HOMEWORK 4 SOLUTIONS

1. Problem 1

1. (a) We consider the multiplicativity of the degree with regards to the following tower:

$$\mathbb{Q} \subset \mathbb{Q}[2^{\frac{1}{3}}] \subset \mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3] \subset \mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3, 2^{\frac{1}{3}}(\zeta_3)^2]$$

as the elements adjoined in the last field are the roots of $x^3 - 2$ in $\mathbb{C}$, so the last field is the splitting field of $x^3 - 2$. We know $x^3 - 2$ to be irreducible over $\mathbb{Q}$, so the extension $\mathbb{Q} \subset \mathbb{Q}[2^{\frac{1}{3}}]$ is cubic. $x^3 - 2$ has at least one linear factor over $\mathbb{Q}[2^{\frac{1}{3}}]$, and its remaining factor(s) may be either one quadratic factor, or two linear factors. But neither of the remaining roots in $\mathbb{C}$ are real, and we have $\mathbb{Q}[2^{\frac{1}{3}}] \subset \mathbb{R}$. Hence $x^3 - 2$ splits into a linear and a quadratic factor over $\mathbb{Q}[2^{\frac{1}{3}}]$, and the extension $\mathbb{Q}[2^{\frac{1}{3}}] \subset \mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3]$ is quadratic. Since $x^3 - 2$ now has at least 2 linear factors over $\mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3]$, it must have 3 linear factors over this field, and thus $\mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3] = \mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3, 2^{\frac{1}{3}}(\zeta_3)^2]$, and the extension $\mathbb{Q} \subset \mathbb{Q}[2^{\frac{1}{3}}, 2^{\frac{1}{3}}\zeta_3, 2^{\frac{1}{3}}(\zeta_3)^2]$ is of degree 6. □

(b) $x^4 - 1$ is already reducible over $\mathbb{Q}$, with $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x + 1)(x - 1)(x^2 + 1)$. So the splitting field of $x^4 - 1$ will be the same as the splitting field of $x^2 + 1$. This field is clearly $\mathbb{Q}[i]$, which has degree 2 over $\mathbb{Q}$. □

(c) $x^4 + 1$ is irreducible over $\mathbb{Q}$ because $(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. The roots of $x^4 + 1$ in $\mathbb{C}$ are known to be ζ_8, $(\zeta_8)^3$, $(\zeta_8)^5$, and $(\zeta_4)^8$, so $\mathbb{Q} \subset \mathbb{Q}[\zeta_8]$ is a quartic extension, and every other root of $x^4 + 1$ is contained in $\mathbb{Q}[\zeta_8]$. Hence $\mathbb{Q}[\zeta_8]$ is the splitting field of $x^4 + 1$, and it has degree 4 over $\mathbb{Q}$. □

2. Problem 2

Let $K = \mathbf{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. Determine $\deg K/\mathbf{Q}$, prove that $K/\mathbf{Q}$ is a Galois extension, and determine its Galois group.

K is a Galois Extension

K is clearly a subfield of the splitting field of $(x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$ as it is constructed by adjoining roots of this polynomial. For each of $\sqrt{p}$, $p = 2, 3, 5, -\sqrt{p}$ is also a root and $-\sqrt{p} \in K$. Thus K contains all the roots so is the splitting field of $(x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$. This polynomial has no repeated roots so $K/\mathbb{Q}$ is a Galois extension.

degree of K

$\mathbb{Q}[\sqrt{3}]$ is not isomorphic to $\mathbb{Q}[\sqrt{2}]$ by previous assignment, as 3 is prime, so is not equal to 2 times a square. But if $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$, then $\mathbb{Q}[\sqrt{3}] = \mathbb{Q}[\sqrt{2}]$ as they are both degree 2 field extensions over $\mathbb{Q}$. But as they are not isomorphic, they are not equal, so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$

Thus $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is degree 2 over $\mathbb{Q}[\sqrt{2}]$, and hence degree 4 over $\mathbb{Q}$. As $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ formed by adjoining roots of $(x^2-2)(x^2-3)$, it is a subfield of the splitting field of that polynomial. As the other roots are just additive inverses of the first two roots, $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is equal to the splitting field of $(x^2-2)(x^2-3)$. As there are no repeated roots, $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a Galois extension. Thus there is a correspondence between its subfields and the subgroups of its automorphism group.

