Nepal Algebra Project 2016 Final exam Solutions

Tribhuvan University

July 30^{th} 2016

1. Consider the polynomial $f(X) = X^5 - 4X \in \mathbb{Z}[X]$. Let E be the decomposition field of f over $\mathbb{Q}$.
(a) Give a basis of E over $\mathbb{Q}$.
(b) Check that the Galois group G_f of f over $\mathbb{Q}$ is isomorphic to the subgroup of $\mathfrak{S}_5$ generated by two disjoint transpositions.
(c) For each subgroup H of G_f, give the subfield E^H of E fixed by H.
(d) Give the list of subfields of E.
(e) Give a primitive element of E over $\mathbb{Q}$.

Solutions. **(a)** The decomposition of f as a product of irreducible polynomials over $\mathbb{Q}$ is $f(X) = X(X^2 - 2)(X^2+2)$. The complex roots of f are 0, $\sqrt{2}$, $-\sqrt{2}$, $i\sqrt{2}$ and $-i\sqrt{2}$ with $i^2 = -1$. Choose an ordering, say $\alpha_1 = 0$, $\alpha_2 = \sqrt{2}$, $\alpha_3 = -\sqrt{2}$, $\alpha_4 = i\sqrt{2}$ $\alpha_5 = -i\sqrt{2}$. The decomposition field E of f over $\mathbb{Q}$ is $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \mathbb{Q}(\alpha_2, \alpha_4) = \mathbb{Q}(\sqrt{2}, i\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$. Hence a basis of E over $\mathbb{Q}$ is $\{1, \sqrt{2}, i, i\sqrt{2}\}$. Any element in E can be written in a unique way $a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$. There are many other bases, for instance $\{1, \alpha_2, \alpha_4, \alpha_2\alpha_4\} = \{1, \sqrt{2}, i\sqrt{2}, 2i\}$.
(b) The elements in G_f permute the α_j, and they are determined by the corresponding permutation in $\mathfrak{S}_5$. These permutations are 1, $(2,3)$, $(4,5)$, $(2,3)(4,5)$. This is a non transitive subgroup of $\mathfrak{S}_5$, abelian non cyclic of order 4 (Klein group). The element of G_f associated to 1 is the identity of E. The element of G_f associated to $(2,3)$ is the automorphism of E which maps $\sqrt{2}$ to $-\sqrt{2}$ and $i\sqrt{2}$ to $i\sqrt{2}$; hence it maps i to $-i$. The image of $a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$ is $a_1 - a_2\sqrt{2} - a_3 i + a_4 i\sqrt{2}$. The element of G_f associated to $(4,5)$ is the automorphism of E which maps $\sqrt{2}$ to $\sqrt{2}$ and $i\sqrt{2}$ to $-i\sqrt{2}$; hence it maps i to $-i$; it is the complex conjugation. The image of $a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$ is $a_1 + a_2\sqrt{2} - a_3 i - a_4 i\sqrt{2}$.
The element of G_f associated to $(2,3)(4,5)$ is the automorphism of E which maps $\sqrt{2}$ to $-\sqrt{2}$ and $i\sqrt{2}$ to $-i\sqrt{2}$; hence it maps i to i. The image of $a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$ is $a_1 - a_2\sqrt{2} + a_3 i - a_4 i\sqrt{2}$.
(c) There are 5 subgroups of G_f, namely
- G_f, its fixed subfield is $\mathbb{Q}$;
- $\{1, (2,3)\}$, its fixed subfield is $\mathbb{Q}(i\sqrt{2})$;
- $\{1, (4,5)\}$, its fixed subfield is $\mathbb{Q}(\sqrt{2})$;
- $\{1, (2,3)(4,5)\}$, its fixed subfield is $\mathbb{Q}(i)$;
- $\{1\}$, its fixed subfield is E.

(d) There are 5 subfields of E, namely $\mathbb{Q}$, $\mathbb{Q}(i\sqrt{2})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, E. **(e)** There are many primitive elements of E over $\mathbb{Q}$, one of them is $\sqrt{2} + i$, it has 4 different images under the action of the Galois group, namely $\sqrt{2}+i, -\sqrt{2}-i, \sqrt{2}-i, -\sqrt{2}+i$.

2. Let $F = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Find $[F : \mathbb{Q}]$. If F normal over $\mathbb{Q}$?

Solutions. The element $\sqrt[3]{2}$ has miniml polynomial $x^3 - 2$ over $\mathbb{Q}$ and $\sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$. We also see that $\mathbb{Q}(\sqrt{2})$ cannot be contained in $\mathbb{Q}(\sqrt[3]{2})$. That implies $[F : \mathbb{Q}] = 6$. F is not a normal extension of $\mathbb{Q}$; if it were, then since it contains $\sqrt[3]{2}$ which is root of the irreducible polynomial $x^3 - 2$, it would have to contain all the other roots. But $F \subset \mathbb{R}$, while the other two roots are non-real. Thus F cannot be normal over $\mathbb{Q}$.

3. Find the order of the Galois group of $x^5 - 2$.

Solutions. Let G be the Galois group. Let ζ be a primitive 5-th root of unity. the the roots of $X^5 - 2$ are $\alpha = \sqrt[5]{2}$ and $\alpha\zeta^j$ for $j = 1, \ldots, 5$. Thus splitting field of $x^5 - 2$ is equal to $\mathbb{Q}(\sqrt[5]{2}, \zeta)$. Now $x^5 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and that implies it is minimal polynomial of α. $\zeta 4$ is a root of $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + 1)$. and thus its minimal polynomial is $q(x) = x^4 + x^3 + x^2 + 1$. Thus $[F : \mathbb{Q}] \leq 20$. But, since this degree must be divisible by both 5 as well as 4, It has to be exactly 20.

4. State the fundamental Theorem of Galois Theory (Galois correspondance).

Solutions. See the Milne's Notes, Theorem 3.16 (page 39).