Solutions to some problems in Vector spaces and Field theory

Exercise. Let \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) be the field generated by elements of the form \( a + b\sqrt{2} + c\sqrt{3} \), where \( a, b, c \in \mathbb{Q} \). Show that \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) is a vector space of dimension 4 over \( \mathbb{Q} \) and find a basis for this vector space.

**Sketch of solution.** If \( F \subseteq K \) is a field extension, then \( K \) is an \( F \)-vector space. The addition on \( K \) is just the field addition. The scalar multiplication map \( F \times K \to K \) is the restriction to \( F \times K \) of the field multiplication map \( K \times K \to K \). So \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) is a vector space over \( \mathbb{Q} \). (You can also verify the vector space axioms directly, “by hand” but this is not necessary).

Write \( K = \mathbb{Q}(\sqrt{2}) \). One verifies easily that \( [K : \mathbb{Q}] = 2 \). We claim that \( \sqrt{3} \notin K \). If \( \sqrt{3} \) did belong to \( K \), we could write \( \sqrt{3} = a + b\sqrt{2} \) with \( a, b \in \mathbb{Q} \). Then \( 3 = a^2 + 2b^2 + 2ab\sqrt{2} \), which implies \( 2ab\sqrt{2} \in \mathbb{Q} \). Since \( \sqrt{2} \) is not rational, it follows that \( a = 0 \) or \( b = 0 \), but this leads to \( \sqrt{3} = b\sqrt{2} \) or \( \sqrt{3} = a \) respectively, both of which are not true (since \( \sqrt{3} \) and \( \sqrt{3}/\sqrt{2} \) are not rational either; this can be proved the same way you show \( \sqrt{2} \) is irrational).

The dimension of this vector space is 4, we find that \( \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \) must be a basis.

Exercise. Let \( V \) be a vector space over a field \( F \). Let \( \alpha \in F \) and \( v \in V \). Show that \( (-\alpha)v = -(\alpha v) = \alpha(-v) \).

**Sketch of proof.** To be careful, we let \( 0 \) be the zero of \( F \) and let \( \vec{0} \) be the zero of \( V \). From the vector space axioms, we have \( 0.v = (0 + 0).v = 0.v + 0.v \). Since \( (V, +, \vec{0}) \) is an additive group, it follows that \( 0.v = \vec{0} \). Similarly one argues that \( \alpha.\vec{0} = \vec{0} \) for all \( \alpha \in F \).

Now \( \vec{0} = 0.v = (\alpha + (-\alpha)).v = \alpha.v + (-\alpha).v \). So \( (-\alpha).v \) is the additive inverse of \( \alpha.v \) in the abelian group \((V, +, \vec{0})\), that is, \( (-\alpha).v = -(\alpha.v) \).

Similarly, using \( \alpha.\vec{0} = \vec{0} \), we get \( \vec{0} = \alpha.\vec{0} = \alpha.(v + (-v)) = \alpha.v + \alpha.(-v) \) and hence \( -(\alpha.v) = \alpha.(-v) \).
that has less than or equal to \( n \) elements. In particular \( V \) is finite dimensional. Let \( m > n \) and \( u_1, \ldots, u_m \) be an \( m \) element subset of \( V \). Then we know \( \{ u_1, \ldots, u_m \} \) can be extended to a basis (lemma 8.9). This would give a basis of \( V \) with more than \( m \) elements, which contradicts the fact that any two basis of \( V \) have the same number of elements (theorem 8.10).

I wrote the result number we are using (like theorem 8.10) just for your convenience. Of course you do not have to do it in an exam. Just write it in a way that makes it clear what you are referring to. For example, I think that the references to the results in the above proof are pretty clear even without quoting the result number explicitly like I did. If you feel it is not quite clear, you may quote the actual result you are using, but most of the time, one can get by without having to do this.

\[
\text{Exercise. Show that } \mathbb{Q}(\sqrt{2}) \text{ and } \mathbb{Q}(\sqrt{3}) \text{ are non isomorphic fields.}
\]

\[
\text{sketch of solution. Suppose } f : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{2}) \text{ was a field isomorphism. Let } \alpha \in f(\sqrt{3}) \in \mathbb{Q}(\sqrt{2}). \text{ Then } \alpha^2 = f(\sqrt{3})^2 = f(3) = f(1) + f(1) = 1 + 1 + 1 = 3. \text{ Since } \alpha \in \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \text{ and } \alpha^2 = 3, \text{ we find that } \alpha = \pm \sqrt{3}. \text{ It follows that } \pm \sqrt{3} \in \mathbb{Q}(\sqrt{2}). \text{ But we already saw in an exercise above that } \sqrt{3} \notin \mathbb{Q}(\sqrt{2}).
\]