Let $g : \mathbb{Q}[\sqrt{2}, \sqrt{3}] \to \mathbb{Q}[x, y]/((x^2-2), (y^2-3))$ be a representation, with $g(x) = \sqrt{2}$, $g(y) = \sqrt{3}$. A ring homomorphism from $\mathbb{Q}[x, y]/((x^2-2), (y^2-3))$ to $\mathbb{C}$ must map x to $\pm\sqrt{2}$ and y to $\pm\sqrt{3}$ to have the ideal as part of the kernel. As each of these is in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, this means the image of the homomorphisms must be $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. As we have a homomorphism between isomorphic fields, it must be an isomorphism. Thus we can consider any automorphism to be g composed with one of these homomorphisms. There are two possible places to map x to, and two to map y to, and as the degree of the field extension is 4, the size of the automorphism group is 4, so these maps must all be distinct.

Given one of these automorphisms, ϕ, $\phi^2(\sqrt{2}) = \sqrt{2}$, as if ϕ changes the sign, then applying again will change it back. Similarly for $\phi^2(\sqrt{3})$. Thus every element of the group is its own inverse, so the group is isomorphic to $C_2 \times C_2$.

The only subgroups of this group are the trivial group and three copies of C_2. By the Galois correspondence theorem, these correspond to $\mathbb{Q}$, and three degree two subgroups of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are two of these subgroups. $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. As 6 is not equal to $2p^2$ or $3p^2$ for any integer p, by previous assignment question $\mathbb{Q}[\sqrt{6}]$ is not isomorphic to either of the other two subfields, so it cannot be equal to them. Thus we have all three subfields of degree 2 in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

As $\sqrt{5}$ is degree 2 over $\mathbb{Q}$, any degree 2 field extension of $\mathbb{Q}$ it is contained in will be equal to $\mathbb{Q}[\sqrt{5}]$. But by previous assignment, as 5 is not the product of 2 or 3 with a square number, and 6 is not the product of 5 with a square number, $\mathbb{Q}[\sqrt{5}]$ is not isomorphic to $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ or $\mathbb{Q}[\sqrt{6}]$. Hence $\sqrt{5}$ is not contained in any of them. As there are no other degree 2 subfields of $\mathbb{Q}[\sqrt{2},\sqrt{3}]$, it is not contained in that field either.

Thus $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]$ is degree 2 over $\mathbb{Q}[\sqrt{2},\sqrt{3}]$, and is thus degree 8 over $\mathbb{Q}$.

Automorphisms of $K/\mathbb{Q}$

Let $f : K \to \mathbb{Q}[x,y,z]/((x^2-2),(y^2-3),(z^2-5))$ be a presentation of K over $\mathbb{Q}$, such that $f(x) = \sqrt{2}$, $f(y) = \sqrt{3}$, $f(z) = \sqrt{5}$. A ring homomorphism from $\mathbb{Q}[x,y,z]/((x^2-2),(y^2-3),(z^2-5))$ to $\mathbb{C}$ must preserve each ideal, so it is uniquely described by whether it maps x to $\sqrt{2}$ or $-\sqrt{2}$, y to $\sqrt{3}$ or $-\sqrt{3}$ and z to $\sqrt{5}$ or $-\sqrt{5}$. As $\pm\sqrt{2},\pm\sqrt{3},\pm\sqrt{5} \in K$, this means that the ring homomorphisms must be isomorphism to K. Thus automorphisms of K are compositions of F with these homomorphisms.

For any automorphism ϕ of K, $\phi(\phi(\sqrt{2})) = \sqrt{2}$ as if the first application changes the sign, then the second will change it back, and if the first does not change it, then the second won't either. This also holds for each of $\sqrt{3}$ and $\sqrt{5}$. Thus every element of the Galois group is its own inverse. Thus as the size of the group is 8, it is isomorphic to $C_2 \times C_2 \times C_2$.

