{Z}$. Then from Equation (6), we have

$$p_1^{a_1'} \cdots p_n^{a_n'} = 1, \tag{7}$$

for some $a_i' \neq 0$. Since each of p_i's is prime, we must have $a_i = 0$ for all i. Therefore, P is linearly independent over $\mathbb{Q}$. □

5.3 Part C

Use your result from (a) to prove the existence of transcendental numbers.

Proposition 9. *Transcendental number exists.*

Proof. If transcendental number does not exist, then all real numbers are algebraic over $\mathbb{Q}$, i.e. $A = \mathbb{R}$. By Lemma 7, $\mathbb{R}$ is countable, which contradicts to Contor's Theorem, saying that $\mathbb{R}$ is not countable. Therefore, there must exist some transcendental numbers. □

6 Question 6

A famous theorem by Lindemann states that if $a \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ then e^a is transcendental. Use this theorem to prove that π is transcendental.

Theorem 10 (Lindermann)**.** *If $a \in \mathbb{C}\{0\}$ is algebraic over $\mathbb{Q}$, then a^a is transcendental.*

Proposition 11. *π is transcendental over $\mathbb{Q}$.*

Proof. First, we show that $i\pi$ is transcendental by contradiction.

If $i\pi$ is algebraic, then by Lindemann, $e^{i\pi}$ is transcendental over $\mathbb{Q}$, which contradicts to the fact that $e^{i\pi} = -1 \in \mathbb{Q}$, which means that $e^{i\pi}$ is algebraic over $\mathbb{Q}$. Therefore, $i\pi$ is transcendental over $\mathbb{Q}$.

Then we prove that π is transcendental over $\mathbb{Q}$ by contradiction.

If π is algebraic over $\mathbb{Q}$, then it is algebraic over $\mathbb{Q}(i)$, i.e. $[\mathbb{Q}(i,\pi) : \mathbb{Q}] < \infty$. Since $i\pi \in \mathbb{Q}(i,\pi)$, we have

$$[\mathbb{Q}(i\pi) : \mathbb{Q}] \leq [\mathbb{Q}(i,\pi,i\pi) : \mathbb{Q}] = [\mathbb{Q}(i,\pi) : \mathbb{Q}] \cdot [\mathbb{Q}(i,\pi,i\ pi) : \mathbb{Q}(i,\pi)] < \infty,$$

thus $i\pi$ is algebraic over $\mathbb{Q}$, which contradicts to the statement proven before. Therefore, π is transcendental over $\mathbb{Q}$. □

7 Question 7

Let R be a principle ideal domain, let $a_1, \ldots, a_n \in R$ be the elements such that $(\gcd(a_i, a_j)) = (1)$ for $i \neq j$, and let $a = a_1 \cdots a_n$. Prove that the map

$$\begin{aligned} \psi : R/(a) &\longrightarrow R/(a_1) \times R/(a_2) \times R/(a_n) \\ [r]_{(a)} &\longmapsto ([r]_{(a_1)}, [r]_{(a_2)}, \ldots, [r]_{(a_m)}) \end{aligned}$$

is an isomorphism of rings. Here we have used the notation $[r]_{(a)} = r + (a)$ for the coset of $r \bmod (a)$, and similarly for (a_i).

Let $V = R/(a_1) \times R/(a_2) \times \cdots \times R/(a_n)$. We write $([r_1]_{(a_1)}, \ldots, [r_n]_{(a_n)}) \in V$ as $([r_i]_{(a_i)})$ for convenience. Define an addition on V as $([r_i]_{(a_i)}) + ([s_i]_{a_i}) := ([r_i + s_i]_{(a_i)})$., where $r_i, s_i \in R$. Since the addition of cosets $[r_i]_{(a_i)}$ are well-defined, this addition is also well-defined.

First, we check that $(V, +)$ forms an abelian group.

For any $r_i, s_i \in R$, where i is between 1 and n, since the addition of R is commutative, we have

$$\begin{aligned}([r_i]_{(a_i)}) + ([s_i]_{(a_i)}) &= ([r_i + s_i]_{(a_i)}) \\ &= ([s_i + r_i]_{a_i}) \\ &= ([r_i]_{(a_i)}) + ([s_i]_{(a_i)}).\end{aligned}$$

Thus this addition on V is commutative.

