Nepal Algebra Project 2019. Module 4. Problem set 1. Solutions.

Due Tuesday July 9, 2019, at 24:00 Kathmandu time

1. *Consider the extension* $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(a) Prove that its Galois group over $\mathbf{Q}$ *is isomorphic to the group* $\mathbf{Z}_2 \times \mathbf{Z}_2$.

(b) Enumerate the subgroups H *of* $\mathbf{Z}_2 \times \mathbf{Z}_2$.

(c) Describe the Galois correspondence between subgroups of $\mathbf{Z}_2 \times \mathbf{Z}_2$ *and subfields of* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Sol.: (a) Any automorphism σ of $F = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ satisfies $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$. The map $\mathrm{Gal}(F/\mathbf{Q}) \longrightarrow \{\pm 1\} \times \{\pm 1\}$ given by $\sigma \mapsto ()$ is an injective group homomorphism. By Galois theory both sides have the same cardinality. Therefore the map is actually an isomorphism. (b) The group $\{\pm 1\} \times \{\pm 1\}$ is isomorphic to the Klein's fourgroup. Apart from the trivial subgroups, it has three subgroups of order 2, each generated by an element of order 2. (c) The subfields corresponding to the trivial subgroups, are the trivial subfields of F: the field F itself and $\mathbf{Q}$. The fixed field of the three subgroups of order 2 are $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{6})$ respectively.

2. *Let* ζ_9 *be a primitive ninth root of unity.*

(a) Show that ζ_9 *is a zero of* $f(X) = (X^9 - 1)/(X^3 - 1) = X^6 + X^3 + 1$ *and show that* $f(x)$ *is the minimum polynomial of* ζ_9 *over* $\mathbf{Q}$.

(b) Show that $\mathbf{Q} \subset \mathbf{Q}(\zeta_9)$ *is a Galois extension with Galois group* $\mathbf{Z}_9^*$.

(c) Enumerate the subgroups H *of* $\mathbf{Z}_9^*$.

(d) Describe the Galois correspondence between subgroups of $\mathbf{Z}_9^*$ *and subfields of* $\mathbf{Q}(\zeta_9)$.

Sol.: (a) Since $\zeta_9^9 = 1$, while $\zeta_9^3 \neq 1$, the fact that $X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$ implies that ζ_9 is a zero of $X^6 + X^3 + 1$. Making the change of variable $X = Y + 1$, the polynomial $X^6 + X^3 + 1$ becomes Eisenstein with respect to the prime 3. Therefore it is irreducible and hence is the mimimum polynomial of ζ_9. (b) Since the roots of $X^9 - 1$ and hence of $X^6 + X^3 + 1$ are powers of ζ_9, the field $\mathbf{Q}(\zeta_9)$ is a splitting field of $X^6 + X^3 + 1$. Therefore it is a Galois extension of $\mathbf{Q}$. For any $\sigma \in G = \mathrm{Gal}(\mathbf{Q}(\zeta_9)/\mathbf{Q})$ there is a unique element $a_\sigma \in \mathbf{Z}_9^*$ for which $\sigma(\zeta_9) = \zeta_9^{a_\sigma}$. The map $\sigma \mapsto a_\sigma$ is an isomorphism of groups $\mathrm{Gal}(\mathbf{Q}(\zeta_9)/\mathbf{Q}) \longrightarrow \mathbf{Z}_9^*$. (c) The group $\mathbf{Z}_9^*$ is cyclic of order 6 it has four subgroups of order 1, 2, 3 and 6 rexpectively. The corresponding subfields are $\mathbf{Q}(\zeta_9)$, $\mathbf{Q}$, $\mathbf{Q}(\zeta_9 + \zeta_9^{-1})$ and $\mathbf{Q}(\zeta_3)$.