# Solutions Exercise sheet 3

**1.** (a) Let $f$ and $g$ be polynomials over a field $F$. Show that $f$ and $g$ are relatively prime if and only if $f$ and $g$ have no common root in any extention of $F$.

(b) If $f, g \in F[x]$ are distinct monic irreducible polynomials then show that they have no common roots in any extention of $F$.

*Solution*: (a) ($\Rightarrow$) Assume that $f$ and $g$ are relatively prime. We want to show that $f$ and $g$ have no common root in any extension of $F$.

If $f$ and $g$ are relatively prime, then there are polynomials $a(x)$ and $b(x)$ such that $a(x)f(x)+b(x)g(x) = 1$. If $\alpha$ is a common root of $f$ and $g$ we then have $1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 0$ which clearly is a contradiction.

($\Leftarrow$) Conversely, assume that $f$ and $g$ have no common root in any extension of $F$. We want to show that $f$ and $g$ are relatively prime.

Suppose $d$ is the greatest common divisor of $f$ and $g$. Then $d$ divides both $f$ and $g$. If $d \neq 1$, it must have at least one root $\alpha$ in some extension $K$ of $F$. Then $x - \alpha$ divides $d$ and hence it divides $f$ and $g$ in $K$. This means $\alpha$ is a root of both $f$ and $g$.

Thus, the only possibility is that $d = 1$, meaning $f$ and $g$ are relatively prime.

(b) Given that $f$ and $g$ are distinct monic irreducible polynomials in $F[x]$, we need to show that they are relatively prime. Let $h$ be a non constant divisor of the polynomials $f$ and $g$. Since $f$ and $g$ are irreducible, then up to constants $h$ coincides with $f$ and $g$. Hence $h(x) = cf(x)$ and $h(x) = dg(x)$ for some constants $c, d$ in $F$. But then $f(x) = c^{-1}dg(x)$. Since $f, g$ are monic $f = g$. But this contradicts the assumption that they are distinct polynomials. Hence $h$ is a constant which means $f$ and $g$ are relatively prime.

Using part (a), they have no common roots in any extension of $F$.

**2.** Let $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$, the set of all algebraic numbers over $\mathbb{Q}$.

(a) Show that $\overline{\mathbb{Q}}$ is a field.

(b) Show that $\overline{\mathbb{Q}} : \mathbb{Q}$ is an infinite extention

*Solution*: (a) To show that the set of all algebraic numbers over $\mathbb{Q}$ is a field, we need to prove that it satisfies the field axioms: closure under addition, closure under multiplication, existence of additive and multiplicative inverses, commutativity, associativity, and distributivity.

Closure under addition and multiplication: Let $a, b$ be any two algebraic numbers in $\overline{\mathbb{Q}}$. We need to show that $a + b$ and $ab$ are algebraic over $\mathbb{Q}$.

Note that if $F$ is a finite extension of $\mathbb{Q}$, and $a \in F$, then $a$ is algebraic over $\mathbb{Q}$.

Let $a, b$ be algebraic over $\mathbb{Q}$. By Exercise 4 we have that

$$[\mathbb{Q}(a, b) : \mathbb{Q}] \leqslant [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(b) : \mathbb{Q}] < \infty.$$

Hence $\mathbb{Q}(a,b)$ is a finite extension of $\mathbb{Q}$, so each element of $\mathbb{Q}(a,b)$ is algebraic over $\mathbb{Q}$. In particular, $a+b, ab \in \mathbb{Q}(a,b)$, so they are algebraic over $\mathbb{Q}$ as well.

Existence of additive and multiplicative inverses: For any non-zero algebraic number $a$ in $\overline{\mathbb{Q}}$, its additive inverse $-a$ and multiplicative inverse $a^{-1}$ exist. We need to show that $a^{-1}$ is an algebraic number.

Let $f$ be a monic polynomial over $\mathbb{Q}$ satisfying $f(a)=0$. Then we can write

$$\begin{aligned} 0 = f(a) = \sum_{k=0}^{n} b_k a^k &= a^n \sum \frac{b_k}{a^n} a^k \\ &= a^n \sum b_{n-k} (a^{-1})^{-k} \\ &= \sum b_{n-k} (a^{-1})^{n-k} \end{aligned}$$

Hence $a^{-1}$ is a zero of the polynomial $\sum_{k=0}^{n} b_{n-k} X^{n-k}$. We can make this polynomial monic by dividing by the leading term. Hence $a^{-1}$ is algebraic over $\mathbb{Q}$.

Commutativity, associativity, and distributivity: These properties are inherited from the field of rational numbers, $\mathbb{Q}$, since all elements of $\overline{\mathbb{Q}}$ are roots of polynomials with coefficients in $\mathbb{Q}$.

