MRQ 2017

School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet II: Field extensionions: Algebraic elements, minimum polynomials, simple extensions (Solutions)

1. **Let K be an extension of the field F such that the degree $|K : F|$ is a prime number. Show that there are no *intermediate* fields between F and K; that is, no fields L satisfying $F \subset L \subset K$.**

Solution: Suppose L is an intermediate field: $F \subseteq L \subseteq K$. Then by the Tower Law

$$|K : F| = |K : L| \cdot |L : F|.$$

Since $|K : F|$ is prime, either $|K : L| = 1$ or $|L : F| = 1$. Thus $L = K$ or $L = F$.

Hence there are no *strictly* intermediate fields L satisfying $F \subset L \subset K$.

2. **For all values of $a, b \in \mathbb{Q}$, determine the minimum polynomial of $a + b\sqrt{2}$ over $\mathbb{Q}$.**

Solution: If $b = 0$, then $a \in \mathbb{Q}$ satisfies the linear polynomial $X - a$ over $\mathbb{Q}$ and this is the minimum polynomial of a over $\mathbb{Q}$.

If $b \neq 0$, then $\alpha = a + b\sqrt{2} \notin \mathbb{Q}$. (For if $\alpha \in \mathbb{Q}$, then $\sqrt{2} = (\alpha - a)/b \in \mathbb{Q}$, which would be a contradiction.) Hence the minimum polynomial of α over $\mathbb{Q}$ cannot be linear. Now

$$\alpha^2 = (a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2.$$

Hence

$$\begin{aligned} \alpha^2 - 2a\alpha &= a^2 + 2b^2 + 2ab\sqrt{2} - 2a^2 - 2ab\sqrt{2} \\ &= 2b^2 - a^2 \end{aligned}$$

and we conclude α is a root of

$$X^2 - 2aX + a^2 - 2b^2.$$

Since α does not satisfy any linear polynomial, we conclude this polynomial is the minimum polynomial of α over $\mathbb{Q}$.

In conclusion, the minimum polynomial of $a + b\sqrt{2}$ over $\mathbb{Q}$ is

$$\begin{aligned} &X - \alpha && \text{if } b = 0, \\ &X^2 - 2aX + (a^2 - 2b^2) && \text{if } b \neq 0. \end{aligned}$$

3. **(a) Show that $\mathbb{C}$ is a simple extension of $\mathbb{R}$.**
   (b) What are the irreducible polynomials over $\mathbb{C}$?
   (c) Show that if α is algebraic over $\mathbb{C}$, then $\mathbb{C}(\alpha) = \mathbb{C}$.

Solution: (a) Every element of $\mathbb{C}$ can be expressed as $a + bi$ where $a, b \in \mathbb{R}$. Hence the smallest subfield of $\mathbb{C}$ containing $\mathbb{R}$ and the element i is $\mathbb{C}$ itself; that is, $\mathbb{C} = \mathbb{R}(i)$. Hence $\mathbb{C}$ is a simple extension of $\mathbb{R}$.

(b) The Fundamental Theorem of Algebra (proved in Complex Analysis books/courses) states that every polynomial $f(X)$ with complex coefficients (that is, $f(X) \in \mathbb{C}[X]$) has a root α in $\mathbb{C}$ and hence factorizes as

$$f(X) = (X - \alpha)\, g(X)$$

for some $g(X) \in \mathbb{C}[X]$. Consequently, the only irreducible polynomials over $\mathbb{C}$ are the linear polynomials (i.e., those of degree one).

(c) If α is algebraic over $\mathbb{C}$, then the minimum polynomial $f(X) \in \mathbb{C}[X]$ is irreducible so, by (b), is of degree one; that is, $f(X) = X - \alpha$ and $\alpha \in \mathbb{C}$. Hence $\mathbb{C}(\alpha) = \mathbb{C}$.

4. **Let α be algebraic over the base field F. Show that every element of the simple extension $F(\alpha)$ is algebraic over F.**

Solution: Let α be algebraic over F. Suppose $f(X)$ is the minimum polynomial of α over F. Then

$$|F(\alpha) : F| = \deg f(X).$$

This is a positive integer, so we conclude that $F(\alpha)$ is a finite extension of F. As a finite extension, it follows that $F(\alpha)$ is an algebraic extension of F; that is, every element of $F(\alpha)$ is algebraic over F.

