

1. Mark each of the following statements T (for 'True') or F (for 'False'). No explanation is required. If you skip a question, you do not get any points for it, so it is better to guess the answer.

(a) If the algebraic closures of two fields are isomorphic, the fields themselves are isomorphic.

False: $\overline{\mathbb{C}} = \mathbb{C} = \overline{\mathbb{R}}$.

(b) $\sqrt{2}$ and $-\sqrt{2}$ are conjugate over the field of real numbers \mathbb{R} .

False: their irreducible polynomials are $x - \sqrt{2}$ and $x + \sqrt{2}$, respectively.

(c) The non-zero elements of any field form a cyclic group with respect to multiplication.

False: For instance, the multiplicative group of non-zero real numbers is not cyclic.

(d) If $\alpha, \beta \in \mathbb{C}$ are conjugate over \mathbb{R} , they are also conjugate over \mathbb{Q} .

True: The minimal polynomial $p(x)$ of α over \mathbb{Q} does not need to be irreducible over \mathbb{R} , but it is at least divisible by the minimal polynomial $q(x)$ of α over \mathbb{R} . If $q(\beta) = 0$, then $p(\beta) = 0$.

(e) If a field F contains a primitive 10th root of unity, the equation $x^{10} = 1$ has exactly ten solutions in F .

True: It cannot have more than ten solutions (it is a 10th degree polynomial), and clearly all elements $1, x, x^2, \dots, x^9$ solve the equation. They are all distinct, because x is primitive.

2. (a) Find all conjugates of $\alpha = 2^{1/3} + i$ over \mathbb{Q} (here $i = \sqrt{-1}$). Do not forget to include α itself.

Let $\zeta = \frac{-1+\sqrt{-3}}{2}$ be a primitive cubic root of unity in \mathbb{C} (so $\zeta^3 = 1$, $\zeta \neq 1$). Then the conjugates of $2^{1/3}$ are $2^{1/3}$, $\zeta 2^{1/3}$, and $\zeta^2 2^{1/3}$. Similarly, conjugates of i are $\pm i$. This implies that α has 6 conjugates:

$$2^{1/3} \pm i, \zeta 2^{1/3} \pm i, \text{ and } \zeta^2 2^{1/3} \pm i.$$

(b) Find all conjugates of the same α over \mathbb{R} .

The degree of α over \mathbb{R} is 2, and its minimal polynomial is $(x - 2^{1/3})^2$. The conjugates of α are the roots of this polynomial: $2^{1/3} \pm i$.

(c) Find all conjugates of α over \mathbb{C} .

The minimal polynomial of α over \mathbb{C} is $x - \alpha$, so α has no other conjugates over \mathbb{C} .

3. Consider the field $E = \mathbb{Q}(\sqrt{2}, i) \supset \mathbb{Q}$. A homomorphism $\phi : E \rightarrow \overline{\mathbb{Q}}$ has the following properties: its restriction to $\mathbb{Q}(\sqrt{2}) \subset E$ is $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, while the restriction to $\mathbb{Q}(i) \subset E$ equals $a + bi \mapsto a - bi$. Find the restriction of ϕ to $\mathbb{Q}(\sqrt{-2}) \subset E$.

Clearly, $\phi(\sqrt{-2}) = \phi(\sqrt{2})\phi(i) = \sqrt{-2}$, therefore $\phi(a + b\sqrt{-2}) = a + b\sqrt{-2}$. This proves that the restriction is the identity.

4. Prove that a degree 5 polynomial $P \in \mathbb{Z}_5[x]$ is irreducible if and only if it has no roots in $GF(125)$.

Suppose P has a root $a \in GF(125)$. Then $\deg(a, \mathbb{Z}_5) \leq [GF(125) : \mathbb{Z}_5] = 3$, so the minimal polynomial of a over \mathbb{Z}_5 has degree at most 3. The minimal polynomial divides P , so P is reducible.

