Math 4108 HW4

Pengfei Zhu

February 1, 2024

Exercise 3.7 Show that $f(X) = X^3 + X + 1$ is irreducible over $\mathbb{Q}$. Let α be a root of f in $\mathbb{C}$. Express $\frac{1}{\alpha}$ and $\frac{1}{\alpha+2}$ as linear combinations of $\{1, \alpha, \alpha^2\}$.

To show the irreducibility of $f(x)$, we can show that $f(X-1)$ is irreducible over $\mathbb{Q}$ applying Eisenstein's criterion. The polynomial $f(X-1) = X^3 - 3X^2 + 6X - 3$ satisfies the conditions of Eisenstein's criterion with $p = 3$. So $f(X) = X^3 + X + 1$ is irreducible over $\mathbb{Q}$.

Now, using the fact that α be a root of f in $\mathbb{C}$ which means $f(\alpha) = 0$, then we plug $f(\alpha)$ back into $f(x)$, we get $1 = -\alpha^3 - \alpha$, dividing both side by α

$$\frac{1}{\alpha} = \frac{-\alpha^3 - \alpha}{\alpha} = -\alpha^2 - 1.$$

For $\frac{1}{\alpha+2}$, we can try to factor $f(\alpha)$ into the form:$(\alpha+2)(\alpha^2+x\alpha+y)$. And so, we get $x = -2$, $y = 5$. Thus, $(\alpha+2)(\alpha^2-2\alpha+5) = \alpha^3+\alpha+10 = (\alpha^3+\alpha+1)+9 = 9$. Therefore,

$$\frac{1}{\alpha+2} = \frac{1}{9}(\alpha^2 - 2\alpha + 5)$$

Exercise 3.9 Show that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.
It is clear that $\mathbb{Q}(\sqrt{2} + \sqrt{5}) \subseteq Q(\sqrt{2}, \sqrt{5})$.

Now consider that

$$(\sqrt{2} + \sqrt{5})^5 = 229\sqrt{2} + 145\sqrt{5}$$

because $\sqrt{2} + \sqrt{5} \in \mathbb{Q}(\sqrt{2} + \sqrt{5})$, and also $229\sqrt{2} + 145\sqrt{5} \in \mathbb{Q}[\sqrt{2} + \sqrt{5}]$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{5})$. Since we showed both inclusions, we have $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.
Determine the minimum polynomial of:

(i) $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$.

Since $(\sqrt{2}+\sqrt{5})^4 = (7+2\sqrt{10})^2 = 89+28\sqrt{10}$, we see that $(\sqrt{2}+\sqrt{5})^4 - 14(\sqrt{2}+\sqrt{5})^2+9 = 0$, and the minimum polynomial over $\mathbb{Q}$ is $X^4-14X+9$.

(ii) $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}[\sqrt{2}]$.

Since $(\sqrt{2} + \sqrt{5})^2 = 7 + 2\sqrt{10} = 2\sqrt{2}(\sqrt{2} + \sqrt{5}) + 3$, the minimum polynomial over $\mathbb{Q}[\sqrt{2}]$ is $X^2 - 2\sqrt{2}X - 3$.

(iii) $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}[\sqrt{5}]$.

Since $(\sqrt{2}+\sqrt{5})^2 = 7+2\sqrt{10} = 2\sqrt{5}(\sqrt{2}+\sqrt{5})-3$, the minimum polynomial over $\mathbb{Q}[\sqrt{5}]$ is $X^2 - 2\sqrt{5}X + 3$.

Exercise 3.15 Let α, β be transcendental numbers. Decide whether the following conclusions are true or false:

(i) $Q(\alpha) \simeq Q(\beta)$;

True. Think of any algebraic dependencies that α has over a ground field $\mathbb{Q}$ as obstructions to $\mathbb{Q}(\alpha) \cong \mathbb{Q}(X)$, where X is an indeterminate, and both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are isomorphic to the field $\mathbb{Q}(X)$ of rational functions over $\mathbb{Q}$.

(ii) $\alpha\beta$ is transcendental;

False. Let α be any transcendental number. Then $\beta := \frac{1}{\alpha}$ is transcendental, and $\alpha \cdot \beta = 1$. Thus, $\alpha\beta$ is not necessarily transcendental.