Chapter 21 \#1(b). Find the minimal polynomial of \( 3^{1/2} + 5^{1/3} \) over \( \mathbb{Q} \).

\[
\text{solution. Let } a = 3^{1/2} + 5^{1/3}. \text{ Then } a - \sqrt{3} = 5^{1/3}, \text{ so } 5 = (a - \sqrt{3})^3 = a^3 - 3\sqrt{3}a^2 + 9a - 3\sqrt{3}. \text{ Rearranging, we get } (a^3 + 9a - 5) = \sqrt{3}(3a^2 + 3). \text{ Squaring both sides and moving all the terms to one side we get a polynomial } f(x) \in \mathbb{Z}[x] \text{ such that } f(a) = 0. \text{ So } a \text{ is algebraic and its minimal polynomial has degree at most } 6. \text{ We claim that this polynomial } f(x) \text{ is the minimal polynomial of } a \text{ over } \mathbb{Q}. \text{ Let } K = \mathbb{Q}(a). \text{ Since } a \text{ satisfies a polynomial of degree } 6, \text{ the minimal polynomial of } a \text{ has degree at most six, so } [K : \mathbb{Q}] \leq 6. \text{ From the above calculation, we find } \sqrt{3} = (a^3 + 9a - 5)/(3a^2 + 3) \in K. \text{ So } 5^{1/3} = a - \sqrt{3} \in K \text{ as well. So } \mathbb{Q}(\sqrt{3})/\mathbb{Q} \text{ and } \mathbb{Q}(5^{1/3})/\mathbb{Q} \text{ are sub-extensions of } K/\mathbb{Q}. \text{ Note that } 5^{1/3} \text{ satisfies the polynomial } x^3 - 5 = 0 \text{ and this polynomial is irreducible over } \mathbb{Q} \text{ (since it has no rational roots, or say, by the Eisenstein’s criteria). So } [\mathbb{Q}(5^{1/3}) : \mathbb{Q}] = 3. \text{ Similarly } \sqrt{3} \text{ satisfies the polynomial } x^2 - 3 = 0 \text{ which is also irreducible over } \mathbb{Q} \text{ (since it has no rational roots). So } [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2. \text{ We have } [K : \mathbb{Q}] = [K : \mathbb{Q}(5^{1/3})][\mathbb{Q}(5^{1/3}) : \mathbb{Q}] = 3[K : \mathbb{Q}(5^{1/3})]. \text{ So } [K : \mathbb{Q}] \text{ is a multiple of } 3. \text{ Similarly } [K : \mathbb{Q}] \text{ is a multiple of } 2. \text{ So } [K : \mathbb{Q}] \geq 6. \text{ It follows that } [K : \mathbb{Q}] = 6. \text{ Since } [\mathbb{Q}(a) : \mathbb{Q}] \text{ is equal to the degree of the minimal polynomial of } a, \text{ it follows that } f(x) \text{ is the minimal polynomial.}
\]

Chapter 21 \#2 (c). Find a basis for \( \mathbb{Q}(\sqrt{2}, i) \) as a \( \mathbb{Q} \)-vector space.

\[
\text{sketch of solution. A basis for the extension } \mathbb{Q}(\sqrt{2}, i)/\mathbb{Q} \text{ is given by } \{ 1, \sqrt{2}, i, 2i \}. \text{ The degree of the extension is } 4. \text{ Let } K = \mathbb{Q}(\sqrt{2}). \text{ Consider the tower of extensions } \mathbb{Q} \subseteq K \subseteq K(i) = \mathbb{Q}(i, \sqrt{2}). \text{ Verify that } [K : \mathbb{Q}] = 2. \text{ Also } [K(i) : K] > 1 \text{ since } K \subseteq \mathbb{R} \text{ and } i \notin \mathbb{R}. \text{ The number } i \text{ is a root of the polynomial } x^2 + 1 \in K[x], \text{ so } [K(i) : K] \leq 2. \text{ It follows that } [K(i) : K] = 2 \text{ as well. So } [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4. \text{ Note that } \{ 1, \sqrt{2} \} \text{ is a basis of } K \text{ over } \mathbb{Q} \text{ and } \{ 1, i \} \text{ is a basis of } K(i) \text{ over } K. \text{ So a basis of } K(i) \text{ over } \mathbb{Q} \text{ is obtained by multiplying the basis elements pairwise (see the proof of theorem 10.4 in classnotes). This gives the basis we mentioned above.}
\]
Chapter 21 #9. Show that \( \mathbb{Q}(3^{1/2}, 3^{1/4}, 3^{1/8}, \ldots) \) is an infinite algebraic extension of \( \mathbb{Q} \).