5. **Show that the polynomial $f(X) = X^4 - 16X^2 + 4$ is irreducible over $\mathbb{Q}$.**

Let α be a root of $f(X)$ in some field extension of $\mathbb{Q}$. Determine the minimum polynomials of α^2 and of $\alpha^3 - 14\alpha$ over $\mathbb{Q}$.

Solution: Consider $f(X) = X^4 - 16X^2 + 4$ over $\mathbb{Q}$. If $f(X)$ factorizes over $\mathbb{Q}$, then it factorizes over $\mathbb{Z}$, by Gauss's Lemma. If we reduce the coefficients modulo 3 (that is, apply the ring homomorphism $\mathbb{Z}[X] \to \mathbb{F}_3[X]$ induced by the natural map $\mathbb{Z} \to \mathbb{F}_3$) then we obtain a factorization of

$$\bar{f}(X) = X^4 - X^2 + 1$$

over $\mathbb{F}_3$. Note

$$\bar{f}(0) = 1, \quad \bar{f}(1) = 1, \quad \bar{f}(2) = 1,$$

so $\bar{f}(X)$ has no linear factors. Therefore $f(X)$ has no linear factors over $\mathbb{Z}$, nor over $\mathbb{Q}$. We conclude that if $f(X)$ factorizes over $\mathbb{Q}$, then it has a factorization

$$f(X) = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Hence

$$\alpha + \gamma = 0, \qquad \alpha\gamma + \beta + \delta = -16,$$

$$\alpha\delta + \beta\gamma = 0, \qquad \beta\delta = 4.$$

The first equation yields $\gamma = -\alpha$ and then the third equation becomes

$$(\delta - \beta)\alpha = 0.$$

If it were the case that $\beta \neq \delta$, then this would force $\alpha = \gamma = 0$. The second equation is then $\beta + \delta = -16$, which is impossible if $\beta\delta = 4$ (as then $\{\beta, \delta\} = \{1, 4\}$ or $\{-1, -4\}$). Hence $\beta = \delta$ and we conclude $\beta = \delta = \pm 2$. The second equation, in this case, becomes

$$-\alpha^2 + 2\beta = -16;$$

that is,

$$\alpha^2 = 2\beta + 16 = 12 \text{ or } 20.$$

This is impossible for $\alpha \in \mathbb{Z}$.

We conclude that $f(X) = X^4 - 16X^2 + 4$ is indeed irreducible over $\mathbb{Q}$.

Let α be a root of $f(X)$ in some extension over $\mathbb{Q}$. Then $\alpha^4 - 16\alpha^2 + 4 = 0$ and $f(X)$ Is the minimum polynomial of α over $\mathbb{Q}$. Let $\beta = \alpha^2$. Certainly β satisfies

$$\beta^2 - 16\beta + 4 = 0;$$

that is, β is a root of $X^2 - 16X + 4$. This must be the minimum polynomial of β over $\mathbb{Q}$, for if it were not, then β would satisfy a linear polynomial over $\mathbb{Q}$, say $X - c$, and then α would satisfy $\alpha^2 - c = 0$, contrary to $f(X)$ being the minimum polynomial of α over $\mathbb{Q}$.

Hence $X^2 - 16X + 4$ is the minimum polynomial of $\beta = \alpha^2$ over $\mathbb{Q}$.

Let $\gamma = \alpha^3 - 14\alpha$. Since α does not satisfy a non-zero polynomial of degree three over $\mathbb{Q}$, γ cannot satisfy a linear polynomial over $\mathbb{Q}$. Hence the minimum polynomial of γ over $\mathbb{Q}$ has degree at least two. Observe, using the fact that $\alpha^4 = 16\alpha^2 - 4$, that

$$\begin{aligned}
\gamma^2 &= (\alpha^3 - 14\alpha)^2 \\
&= \alpha^6 - 28\alpha^4 + 196\alpha^2 \\
&= \alpha^2(16\alpha^2 - 4) - 28(16\alpha^2 - 4) + 196\alpha^2 \\
&= 16\alpha^4 - 4\alpha^2 - 448\alpha^2 + 112 + 196\alpha^2 \\
&= 16(16\alpha^2 - 4) - 256\alpha^2 + 112 \\
&= 256\alpha^2 - 64 - 256\alpha^2 + 112 \\
&= 48.
\end{aligned}$$

Hence γ is a root of $X^2 - 48$ and this must then be the minimum polynomial of $\gamma = \alpha^3 - 14\alpha$ over $\mathbb{Q}$.

