QUIZ

(1) Let $f(x) \in F[x]$ be a separable polynomial, let K be a splitting field of f over F, then the Galois group, $G(f)$, of f is defined to be the group $\mathrm{Gal}(K/F)$. Now, the Galois groups $G(f)$ and $G(g)$ over $\mathbb{Q}$ of the polynomials $f(x) = x^3 - 3x + 1$ and $g(x) = x^3 + 3x - 1$ are
 (a) $G(f) = G(g) = A_3$.
 (b) $G(f) = G(g) = S_3$.
 (c) $G(f) = S_3$ and $G(g) = A_3$.
 (d) $G(f) = A_3$ and $G(g) = S_3$
 Answer: (d). Both f and g are irreducible over $\mathbb{Q}$. Also $disc(f) = 81$ and $disc(g) = -135$, hence $G(f) = A_3$ and $G(g) = S_3$.

(2) Let $\mathbb{F}_q$ denote the finite field of cardinality q, where q is a prime power. Consider the following three statements: (P) $\mathbb{F}_{2401}$ contains a subfield isomorphic to $\mathbb{F}_{49}$, and (Q) The two fields $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ are isomorphic, (R) The multiplicative group $\mathbb{F}_{121}^*$ contains an element of order 11 . Then,
 (a) All statements are true.
 (b) Two of the statements are true.
 (c) Two of the statements are false.
 (d) All statements are false.
 Answer: (b). (P) and (Q) are true, (R) is false.

(3) Let $\mathbb{F}_q$ denote the finite field of cardinality q, where q is a prime power. Which element does NOT generate $\mathbb{F}_{11}^*$?
 (a) 2 (mod 11).
 (b) 3 (mod 11).
 (c) 7 (mod 11).
 (d) 8 (mod 11)
 Answer: (b). 3 (mod 11) is not a generator, the other elements are generators.

(4) Let $\mathbb{F}_q$ denote the finite field of cardinality q, where q is a prime power. The number of subfields of $\mathbb{F}_{4096}$ are
 (a) Two
 (b) Four
 (c) Six
 (d) Twelve
 Answer (c): Note that $4096 = 2^{12}$ and so $\mathrm{Gal}(\mathbb{F}_{4096}/\mathbb{F}_2) = \mathbb{Z}/12\mathbb{Z}$. Hence, the number of subfields is equal to the number of subgroups of a cyclic group of order 12, which is six.

(5) The number of irreducible polynomials of degree 6 over $\mathbb{F}_2$ is
 (a) One
 (b) Three
 (c) Six
 (d) Nine

Answer (d): We know that $x^{64}-x$ is the product of all irreducible polynomials over $\mathbb{F}_2$ of degree d where d is a divisor of 6 (that is, $d=1,2,3,6$). The irreducible polynomials of degrees $1,2$ and 3 over $\mathbb{F}_2$ are $x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1$, hence their degrees add up to $1+1+2+3+3=10$. Hence the number of irreducible polynomials of degree 6 over $\mathbb{F}_2$ is $(64-10)/6=9$.

(6) Let $\mathbb{F}_q$ denote the finite field of cardinality q, where q is a prime power. The number of intermediate subfields L such that $\mathbb{F}_8 \subset L \subset \mathbb{F}_{32}$ are
(a) One
(b) Two
(c) Four
(d) None of the above

Answer (d). Actually $\mathbb{F}_8$ is not contained in $\mathbb{F}_{32}$ (since $8=2^3$ and $32=2^5$, and 3 does not divide 5). So the number of such subfields is zero, and the correct answer is (d).