Sketch of solution. To fix ideas it may help to observe that all the fields discussed in this exercise are subfields of \( \mathbb{C} \). Let \( K = \mathbb{Q}(3^{1/2}, 3^{1/4}, 3^{1/8}, \ldots) \). Let \( K_n = \mathbb{Q}(3^{1/2^n}) \). Note that \( 3^{1/2^n} \) satisfies the polynomial \( x^{2^n} - 3 = 0 \) which is irreducible by Eisenstein’s criteria, so \([K_n : \mathbb{Q}] = 2^n\). In particular \( K_n/\mathbb{Q} \) is finite hence algebraic extension. Observe that \( K_n \subseteq K \), \( K_1 \subseteq K_2 \subseteq \cdots \) and \( K = \bigcup_{n=1}^{\infty} K_n \) (just verify that an increasing union of subfields is again a field, so \( \bigcup_{n=1}^{\infty} K_n \) is a field and it contains all the \( 3^{1/2^n} \), so it must contain \( K \), the other inclusion is clear). So if \( a \in K \), then \( a \in K_n \) for some \( n \geq 1 \). Since \( K_n/\mathbb{Q} \) is algebraic extension, it follows that \( a \) is algebraic over \( \mathbb{Q} \). Since each \( a \in K \) is algebraic over \( \mathbb{Q} \), the extension \( K/\mathbb{Q} \) is algebraic.

If \( K/\mathbb{Q} \) were finite, then \([K : \mathbb{Q}] = [Q : K_n][K_n : K] = 2^n[K_n : K] \) which shows \([K : \mathbb{Q}] \) is a multiple of \( 2^n \) for all \( n \) which is absurd. So \( K/\mathbb{Q} \) is an infinite extension. \( \square \)

Chapter 21 #13. Show that the fields \( \mathbb{Q}(3^{1/4}) \) and \( \mathbb{Q}(3^{1/4}i) \) are not equal but are isomorphic.

solution. Consider the polynomial \( f(x) = x^4 - 3 \in \mathbb{Q}[x] \). This polynomial is irreducible in \( \mathbb{Q}[x] \) by Eisenstein’s criteria. Note that both \( 3^{1/4} \) and \( 3^{1/4}i \) are roots of the polynomial \( f(x) \). So \( f(x) \) is the minimal polynomial of both these numbers. It follows that \( \mathbb{Q}(3^{1/4}) \cong \mathbb{Q}[x]/(f(x)) \) and \( \mathbb{Q}(3^{1/4}i) \cong \mathbb{Q}[x]/(f(x)) \). So the two fields \( \mathbb{Q}(3^{1/4}) \) and \( \mathbb{Q}(3^{1/4}i) \) are isomorphic. These two fields are not equal since, for example the first field is contained in \( \mathbb{R} \) while the second one is not. \( \square \)

Exercise: Let \( a \) and \( b \) be non-square positive integers such that \( \gcd(a, b) = 1 \). Show that \( \mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b}). \)

solution. Let \( c = \sqrt{a} + \sqrt{b} \). Note that \( c^2 = a + b + 2\sqrt{ab} \), so \( \sqrt{ab} = (c^2 - a - b)/2 \in \mathbb{Q}(c) \). Now it follows that \( \sqrt{b} = (\sqrt{ab} + b)/c \in \mathbb{Q}(c) \). Similarly, \( \sqrt{a} \in \mathbb{Q}(c) \) as well. So \( \mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}(c) \). The other inclusion is clear. \( \square \)

One more old homework problem: Let \( R \) be a commutative ring and \( P_1, \ldots, P_n \) be prime ideals in \( R \). Suppose \( I \) is an ideal of \( R \) such that \( I \) is not contained in \( P_j \) for each \( j \). Then \( I \) is not contained in \( P_1 \cup \cdots \cup P_n \).

solution. Induct on \( n \), the case \( n = 1 \) is trivial. Suppose the result holds for \( n - 1 \). Then by induction hypothesis, \( I \) is not contained in \( P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_n \) for each \( i \). So we may pick \( x_i \in I \) such that \( x_i \notin P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_n \). If \( x_i \notin P_i \) as well for some \( i \), then we are done. So we may assume \( x_i \in P_i \) for each \( i \) and \( x_i \notin P_j \) for each \( j \neq i \). Let \( x = \sum x_1 \cdots x_{i-1}x_{i+1} \cdots x_n \in I \). Note that each term in the sum except the first one is in \( P_1 \), so if \( x \in P_1 \), then that would imply that the first term \( x_2x_3 \cdots x_n \in P_1 \) which would imply \( x_j \in P_1 \) for some \( j \neq 1 \), which is a contradiction. So \( x \notin P_1 \). By identical argument, we conclude that \( x \notin P_j \) for each \( j \). \( \square \)