6. **Determine the following degrees of field extensions:**

   (a) $|\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}|$
   (b) $|\mathbb{Q}(\mathrm{e}^{2\pi i/5}) : \mathbb{Q}|$
   (c) $|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}|$
   (d) $|\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}|$
   (e) $|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}|$
   (f) $|\mathbb{Q}(\sqrt{6}, i) : \mathbb{Q}(i)|$

Solution: (a) First observe that $\sqrt[5]{3}$ is a root of $X^5 - 3$, which is an irreducible polynomial over $\mathbb{Q}$ by Eisenstein's Criterion. Hence $X^5 - 3$ is the minimum polynomial of $\sqrt[5]{3}$ over $\mathbb{Q}$ and therefore

$$|\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}| = 5.$$

(b) Let $\omega = \mathrm{e}^{2\pi i/5}$. Note $\omega^5 = 1$, but $X^5 - 1$ is not irreducible over $\mathbb{Q}$ as it factorizes as

$$X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1).$$

Substituting ω into this factorization we conclude

$$0 = (\omega - 1)(\omega^4 + \omega^3 + \omega^2 + \omega + 1),$$

so

$$\omega^4 + \omega^3 + \omega^2 + \omega + 1 = 0$$

since $\omega \neq 1$. Thus ω satisfies the polynomial $X^4 + X^3 + X^2 + X + 1$, which is an irreducible polynomial over $\mathbb{Q}$ as observed in Example 1.24(iii) (taking $p = 5$ in that example). Hence the minimum polynomial of $\omega = \mathrm{e}^{2\pi i/5}$ over $\mathbb{Q}$ is $X^4 + X^3 + X^2 + X + 1$ and

$$|\mathbb{Q}(\mathrm{e}^{2\pi i/5}) : \mathbb{Q}| = 4.$$

(c) We use the Tower Law to observe

$$|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|.$$

Now $\sqrt{2}$ is a root of $X^2 - 2$ and this is an irreducible polynomial over $\mathbb{Q}$ by Eisenstein's Criterion. Thus $X^2 - 2$ is the minimum polynomial of $\sqrt{2}$ over $\mathbb{Q}$ and

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2.$$

Now i is a root of $X^2 + 1$. If this polynomial were reducible over $\mathbb{Q}(\sqrt{2})$, it would factorize as

$$X^2 + 1 = (X - i)(X + i)$$

over $\mathbb{Q}(\sqrt{2})$ and so $i \in \mathbb{Q}(\sqrt{2})$, which is not true as $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Hence $X^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and is therefore the minimum polynomial of i over $\mathbb{Q}(\sqrt{2})$. Thus

$$|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})| = 2$$

and we conclude

$$|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 2 \times 2 = 4.$$

(d) Now $\sqrt{2}i$ is a root of $X^2 + 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. We conclude $X^2 + 2$ is the minimum polynomial of $\sqrt{2}i$ over $\mathbb{Q}$ and

$$|\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}| = 2.$$

(e) We use the Tower Law to observe

$$|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})| \cdot |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|.$$

We already know (see part (c)) that

$$|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$$

and indeed this tells us that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. Now $\sqrt{5}$ satisfies the polynomial $X^2 - 5$. If this were reducible over $\mathbb{Q}(\sqrt{2})$, it would factorize into linear factors and then necessarily $\sqrt{5} \in \mathbb{Q}(\sqrt{2})$; that is,

$$\sqrt{5} = a + b\sqrt{2}$$

for some $a, b \in \mathbb{Q}$. If $b = 0$, then $\sqrt{5} \in \mathbb{Q}$, which we know is false. If $a = 0$, then $\sqrt{5} = b\sqrt{2}$, so $\sqrt{10} = 2b \in \mathbb{Q}$, which again is false. Thus $a, b \neq 0$ and, upon squaring,

$$5 = a^2 + 2ab\sqrt{2} + 2b^2;$$

that is,

$$\sqrt{2} = \frac{5 - a^2 - 2b^2}{2ab} \in \mathbb{Q},$$

again a contradiction. Hence $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$ and $X^2 - 5$ is irreducible over $\mathbb{Q}(\sqrt{2})$. It is therefore the minimum polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2})$ and we conclude

$$|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})| = 2$$

and hence

$$|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}| = 4.$$

(f) We know i has minimum polynomial $X^2 + 1$ over $\mathbb{Q}$, so $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ and $\{1, i\}$ is a basis for $\mathbb{Q}(i)$ over $\mathbb{Q}$.