3. Problem 3

Note that K is a Galois extension (it is the splitting field of $x^{p-1}+\cdots+x+1$ over $\mathbb{Q}$, which has characteristic 0). We know from last assignment that the Galois group of K is isomorphic to $(\mathbb{Z}_p^*,\cdot)$, which is isomorphic to the cyclic group of order $p-1$. We know that the order of subgroups of cyclic groups divides the order of the group itself, and that there is exactly one subgroup for each divisor. Then as $p-1$ is even, we see that there is exactly one subgroup of C_{p-1} that has order $\frac{p-1}{2}$, or index 2.

As the Galois group of K only has one subgroup of index 2, it follows that K contains an unique degree 2 extension of $\mathbb{Q}$ by Galois correspondence.

Question 4

Lecture 22 April 41:43

Find quartic polynomials in $\mathbb{Q}[x]$ whose Galois group is isomorphic to:

a) The dihedral group D_4 of order 8.

We claim that $x^4 - 2$ has this Galois group. Let K be its splitting field. It was proven in lecture that the Galois group of $x^4 - 2$ over $\mathbb{Q}[i]$ is C_4, so $|\operatorname{Aut}(K/\mathbb{Q}[i])| = 4$. $\mathbb{Q}[i]$ itself is a Galois extension of degree 2 and so has a Galois group of size 2, i.e. $|\operatorname{Aut}\mathbb{Q}[i]/\mathbb{Q}| = 2$. The sizes of these groups corresponds to the degrees of the extensions, and so $\deg K/\mathbb{Q}[i] = 4$ and $\deg \mathbb{Q}[i]/\mathbb{Q} = 2$. Hence, applying the multiplicative property of the degree, $\deg K/\mathbb{Q} = 8$ and its Galois group must have size 8.

Furthermore, each automorphism in the Galois group permutes the roots of $x^4 - 2$ in a unique way, which defines an injective homomorphism from the Galois group to S_4. This implies the Galois group must in fact be a subgroup of S_4. Additionally, since $|S_4| = 2^3 \cdot 3$, all subgroups of size $8 = 2^3$ of S_4 are 2-Sylow subgroups and are hence isomorphic by the second isomorphism theorem. Since D_4 is a subgroup of S_4 of size 8, this implies the Galois group is in fact isomorphic to D_4 as required.

Credit for some of this reasoning is attributed to this stack exchange post. Initially I had calculated the Galois group of $x^4 - 2$ by hand and consulted this post to check my answer, but it provided a much cleaner way of concluding the same result.

b) The cyclic group C_4.

By Assignment 3 Problem 3, we know that $\mathbb{Q}[\zeta_5]$ has the Galois group C_4. Hence, $x^4 + x^3 + x^2 + x + 1$, the minimum polynomial of ζ_5, has this Galois group.

Isomorphic by Sylow's second theorem (all Sylow p-groups are conjugate).

5. Problem 5

Let $\zeta = \zeta_7$. I want to show that $\zeta + \zeta^2 + \zeta^4 = -\frac{1}{2} + \frac{\sqrt{-7}}{2}$ by evaluating $(2(\zeta + \zeta^2 + \zeta^4) + 1)^2$:

$$\begin{aligned}(2(\zeta + \zeta^2 + \zeta^4) + 1)^2 &= 4(\zeta + \zeta^2 + \zeta^4)^2 + 4(\zeta + \zeta^2 + \zeta^4) + 1 \\ &= 4\begin{pmatrix} \zeta^2 + \zeta^3 + \zeta^5 \\ +\zeta^3 + \zeta^4 + \zeta^6 \\ +\zeta^5 + \zeta^6 + \zeta^8 \end{pmatrix} + 4(\zeta + \zeta^2 + \zeta^4) + 1 \\ &= 8(\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) + 1 \\ &= -7\end{aligned}$$

1 Correct

The value of $\zeta + \zeta^2 + \zeta^4$ itself is not so important; once you have calculated

$$(2(\zeta + \zeta^2 + \zeta^4) + 1)^2 = \dots$$

Expand

Since

$$\zeta^6 + \dots + \zeta + 1 = 0$$

via the minimal polynomial of ζ.