412 Individual HW9

Jack Madden

April 2024

Problem 1

The problem is similar to problem 6 from the previous homework. We find using the quadratic formula and the substitution $y = x^2$ that the roots of this polynomial are $\pm\sqrt{5 \pm 2\sqrt{6}}$. Let us show that this polynomial is irreducible in $\mathbb{Z}$, and therefore $\mathbb{Q}$ Assuming that the quartic could be factored into two quadratics $(x^2 + bx + c)(x^2 + dx + e)$, yields the following system:

$$b + d = 0$$

$$c + e + bd = 0$$

$$ce = 1$$

This system allows us to arrive at the contradiction $b = \sqrt{2}, \sqrt{2}i$. Thus the polynomial is irreducible. Also, we have that $\sqrt{5+2\sqrt{6}}\sqrt{5-2\sqrt{6}} = 1$ and hence $\mathbb{Q}(\sqrt{5+2\sqrt{6}}) = \mathbb{Q}(\sqrt{5-2\sqrt{6}})$ and thus $\mathbb{Q}(\sqrt{5+2\sqrt{6}})$ is the splitting field of this polynomial. Thus, since the degree of this extension is 4, we have that $|Gal(\mathbb{Q}(\sqrt{5-2\sqrt{6}})/\mathbb{Q})| = 4$, and therefore it is either V_4 or $\mathbb{Z}_4$. Consider the 4 maps in $Gal(\mathbb{Q}(\sqrt{5-2\sqrt{6}})/\mathbb{Q})$

$$Id : \sqrt{5+2\sqrt{6}} \to \sqrt{5+2\sqrt{6}}$$

$$\sigma_1 : \sqrt{5+2\sqrt{6}} \to -\sqrt{5+2\sqrt{6}}$$

$$\sigma_2 : \sqrt{5+2\sqrt{6}} \to \sqrt{5-2\sqrt{6}}$$

$$\sigma_3 : \sqrt{5+2\sqrt{6}} \to -\sqrt{5-2\sqrt{6}}$$

We first have:

$$\sigma_1^2\left(\sqrt{5+2\sqrt{6}}\right) = \sigma_1\left(-\sqrt{5+2\sqrt{6}}\right) = \sigma_1(-1)\sigma_1\left(\sqrt{5+2\sqrt{6}}\right) = \sqrt{5+2\sqrt{6}} = Id(\sqrt{5+2\sqrt{6}})$$

Due to the relations $\sqrt{5+2\sqrt{6}}\sqrt{5-2\sqrt{6}} = 1, (-\sqrt{5+2\sqrt{6}})(-\sqrt{5-2\sqrt{6}}) = 1$, we observe that:

$$\sigma_2^2\left(sqrt5+2\sqrt{6}\right) = \sigma_2(\sqrt{5-2\sqrt{6}}) = \frac{\sigma_2(1)}{\sigma_2(\sqrt{5+2\sqrt{6}})} = \frac{1}{\sqrt{5-2\sqrt{6}}} = \sqrt{5+2\sqrt{6}} = Id(\sqrt{5}+2\sqrt{6})$$

Hence, since we have at least 2 elements of order 2, this is the Klein 4 group, and it is generated by σ_1, σ_2, as it can be computed that $\sigma_1 \circ \sigma_2 = \sigma_3$.

Problem 2

$f(x) = x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, since neither $x = 0, 1$ is a root. Therefore, we by Kronecker's theorem, we have that $\mathbb{Z}_2[x]/f(x) \cong \mathbb{Z}_2(\alpha)$ for α such that $f(\alpha) = 0$. We claim that $\mathbb{Z}_2(\alpha)$ is a splitting field. Notice that the elements of $\mathbb{Z}_2$ are of the form $a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Z}_2$. By the fact that $f(\alpha) = \alpha^3 + \alpha + 1 = 0$ we obtain the relation $\alpha^3 = \alpha + 1$. Thus, we find that:

$$f(\alpha^2+\alpha) = (\alpha^2+\alpha)^3 = (\alpha^4+\alpha^2)(\alpha^2+\alpha)+\alpha^2+\alpha+1 = (\alpha(\alpha+1)+\alpha^2)(\alpha^2+\alpha)+\alpha^2+\alpha+1 =$$

$$\alpha(\alpha^2+\alpha)+\alpha^2+\alpha+1 = \alpha+1+\alpha^2+\alpha^2+\alpha+1 = 0$$