Now $\sqrt{6}$ is a root of $X^2 - 6$. If this were to factorize into linear factors over $\mathbb{Q}(i)$, then $\sqrt{6} \in \mathbb{Q}(i)$ and we could write $\sqrt{6} = a + bi$ for some $a, b \in \mathbb{Q}$. However, $\sqrt{6}$ is real, so necessarily $b = 0$, but this is a contradiction as $\sqrt{6} \notin \mathbb{Q}$, contrary to the equation $\sqrt{6} = a$. Hence $X^2 - 6$ is irreducible over $\mathbb{Q}(i)$ and is the minimum polynomial of $\sqrt{6}$ over $\mathbb{Q}(i)$. Thus

$$|\mathbb{Q}(\sqrt{6}, i) : \mathbb{Q}(i)| = 2.$$

7. **Let $\alpha \in \mathbb{C}$ be a root of the polynomial $X^2 + 2X + 5$. Express the element**

$$\frac{\alpha^3 + \alpha - 2}{\alpha^2 - 3}$$

of $\mathbb{Q}(\alpha)$ as a linear combination of the basis $\{1, \alpha\}$.

Solution: We first deal with the numerator and denominator of the given fraction. Dividing the appropriate polynomial by $X^2 + 2X + 5$, we observe

$$\begin{aligned} X^3 + X - 2 &= X(X^2 + 2X + 5) - 2X^2 - 4X - 2 \\ &= (X - 2)(X^2 + 2X + 5) + 8, \end{aligned}$$

so upon substituting α,

$$\alpha^3 + \alpha - 2 = 8.$$

Similarly

$$X^2 - 3 = (X^2 + 2X + 5) - 2X - 8,$$

so upon substituting α,

$$\alpha^2 - 3 = -2\alpha - 8.$$

To divide by this element, we shall apply the method to determine the greatest common divisor of the polynomials

$$a_0(X) = X^2 + 2X + 5 \qquad \text{and} \qquad a_1(X) = -2X - 8.$$

Divide $a_0(X)$ by $a_1(X)$ to give quotient and remainder:

$$\begin{aligned} a_0(X) &= X^2 + 2X + 5 \\ &= -\tfrac{1}{2}X \cdot (-2X - 8) - 2X + 5 \\ &= (-\tfrac{1}{2}X + 1)(-2X - 8) + 13. \end{aligned}$$

We take $a_2 = 13$. As this is a unit in $\mathbb{Q}[X]$, we conclude that $a_0(X)$ and $a_1(X)$ are coprime in this Euclidean domain. Reversing the steps in the calculation:

$$\begin{aligned} 13 &= a_0(X) - (-\tfrac{1}{2}X + 1)\, a_1(X) \\ &= a_0(X) + (\tfrac{1}{2}X - 1)(-2X - 8). \end{aligned}$$

Substituting α gives

$$13 = (\tfrac{1}{2}\alpha - 1)(-2\alpha - 8).$$

Hence

$$\frac{1}{\alpha^2 - 3} = \frac{1}{-2\alpha - 8} = \tfrac{1}{13}\left(\tfrac{1}{2}\alpha - 1\right).$$

We finally conclude, using all above calculations, that

$$\begin{aligned} \frac{\alpha^3 + \alpha - 2}{\alpha^2 - 3} &= \frac{8}{-2\alpha - 8} \\ &= \tfrac{8}{13}\left(\tfrac{1}{2}\alpha - 1\right) \\ &= \tfrac{4}{13}(\alpha - 2). \end{aligned}$$

8. **Show that $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{5})$.**
Determine the minimum polynomial of $\sqrt{2} + \sqrt{5}$ over the following subfields:

(i) $\mathbb{Q}$; **(ii)** $\mathbb{Q}(\sqrt{2})$; **(iii)** $\mathbb{Q}(\sqrt{5})$.