Conversely, suppose P is reducible. It is easy to see that then P has an irreducible factor $Q(x) \in \mathbb{Z}_5[x]$ of degree either 1 or 3. If $\deg(Q) = 1$, then Q has a root

a in $\mathbb{Z}_5 \subset GF(125)$; clearly, $P(a) = 0$. If $\deg(Q) = 3$, let a be a root of Q in $\overline{\mathbb{Z}_5}$. Then $\deg(a, \mathbb{Z}_5) = 3$, and $[\mathbb{Z}_5(a), \mathbb{Z}_5] = 3$. This implies $\mathbb{Z}_5(a) = GF(125)$, so $a \in GF(125)$ is a root of Q (and so also of P).

5. (a) Let p be an odd prime, and $a \in \overline{\mathbb{Z}_p}$ be a quartic (4th) primitive root of unity. Find the degree of a over \mathbb{Z}_p (your answer will depend on whether $p = 4k + 1$ or $p = 4k + 3$).

Recall that the multiplicative group of $GF(p^n)$ is a multiplicative group of order $p^n - 1$. $GF(p^n)$ contains a primitive quartic root of unity if and only if this group has elements of order exactly 4; this happens if and only if $4 \mid p^n - 1$. Note also that if b is a primitive n -th root of unity, all other n -th roots of unity are powers of b , so if a field contains one primitive n -th root of unity, it contains all of them.

Suppose $p = 4k + 1$, so $4 \mid p - 1$. Then the previous argument shows that $a \in GF(p) = \mathbb{Z}_p$, so the degree of a over \mathbb{Z}_p equals 1. On the other hand, if $p = 4k + 3$, then $4 \nmid p - 1$, $4 \mid p^2 - 1$, so $a \notin \mathbb{Z}_p$, $a \in GF(p^2)$, and the degree of a over \mathbb{Z}_p equals 2.

(b) Prove that there are no primitive quartic roots of unity in $\overline{\mathbb{Z}_2}$.

Let $a \in \overline{\mathbb{Z}_2}$ be a quartic root of unity. Then $0 = a^4 - 1 = a^4 + 1 = (a + 1)^4 = (a - 1)^4$, so $a = 1$. Clearly, 1 is not a primitive quartic root of unity.

Additional problems

1. As $2^{1/2}$ is irrational, its minimal polynomial equals $x^2 - 2$, so $[\mathbb{Q}(2^{1/2}) : \mathbb{Q}] = 2$. Similarly, $[\mathbb{Q}(3^{1/3}) : \mathbb{Q}] = 3$. Notice that $2^{1/2} \notin \mathbb{Q}(3^{1/3})$ (because 2 does not divide 3), so by the same argument, $[(\mathbb{Q}(3^{1/3}))(2^{1/2}) : \mathbb{Q}(3^{1/3})] = 2$. So the degree you are asked to find equals 6.

2. Actually, such an extension does not exist. Indeed, if F has this property, then minimal polynomial of any element $\alpha \in F - \mathbb{R}$ must have degree 3 (we know that its degree must divide 3), but there are no irreducible cubic polynomials over \mathbb{R} (because any cubic polynomial has a root). Remark: it can be shown that any algebraic extension of a field is isomorphic to a subfield of the algebraic closure; since the algebraic closure of \mathbb{R} has degree 2 over \mathbb{R} , the only non-trivial algebraic extension of \mathbb{R} is $\mathbb{C} \supset \mathbb{R}$ (in the sense that any other algebraic extension is isomorphic to this one).

3. Set $\alpha = \sqrt{3} - \sqrt{5}$. We see that $\alpha^2 = 8 + 2\sqrt{15}$, so $(\alpha^2 - 8)^2 - 60 = 0$. In this way, we see that α is a root of a quartic polynomial (a more standard way to find it would be to start writing powers: $1, \alpha, \alpha^2, \alpha^3, \dots$ and look for linear dependence). Now we should check that this is actually the minimal polynomial. Indeed, if we set $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, it is easy to see that $[E : \mathbb{Q}] = 4$ (because $\sqrt{3}$ is irrational and $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$). Thus, $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ form a basis of E over \mathbb{Q} , and from the explicit formulas, one sees that $\{1, \alpha, \alpha^2, \alpha^3\}$ are linearly independent, and so α is not a root of any polynomial of degree less than 4. Actually, since $\alpha \in E$, we know that the degree of α must divide 4, so it is enough to check that $\{1, \alpha, \alpha^2\}$ are linearly independent.