For any $r_i, s_i, t_i \in R$, where i is between 1 and n, by associativity of addition of cosets, we have

$$\begin{aligned}(([r_i]_{(a_i)}) + ([s_i]_{(a_i)})) + ([t_i]_{(a_i)}) &= ([r_i + s_i]_{(a_i)}) + ([t_i]_{(a_i)}) \\ &= ([(r_i + s_i) + t_i]_{(a_i)}) \\ &= ([r_i + (s_i + t_i)_{(a_i)}]) \\ &= ([r_i]_{(a_i)}) + ([s_i + t_i]_{(a_i)}) \\ &= ([r_i]_{(a_i)}) + ([s_i]_{(a_i)}) + ([t_i]_{(a_i)}).\end{aligned}$$

Therefore, this addition on V is associative.

Let 0 be the additive identity of R. The additive identity in V is $([0]_{(a_i)})$, because for any $r_i \in R$, we have

$$([r_i]_{(a_i)}) + ([0]_{(a_i)}) = ([r_i + 0]_{(a_i)}) = ([r_i]_{(a_i)})$$

.

For any $r_i \in R$, the additive inverse of $([r_i]_{(a_i)})$ is $([-r_i]_{(a_i)})$, since

$$([r_i]_{(a_i)}) + ([-r_i]_{(a_i)}) = ([r_i + (-r_i)]_{(a_i)}) = ([0]_{(a_i)})$$

.

So far, we have shown that $(V, +)$ is an abelian group.

Then, we define an multiplication on V as $([r_i]_{(a_i)}) \cdot ([s_i]_{(a_i)}) := ([r_i s_i]_{(a_i)})$, where $r_i s_i$ uses the multiplication in R. This multiplication is also well-defined, because the multiplication of cosets is well-defined. We will show that $(V, \cdot)$ forms a monoid.

For any r_i, s_i, t_i in R, by associativity of multiplication on R, we have

$$\begin{aligned}(([r_i]_{(a_i)}) \cdot ([s_i]_{(a_i)})) \cdot ([t_i]_{(a_i)}) &= ([r_i s_i]_{(a_i)}) \cdot ([t_i]_{(a_i)}) \\ &= ([(r_i s_i) t_i]_{(a_i)}) \\ &= ([r_i (s_i t_i)]_{(a_i)}) \\ &= ([r_i]_{(a_i)}) \cdot ([s_i t_i]_{(a_i)}) \\ &= ([r_i]_{(a_i)}) \cdot (([s_i]_{(a_i)}) \cdot ([t_i]_{(a_i)})).\end{aligned}$$

Hence, this multiplication on V is associative.

Let 1 be the multiplicative identity of R, then the multiplicative identity of V is $([1]_{(a_i)})$, because for any $r_i \in R$, we have $([1]_{(a_i)}) \cdot ([r_i]_{(a_i)}) = ([1 \cdot r_i]_{(a_i)}) = ([r_i]_{(a_i)})$.

Therefore, $(V, \cdot)$ forms a monoid.

For any $r_i, s_i, t_i \in R$, from the distributivity of R, we have

$$\begin{aligned}([r_i]_{(a_i)}) \cdot (([s_i]_{(a_i)}) + ([t_i]_{(a_i)})) &= ([r_i]_{(a_i)}) \cdot ([s_i + t_i]_{(a_i)}) \\ &= ([r_i(s_i + t_i)]_{(a_i)}) \\ &= ([r_i s_i + r_i t_i]_{(a_i)}) \\ &= ([r_i]_{(a_i)}) \cdot ([s_i]_{(a_i)}) + ([r_i]_{(a_i)}) \cdot ([t_i]_{(a_i)}).\end{aligned}$$

Hence, multiplication have left distributivity with respect to addition. Simliarly, the right distributivity also holds.

Combining abelian group $(V, +)$, monoid $(V, \cdot)$ and distributivity, we can conclude that $(V, +, \cdot)$ forms a ring.