Solution: We have already calculated the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$ in Question 6(e):

$$|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}| = 4.$$

Since $\sqrt{2} + \sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{5})$, certainly

$$\mathbb{Q}(\sqrt{2} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5}).$$

The Tower Law tells us that $|\mathbb{Q}(\sqrt{2} + \sqrt{5}) : \mathbb{Q}|$ divides $|\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}| = 4$, so it equals 1, 2 or 4. Moreover, we also know that $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q}$ (as built, via the proof of the Tower Law, from the basis $\{1, \sqrt{2}\}$ for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and the basis $\{1, \sqrt{5}\}$ for $\mathbb{Q}(\sqrt{5}$ over $\mathbb{Q})$. It follows that $\sqrt{2} + \sqrt{5} \notin \mathbb{Q}$ as otherwise we would have a linear dependence relation

$$\sqrt{2} + \sqrt{5} + c = 0$$

for some $c \in \mathbb{Q}$.

Hence $\sqrt{2} + \sqrt{5}$ does not satisfy a linear polynomial over $\mathbb{Q}$. Suppose it satisfies a quadratic polynomial

$$X^2 + aX + b$$

where $a, b \in \mathbb{Q}$; that is,

$$(\sqrt{2} + \sqrt{5})^2 + a(\sqrt{2} + \sqrt{5}) + b = 0$$

or

$$2\sqrt{10} + a\sqrt{2} + b\sqrt{5} + (7 + b) = 0.$$

This also is impossible since $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ is linearly independent over $\mathbb{Q}$. We conclude that $\sqrt{2} + \sqrt{5}$ does not satisfy a linear or quadratic polynomial over $\mathbb{Q}$. Hence

$$|\mathbb{Q}(\sqrt{2} + \sqrt{5}) : \mathbb{Q}| = 4$$

and, from the inclusion $\mathbb{Q}(\sqrt{2}+\sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{5})$, we conclude

$$\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2},\sqrt{5}).$$

(i) We have observed the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{5}$ over $\mathbb{Q}$ must have degree four. We start by calculating

$$\begin{aligned}\alpha^4 = (\sqrt{2}+\sqrt{5})^4 &= (7+2\sqrt{10})^2 \\ &= 28\sqrt{10}+89 \\ &= 14(7+2\sqrt{10})-9 \\ &= 14(\sqrt{2}+\sqrt{5})^2-9 \\ &= 14\alpha^2-9,\end{aligned}$$

so

$$\alpha^4 - 14\alpha^2 + 9 = 0.$$

Hence $\alpha = \sqrt{2}+\sqrt{5}$ is a root of X^4-14X^2+9. This must then be the minimum polynomial of $\sqrt{2}+\sqrt{5}$ over $\mathbb{Q}$.

(ii) By the Tower Law, $|\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}(\sqrt{2})| = 2$, so the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{5}$ over $\mathbb{Q}(\sqrt{2})$ has degree two. Observe

$$\begin{aligned}\alpha^2 = (\sqrt{2}+\sqrt{5})^2 &= 7+2\sqrt{10} \\ &= 7+2\sqrt{2}\cdot\sqrt{5} \\ &= 3+2\sqrt{2}\,(\sqrt{2}+\sqrt{5}) \\ &= 3+2\sqrt{2}\,\alpha,\end{aligned}$$

so

$$\alpha^2 - 2\sqrt{2}\,\alpha - 3 = 0.$$

Hence α is a root of the polynomial $X^2 - 2\sqrt{2}\,X - 3$, so this must be the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{5}$ over $\mathbb{Q}(\sqrt{2})$.

(iii) Similarly $|\mathbb{Q}(\sqrt{2}+\sqrt{5}) : \mathbb{Q}(\sqrt{5})| = 2$ and the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{5}$ over $\mathbb{Q}(\sqrt{5})$ has degree two. Observe

$$\begin{aligned}\alpha^2 = (\sqrt{2}+\sqrt{5})^2 &= 7+2\sqrt{10} \\ &= 7+2\sqrt{5}\cdot\sqrt{2} \\ &= -3+2\sqrt{5}\,(\sqrt{2}+\sqrt{5}) \\ &= -3+2\sqrt{5}\,\alpha,\end{aligned}$$

so

$$\alpha^2 - 2\sqrt{5}\,\alpha + 3 = 0.$$

Hence α is a root of the polynomial $X^2 - 2\sqrt{5}\,X + 3$, so this must be the minimum polynomial of $\alpha = \sqrt{2}+\sqrt{5}$ over $\mathbb{Q}(\sqrt{5})$.