4. Any element of degree 3 must generate $GF(27)$ over \mathbb{Z}_3 ; on the other hand, as $[GF(27) : \mathbb{Z}_3] = 3$, the degree of any element of $GF(27)$ (over \mathbb{Z}_3) divides 3, that is, it is either 1 or 3. Since only the elements of \mathbb{Z}_3 have degree 1, the set of all elements of degree 3 is $GF(27) - \mathbb{Z}_3$, which has $27 - 3 = 24$ elements.

5. The multiplicative group $GF(4)^\times$ is isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$. Any non-zero element of $\mathbb{Z}/3\mathbb{Z}$ has order 3, so any $a \in GF(4)^\times$ which is not the unity is a primitive cubic root of unity.

6. If α has degree 2 over \mathbb{Z}_3 , then $\alpha \in GF(9)$, so $\alpha^9 = \alpha$. Setting $\beta = \alpha^4$, we need to check that $\beta^3 = \beta$ (this is the defining property of \mathbb{Z}_3). But $\beta^3 = \alpha^{12} = \alpha^3\alpha^9 = \alpha^3\alpha = \alpha^4 = \beta$.

7. The multiplicative group $GF(25)^\times$ is a cyclic group of order 24, so there are two elements of degree 4: if we identify $GF(25)^\times$ with $\mathbb{Z}/24\mathbb{Z}$, they are the cosets of 6 and of 18. As for \mathbb{C} , we are looking for elements $z \in \mathbb{C}$ such that $z^4 = 1$, but $z^n \neq 1$ for any $n < 4$. There are two such elements: $\sqrt{-1}$ and $-\sqrt{-1}$.

8. The easiest way is to use a problem from the homework, which states that $(x^{64} - x)$ is the product of all irreducible monic polynomials in $\mathbb{Z}_2[x]$ whose degree divides 6. Notice that in $\mathbb{Z}_2[x]$, any non-zero polynomial is monic. Denote by P_k the product of all irreducible polynomials of degree k , then the statement is that $x^{64} - x = P_6 P_3 P_2 P_1$. Notice that there are only two polynomials of degree 1, and $P_1 = x(x + 1)$. Since $P_1 P_2 = x^4 - x$, we know that $\deg(P_2) = 2$. Similarly, $\deg(P_3) = 8 - 2 = 6$. This implies that $\deg(P_6) = 64 - 2 - 2 - 6 = 54$. As P_6

is a product of polynomials of degree 6, the number of polynomials in the product equals $54/6 = 9$.

9. Clearly, 0 is algebraic over F , so let us assume $\alpha \neq 0$. As α lies in the subfield formed by polynomials of α , its inverse should also belong to this subfield. Thus, $1/\alpha = P(\alpha)$ for some $P(x) \in F[x]$, and α is a root of polynomial $xP(x)$.

10. Notice that ϕ^2 is the operator of multiplication by α^2 ; that is, $\phi^2 : z \mapsto \alpha^2 z$. More generally, for any polynomial $P(x) \in F[x]$, we have $P(\phi) : z \mapsto P(\alpha)z$. Let σ be the characteristic polynomial of ϕ ; by the Cayley-Hamilton Theorem, $\sigma(\phi) = 0$, so we see that $\sigma(\alpha) = 0$. Now notice that the degree of σ equals the dimension of E over F ; on the other hand, the degree of a minimal polynomial of α equals $[F(\alpha) : F]$. Since we assumed $E = F(\alpha)$, the degree of σ equals the degree of a minimal polynomial, so σ is a minimal polynomial.

11. Set $F = \mathbb{R}(x^2)$, $E = \mathbb{R}(x)$. It is easy to see that $E = F(\alpha)$, where $\alpha = x \in \mathbb{R}(x)$. The degree of the simple extension $[F(\alpha) : F]$ equals the degree of the minimal polynomial of α over F . Notice that α satisfies the equation $\alpha^2 - (x^2) = 0$ (the coefficient x^2 is in $\mathbb{R}(x^2)$), so the degree of the extension is at most 2. Since $x \notin \mathbb{R}(x^2)$, the degree cannot be 1, so it equals 2.