For any $r, s \in R$, from the definition of addition and multiplication of cosets, and the definition of ψ, we have $\psi([r]_{(a)} + [s]_{(a)}) = \psi([r+s]_{(a)}) = ([r+s]_{(a_i)}) = \psi(r) + \psi(s)$ and $\psi([r]_{(a)}[s]_{(a)}) = \psi([rs]_{(a)}) = ([rs]_{(a_i)}) = \psi(r) \cdot \psi(s)$. Therefore, ψ is a ring homomorphism.

Now we show that ψ is injective. If $\psi([r]_{(a_i)}) = \psi([r']_{(a_i)})$ where $r, r' \in R$, then $([r]_{(a_i)}) = ([r'])_{(a_i)}$, thus $[r]_{(a_i)} = [r']_{(a_i)}$ for all i, hence $[r - r']_{(a_i)} = [0]_{(a_i)}$ for all i, so $r - r' \in (a_i)$.

Then we show that if $r - r' \in (a_i)$ for all i, then $r - r' \in (a)$. In fact, it is enough to prove that for any i and j, if $r - r' \in (a_i)$ and $r - r' \in (a_j)$ and $(gcd(a_i, a_j)) = (1)$, then $r - r' \in (a_i a_j)$. From lectures, we know that Bezout's Identity holds in PID. Since $(gcd(a_i, a_j)) = (1)$, there exists two element $m_i, m_j \in R$ such that $m_i a_i + m_j a_j = 1$, so $r - r' = (r - r')m_i a_i + (r - r')m_j a_j$. From $r - r' \in (a_i)$ and $r - r' \in (a_j)$, we know that there exists two elements $q_i, q_j \in R$ such that $r - r' = q_i a_i$ and $r - r' = q_j a_j$, then $r - r' = q_j a_j m_i a_i + q_i a_i m_j a_j = (q_j m_i + q_i m_j) a_i a_j$, so $r - r' \in (a_i a_j)$. Therefore, $r - r' \in (a)$, which means that $[r - r']_{(a)} = [0]_{(a)}$, so ψ is injective.

Then we show that ψ is surjective. Let $\tilde{a}_i = a/a_i$. Consider an arbitrary element $([r_i]_{(a_i)}) \in V$.

We claim that $(\gcd(a_i, \tilde{a}_i)) = (1)$. In fact, it is enough to show that if $(\gcd(a_i, a_j)) = (1)$ and $(\gcd(a_i, a_k)) = (1)$, then $(\gcd(a_i, a_j a_k)) = (1)$. By Bezout's Identity, there exist elements $x_i, x_j, y_i, y_k \in R$ such that $x_i a_i + x_j y_j = 1$ and $y_i a_i + y_k a_k = 1$. Multiplying these two equations gives $(x_i y_i a_i + x_i y_k a_k + x_j a_j y_i) a_i + x_j y_j a_j a_k = 1$, so $(\gcd(a_i, a_j a_k)) = 1$. Therefore, $(\gcd(a_i, \tilde{a}_i)) = (1)$.

Since $(\gcd(a_i, \tilde{a}_i)) = (1)$, by Bezout's Identity, there exists two elements $x_i, y_i \in R$ such that $x_i a_i + y_i \tilde{a}_i = 1$, so $r_i x_i a_i + r_i y_i \tilde{a}_i = r_i$, i.e. $r_i y_i \tilde{a}_i \in [r_i]_{(a_i)}$. From the definition of $\tilde{a}_i$, we also know that $\tilde{a}_i \in (a_j)$ for all $j \neq i$, hence $[r_i y_i \tilde{a}_i]_{(a_j)} = [0]_{(a_j)}$. Let $r = \sum_{i=1}^{n} r_i y_i \tilde{a}_i$, then we have $[r]_{(a_i)} = [r_i]_{(a_i)}$, therefore $([r]_{(a_i)}) = ([r_i]_{(a_i)})$. So far, we have shown that for any $([r_i])_{(a_i)}$, there exists an $r \in R$ such that $([r]_{(a_i)}) = ([r_i]_{(a_i)})$, thus $\psi([r]_{(a)}) = ([r_i]_{(a_i)})$, so ψ is surjective.

Therefore, ψ is bijective, so it is a ring isomorphism.