9. **Let α and β be algebraic elements over the base field F. Suppose that the minimum polynomial of α over F has degree m, the minimum polynomial of β over F has degree n, and that m and n are coprime. Show that $|F(\alpha,\beta) : F| = mn$.**

Solution: By the Tower Law, applied twice,

$$\begin{aligned}|F(\alpha,\beta):F| &= |F(\alpha,\beta):F(\alpha)|\cdot|F(\alpha):F| \\ &= |F(\alpha,\beta):F(\beta)|\cdot|F(\beta):F|.\end{aligned}$$

Hence $|F(\alpha):F| = m$ and $|F(\beta):F| = n$ both divide $|F(\alpha,\beta):F|$. Since m and n are coprime, we conclude that mn divides $|F(\alpha,\beta):F|$.

However, β satisfies a polynomial of degree n over $F(\alpha)$ (namely it is a root of the minimum polynomial of β over F), so the minimum polynomial of β over $F(\alpha)$ has degree $\leqslant n$, so

$$|F(\alpha,\beta):F(\alpha)| \leqslant n$$

and hence

$$|F(\alpha,\beta):F| = |F(\alpha,\beta):F(\alpha)|\cdot|F(\alpha):F| \leqslant mn.$$

Combining this with the fact that mn divides $|F(\alpha,\beta):F|$, we conclude

$$|F(\alpha,\beta):F| = mn.$$

10. **Let α be transcendental over the field F. Show that there is an isomorphism ψ from the field $F(X)$ of rational functions in the indeterminate X over F to the simple extension $F(\alpha)$ satisfying $X\psi = \alpha$ and $b\psi = b$ for all $b \in F$.**

Solution: Suppose α is transcendental over F. First define the map $\phi\colon F[X] \to F(\alpha)$ by evaluating a polynomial at α:

$$\phi\colon g(X) \mapsto g(\alpha).$$

This map was considered during Chapter 2 of the lecture notes and we observed (see Lemma 2.11(ii)) that ϕ is a ring homomorphism. Since α is transcendental, $\ker\phi = \{0\}$ and hence ϕ is an injective map.

We now extend ϕ to a map

$$\psi\colon F(X) \to F(\alpha)$$

by defining

$$\left(\frac{g(X)}{h(X)}\right)\psi = \frac{g(\alpha)}{h(\alpha)}.$$

We need to check ψ is a well-defined ring homomorphism that is bijective.

First note that since $h(\alpha) \neq 0$ whenever $h(X)$ is a non-zero polynomial, it is certainly the case that $g(\alpha)/h(\alpha)$ is some element of $F(\alpha)$. Now suppose that $g_1(X)/h_1(X) = g_2(X)/h_2(X)$ in $F(X)$. This means

$$g_1(X)\,h_2(X) = g_2(X)\,h_1(X),$$

so upon applying ϕ (that is, evaluating at α),

$$g_1(\alpha)\,h_2(\alpha) = g_2(\alpha)\,h_1(\alpha).$$

Hence

$$\frac{g_1(\alpha)}{h_1(\alpha)} = \frac{g_2(\alpha)}{h_2(\alpha)}$$

(using the fact that $h_1(\alpha) \neq 0$ and $h_2(\alpha) \neq 0$), which shows

$$\left(\frac{g_1(X)}{h_1(X)}\right)\psi = \left(\frac{g_2(X)}{h_2(X)}\right)\psi,$$

so ψ is indeed well-defined.

Now if $g_1(X)/h_1(X), g_2(X)/h_2(X) \in F(X)$, then

$$\begin{aligned}\left(\frac{g_1(X)}{h_1(X)} + \frac{g_2(X)}{h_2(X)}\right)\psi &= \left(\frac{g_1(X)\,h_2(X) + g_2(X)\,h_1(X)}{h_1(X)\,h_2(X)}\right)\psi \\ &= \frac{g_1(\alpha)\,h_2(\alpha) + g_2(\alpha)\,h_1(\alpha)}{h_1(\alpha)\,h_2(\alpha)} \\ &= \frac{g_1(\alpha)\,h_2(\alpha)}{h_1(\alpha)\,h_2(\alpha)} + \frac{g_2(\alpha)\,h_1(\alpha)}{h_1(\alpha)\,h_2(\alpha)} \\ &= \frac{g_1(\alpha)}{h_1(\alpha)} + \frac{g_2(\alpha)}{h_2(\alpha)} \\ &= \left(\frac{g_1(X)}{h_1(X)}\right)\psi + \left(\frac{g_2(X)}{h_2(X)}\right)\psi\end{aligned}$$