(iii) α^β is transcendental;

False. e and $\ln(2)$ are transcendental (listed in class), but $e^{\ln(2)} = 2$ is not.

(iv) α^2 is transcendental.

True. If α^2 were algebraic, there would exist $a_0, a_1, \ldots, a_n$ such that $a_0 + a_1\alpha^2 + \ldots + a_n\alpha^{2n} = 0$, and this would imply that α is algebraic.

4. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(a) Prove that $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$.

Proof. Suppose, for a contradiction, that there exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{5}$, where b must be non-zero, since $\sqrt{3}$ is irrational. Then $a^2 = (\sqrt{3} - b\sqrt{5})^2 = (3 + 5b^2) - 2b\sqrt{15}$, and so $\sqrt{15} = \frac{5b^2-a^2+3}{2b} \in \mathbb{Q}$. This is a contradiction. $\square$

(b) Find a basis of K over $\mathbb{Q}$.

We can write $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ as $\mathbb{Q}(\sqrt{3})[\sqrt{5}]$. The set $\{1, \sqrt{3}\}$ is clearly a basis for $\mathbb{Q}[\sqrt{3}]$ over $\mathbb{Q}$. Since $\sqrt{3} \notin \mathbb{Q}[\sqrt{5}]$, we must have $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}[\sqrt{3}]) \geq 2$. On the other hand, from the trivial observation that $(\sqrt{5})^2 - 5 = 0$, we conclude that $X^2 - 5$ is the minimum polynomial of $\sqrt{5}$ over $\mathbb{Q}[\sqrt{3}]$, and that $\{1, \sqrt{5}\}$ is a basis. Then, from Theorem 3.3, we deduce that $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

(c) Show that the only subfields of K are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{15})$, and K itself.

First of all, $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, so it is assert that it is a subfield of K. We found already that these are basis, and their union will also be a subfield in K. Q and K are trivial subfield. The formal way might involve the Fundamental Theorem.

Having a question, isn't $\{1, \sqrt{3}+\sqrt{5}, (\sqrt{3}+\sqrt{5})^2, (\sqrt{3}+\sqrt{5})^3\}$basis and subfields of K?

(d) Find the minimum polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$.

The minimum polynomials of degree 4. From the information that $(\sqrt{3}+\sqrt{5})^2 = 8+2\sqrt{15}$ and $(\sqrt{3}+\sqrt{5})^4 = 124+32\sqrt{15} = 16(8+2\sqrt{15})-4$, we can manipulate two terms, and find that the minimum polynomial is X^4-16X^2+4.

5. Show that $[\mathbb{Q}(\sqrt{5}+\sqrt[3]{2}):\mathbb{Q}] = 6$.
Let $\alpha = \sqrt{5}+\sqrt[3]{2}$. Then $(\alpha-\sqrt{5})^3 = 2$. Following by direct computation:

$$x^3 - 3\sqrt{5}x^2 + 15x - 5\sqrt{5} = 2$$
$$x^3 + 15x - 2 = \sqrt{5}(3x^2+5)$$
$$(\alpha^3 + 6\alpha - 2)^2 = 5(3\alpha^2+2)^2$$
$$x^6 + 30x^4 - 4x^3 + 225x^2 - 60x + 4 = 45x^4 + 150x^2 + 125$$
$$= x^6 - 15x^4 - 4x^3 + 75x^2 - 60x - 121 = 0$$

Therefore, α is a root of a polynomial of degree 6, and so $[\mathbb{Q}(\sqrt{5}+\sqrt[3]{2}):\mathbb{Q}] \le 6$. On the other hand, $[Q(\sqrt{5}+\sqrt[3]{2}):Q]$ is a multiple of 6 because $[Q(\sqrt{5}):Q] = 2$ and $[Q(\sqrt[3]{2}):Q] = 3$. Therefore, $[\mathbb{Q}(\sqrt{5}+\sqrt[3]{2}):\mathbb{Q}] = 6$.

6. Let L be a field, K be a subfield of L, and $a, b \in L$ be algebraic over K of degrees m and n respectively. Prove that if m and n are relatively prime, then $[K(a,b):K] = mn$.