With all the above properties, $\overline{\mathbb{Q}}$ indeed forms a field.

(b) Let $p$ be any prime number. Consider the polynomial $f(X) := X^n - p$ over the rationals. By Eisenstein's criterion $f$ is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}[\sqrt[n]{p}] : \mathbb{Q}] = n$, but $\mathbb{Q}[\sqrt[n]{p}] \subseteq \overline{Q}$ for all $n \in \mathbb{Z}_{\geqslant 0}$. Hence $\dim_{\mathbb{Q}}(\overline{\mathbb{Q}}) = \infty$.

**3.** Let $\mathbb{A} = \mathbb{R} \bigcap \overline{\mathbb{Q}}$. Show that $\mathbb{A}$ is countable, and conclude that there are real numbers which are transcendental.

*Solution*:

*Claim.* The set of polynomials with rational coefficients is countable.

*Proof of claim.* Since $\mathbb{Q}$ is countable, for each $n \geqslant 1$ we have that $\mathbb{Q}^n$ is countable as well.

For $n \geqslant 1$ let $P_n$ be the set of all polynomials with rational coefficients and degree $n$. For a rational polynomial

$$f(X) = a_n X^n + \cdots + a_1 X + a_0,$$

we define a function $p_n : P_n \to \mathbb{Q}^{n+1}$, by

$$p_n(f) := (a_n, \ldots, a_1, a_0).$$

This functions is onto, and is clearly one-to-one. Hence it is a bijection. Thus for each $n$ the set $P_n$ is countable.

We can write the set of all raional polynomials as a countable union

$$\bigcup_n P_n,$$

and since a countable union of countable sets is countable, we obtain our claim.

Since each algebraic number is a root of a polynomial with rational coefficients (which are countable), the set of algebraic numbers is countable as well. The real numbers $\mathbb{R}$ are uncountable, but since $\overline{\mathbb{Q}}$ is countable, $\mathbb{R} \bigcap \overline{\mathbb{Q}}$ is countable as well. From the cardinality of the two sets, it follows that there exist real numbers which are not algebraic, i.e. they are transcendental.

**4.** Let $L : K$ be an algebraic field extension. Let $K_1, K_2$ be two fields with $K \subseteq K_1, K_2 \subseteq L$, such that the field extensions $K_1 : K$ and $K_2 : K$ are finite. The composite of $K_1$ and $K_2$ is defined as $K_1K_2 := K(K_1 \cup K_2)$. Show:

(a) $[\,K_1K_2 : K_2\,] \leqslant [\,K_1 : K\,]$

(b) $[\,K_1K_2 : K\,] \leqslant [\,K_1 : K\,] \cdot [\,K_2 : K\,]$

(c) If $\gcd([\,K_1 : K\,], [\,K_2 : K\,]) = 1$, then equality holds in (b).

Remark: If equality holds in (b), $K_1$ and $K_2$ are said to be *linearly disjoint* over $K$.

*Solution*: (a) Let $A$ be a basis of $K_1$ over $K$. Since $K_1 = K(A)$, we also have $K_1K_2 = K_2(A)$. We know from the lectures that for $a \in A$ we have $K_2(a) = K_2[a]$. Applying this iteratively to the elements of $A$ yields that $K_2(A) = K_2[A]$. Thus, we see that $K_1K_2 = \left\{\sum' a_ib_i : a_i \in K_1, b_i \in K_2\right\}$, where $\sum'$ denotes a finite sum. From this, we observe that $A$ is a generating system of $K_1K_2$ as a $K_2$-vector space. Therefore, $[\,K_1K_2 : K_2\,] \leqslant |A| = [\,K_1 : K\,]$.

(b) The multiplicativity of field degrees and part (a) imply

$$[\,K_1K_2 : K\,] = [\,K_1K_2 : K_2\,] \cdot [\,K_2 : K\,] \leqslant [\,K_1 : K\,] \cdot [\,K_2 : K\,].$$

(c) It suffices to show that if $\gcd([\,K_1 : K\,], [\,K_2 : K\,]) = 1$, then $[\,K_1K_2 : K\,] \geqslant [\,K_1 : K\,] \cdot [\,K_2 : K\,]$. Since $[\,K_1K_2 : K\,] = [\,K_1K_2 : K_2\,] \cdot [\,K_2 : K\,]$, $[\,K_2 : K\,]$ divides $[\,K_1K_2 : K\,]$. Similarly, $[\,K_1 : K\,]$ divides $[\,K_1K_2 : K\,]$. From the coprimality, we deduce that $[\,K_1 : K\,] \cdot [\,K_2 : K\,]$ divides the degree $[\,K_1K_2 : K\,]$, and thus

$$[\,K_1K_2 : K\,] \geqslant [\,K_1 : K\,] \cdot [\,K_2 : K\,].$$