and

$$\begin{aligned}\left(\frac{g_1(X)}{h_1(X)} \cdot \frac{g_2(X)}{h_2(X)}\right)\psi &= \left(\frac{g_1(X)\,g_2(X)}{h_1(X)\,h_2(X)}\right)\psi \\ &= \frac{g_1(\alpha)\,g_2(\alpha)}{h_1(\alpha)\,h_2(\alpha)} \\ &= \frac{g_1(\alpha)}{h_1(\alpha)} \cdot \frac{g_2(\alpha)}{h_2(\alpha)} \\ &= \left(\frac{g_1(X)}{h_1(X)}\right)\psi \cdot \left(\frac{g_2(X)}{h_2(X)}\right)\psi.\end{aligned}$$

Thus ψ is a ring homomorphism $F(X) \to F(\alpha)$.

Observe $g(X)/h(X)$ belongs to the kernel of ψ if and only if $g(\alpha)/h(\alpha) = 0$; that is, $g(\alpha) = 0$. Since α is transcendental, this occurs only when $g(X) = 0$, so

$$\ker\psi = \{0\}$$

and ψ is injective. Therefore $F(X) \cong \operatorname{im}\psi$ and $\operatorname{im}\psi$ is a subfield of $F(\alpha)$. However $F \subseteq \operatorname{im}\psi$ as the constant polynomial b maps to b under ψ for all $b \in F$. Similarly $X\psi = \alpha$, so $\alpha \in \operatorname{im}\psi$. Thus, $\operatorname{im}\psi$ is a subfield of $F(\alpha)$ containing both F and α, so $\operatorname{im}\psi = F(\alpha)$.

In conclusion, ψ is an isomorphism $F(X) \to F(\alpha)$ that satisfies $X\psi = \alpha$ and $b\psi = b$ for all $b \in F$.

11. **(a) Show that the field $\mathbb{A}$ of algebraic numbers over $\mathbb{Q}$ is countable.**
(b) Show that $\mathbb{C}$ is an infinite degree extension of $\mathbb{A}$.
(c) Show that $\mathbb{C}$ contains elements that are transcendental over $\mathbb{Q}$.

Solution: (a) Recall that $\mathbb{Q}$ is uncountable, so there exists a bijection $\mathbb{N} \to \mathbb{Q}$. We also know $\mathbb{N} \times \mathbb{N}$ is countable. It follows that $\mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}$ (k times) is a countable set, for any choice of positive integer k.

For a fixed degree d, any polynomial of degree d over $\mathbb{Q}$ has the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_dX^d$$

for some $a_0, a_1, \ldots, a_d \in \mathbb{Q}$. The collection of possible coefficients is in one-correspondence with $\mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}$ ($d+1$ times). Hence there are countably many polynomials $f(X) \in \mathbb{Q}[X]$ of degree d. Each such polynomial $f(X)$ has at most d roots in $\mathbb{C}$. Let us write $Z_{f(X)}$ for the set of roots of $f(X)$ in $\mathbb{C}$. Hence

$$\mathbb{A} = \bigcup_{d=1}^{\infty} \bigcup_{f(X) \in \mathcal{P}_d} Z_{f(X)}$$

where $\mathcal{P}_d$ is the (countable) set of polynomials of degree d in $\mathbb{Q}[X]$.

Thus $\mathbb{A}$ is a countable union of finite sets, so as a countable union of countable sets, $\mathbb{A}$ is countable.

(b) If $\mathbb{C}$ were a finite extension of $\mathbb{A}$, it would have some basis $\{v_1, v_2, \ldots, v_n\}$ over $\mathbb{A}$. Then every element of $\mathbb{C}$ would be uniquely expressible in the form

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

where $a_1, a_2, \ldots, a_n \in \mathbb{A}$. Hence there would be a bijection $\mathbb{A}^n \to \mathbb{C}$ and, since $\mathbb{A}$ is countable, we would conclude $\mathbb{C}$ is countable. As $\mathbb{C}$ is actually an uncountable set, we conclude that $\mathbb{C}$ is an infinite degree extension of $\mathbb{A}$.

(c) Since $|\mathbb{C} : \mathbb{A}| = \infty$, we know $\mathbb{A} \neq \mathbb{C}$, so $\mathbb{C}$ contains elements that are not algebraic over $\mathbb{Q}$; that is, $\mathbb{C}$ contains elements that are transcendental over $\mathbb{Q}$.