Proof. First, $K(a)$ is the smallest field containing K and a by definition, and also that $K[a] = K(a)$.(shown in class) Therefore, $K(a,b) = K[a](b) = K[a][b]$ is the smallest field containing K and also both a and b. Thus, $K[b][a] = K(b,a) = K(a,b) = K[a][b]$. Now, we have the following relation:

$$K \subseteq K[a] \subseteq K[a][b] = K(a,b)$$

, and so we can write

$$[K(a,b):K] = [K[a]:K] \cdot [K[a][b]:K[a]],$$

but therefore $m = [K[a]:K]$ divides $[K(a,b):K]$. By symmetry, n also divides $[K(a,b):K]$, and so $[K(a,b):K] \ge mn$ since m and n are relatively prime.

On the other hand, let $g(b) = 0$ for some $g(x) \in K[x]$ of degree n. Note $K[x] \subseteq K[a][x]$, and so $g(x) \in K[a][x]$ as well. Thus, $g(b) = 0$. Let $h(x) \in K[a][x]$ be the minimal polynomial for b, so that $h \mid g$. It follows that $\deg h \le n$, and so $[K[a][b]:K[a]] = \deg h \le n$. Thus,

$$mn \le [K(a,b):K] = [K[a]:K] \cdot [K[a][b]:K[a]] = m \cdot [K[a][b]:K[a]] \le mn,$$

As a result, $[K(a,b):K] = mn$. □

7. Let K be a field. Prove that the following conditions are equivalent.

(a) Every polynomial in $K[x]$ of degree ≥ 1 has a root in K.

(a) $\Rightarrow$ (b)

Assume (a) holds. Let $f(x)$ be any polynomial of degree ≥ 1 in $K[x]$. By (a), there exists a root c in K such that $f(c) = 0$. Therefore, we can write $f(x) = (x-c)g(x)$, where $g(x)$ is another polynomial in $K[x]$. Since $\deg(g) = \deg(f) - 1$, we can repeat this process for $g(x)$ until all factors are linear. This implies that every polynomial of degree ≥ 1 in $K[x]$ can be factored into linear polynomials.

(b) Every polynomial in $K[x]$ of degree ≥ 1 splits over K, that is, it factors as a product of linear polynomials.

(b) $\Rightarrow$ (c)

Assume (b) holds. Let $f(x)$ be an irreducible polynomial in $K[x]$. Since $f(x)$ is irreducible, it cannot be factored into non-trivial polynomials. By (b), every polynomial splits over K, including irreducible ones. Therefore, $f(x)$ can only be a product of linear polynomials. Since $f(x)$ is irreducible, there must be only one linear factor, and thus, $f(x)$ has degree 1.

(c) Every irreducible polynomial in $K[x]$ has degree 1.

(c) $\Rightarrow$ (d)

Assume (c) holds. Let L be an algebraic extension of K, and let $a \in L$. Since a is algebraic over K, there exists a polynomial $f(x) \in K[x]$ such that $f(a) = 0$. By (c), $f(x)$ must be irreducible and of degree 1, implying that a is in fact in K. Since a was chosen arbitrarily from L, L must be contained in K, and therefore $L = K$.

(d) There is no algebraic extension of K except K itself.

(d) $\Rightarrow$ (a)

Assume (d) holds. Let $f(x)$ be any polynomial of degree ≥ 1 in $K[x]$. If $f(x)$ has no roots in K, then by (d), there must be an algebraic extension L of K containing a root of $f(x)$. But this contradicts (d), as L cannot be a proper extension of K. Therefore, every polynomial of degree ≥ 1 in $K[x]$ has a root in K.

These four implications establish the equivalence of the given conditions.

A field K is called algebraically closed if any of the conditions above are satisfied.

8. Prove that an algebraically closed field must contain infinitely many elements.

Proof. Let F be a finite field and consider the polynomial

$$f(x) = 1 + \prod_{a \in F} (x - a).$$

The coefficients of $f(x)$ lie in the field F, and thus $f(x) \in F[x]$. $f(x)$ is a non-constant polynomial.

But for each $a \in F$, we have $f(a) = 1 \neq 0$. So the polynomial $f(x)$ has no root in F. Hence, the finite field F is not algebraically closed. It follows that every algebraically closed field must be infinite. $\square$