Also:

$$f(\alpha^2) = (\alpha^2)^3+\alpha^2+1 = \alpha^3\alpha^3+\alpha^2+1 = (\alpha+1)(\alpha+1)+\alpha^2+1 = \alpha^2+1+\alpha^2+1 = 0$$

We claim that since this extension is degree 3, by transitivity of degree since 3 is prime, there can be no smaller field containing these roots. Since $\mathbb{Z}_2(\alpha) \cong \mathbb{F}_{2^3}$, $\mathbb{Z}_2(\alpha)/\mathbb{Z}_2$ is Galois and from the previous homework we have that $Gal(\mathbb{Z}_{2^3}/\mathbb{Z}) \cong \mathbb{Z}_3$.

Problem 3

We know that by the Galois Correspondence, L corresponds to the group $G(K/L) \subset G(K/F)$. Suppose that some $\alpha \in L$, and call $f = irr(\alpha, F)$. We can show that L/F is Galois, by showing that any β such that $f(\beta) = 0$ must be in L. This is equivalent to showing that for any $\sigma \in G(K/L)$, $\sigma(\beta) = \beta$. We proceed using contradiction. Suppose there exists some β conjugate to α, $\sigma \in G(K/L)$ such that $\sigma(\beta) = \gamma \neq \beta$. Consider the isomorphism τ between $F(\alpha)$ and $F(\beta)$ over F such that $\tau(\alpha) = \beta$. Since K/F is Galois, this can be extended to an automorphism $\tau' \in G(K/F)$. Since we have that $G(K/F)$ is Abelian, and $\tau', \sigma, \in G(K/F)$

$$\sigma(\tau'(\alpha)) = \tau'(\sigma(\alpha))$$

$$\gamma = \sigma(\beta) \neq \tau'(\alpha) = \beta$$

but this is a contradiction. Thus, $\beta \in L$ and L/F is Galois.
The shorter proof is that any subgroup of an Abelian group will be normal, and normal subgroups correspond to normal extensions and as we have not addressed separability in the class these are Galois extensions. This felt too immediate for me so I gave the previous proof.

Problem 4

Problem 5

a) We can solve this problem using Vieta's formulas:

$$(x_1+x_2+x_3)^2 = x_1^2+x_2^2+x_3^2+2(x_1x_2+x_1x_3+x_2x_3)$$

Observe that $x_1x_2+x_1x_3+x_2x_3 = -6$ and $x_1+x_2+x_3 = 0$ by Vieta's formulas. Hence, $x_1^2+x_2^2+x_3^2 = 12$.

b) We can again solve this problem using Vieta's formula:

$$\frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3} = \frac{x_1x_2+x_1x_3+x_2x_3}{x_1x_2x_3}$$

By Vieta's formulas we have $x_1x_2+x_1x_3+x_2x_3 = -6$ and $x_1x_2x_3 = 7$. Hence this quantity is $-\frac{6}{7}$.

c) Given that $x_1+x_2+x_3 = 0$, we have that:

$$\frac{x_1}{x_2}+\frac{x_2}{x_1}+\frac{x_1}{x_3}+\frac{x_3}{x_1}+\frac{x_2}{x_3}+\frac{x_3}{x_2} = \frac{x_1+x_2}{x_3}+\frac{x_1+x_3}{x_2}+\frac{x_2+x_3}{x_1} = \frac{-x_3}{x_3}+\frac{-x_2}{x_2}+\frac{-x_1}{x_1} = -1+-1+-1 = 3$$

Problem 6

a) We have that:

$$L_1L_2 = (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)$$

$$L_1L_2 = \alpha_1^2 + \omega^2\alpha_1\alpha_2 + \omega\alpha_1\alpha_3 + \omega\alpha_1\alpha_2 + \alpha_2^2 + \omega^2\alpha_2\alpha_3 + \omega^2\alpha_1\alpha_3 + \omega\alpha_2\alpha_3 + \alpha_3^2$$

Simplifying:

$$L_1L_2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \omega(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + \omega^2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$$

Using $\omega + \omega^2 + 1 = 0$ gives $\omega + \omega^2 = -1$

$$L_1L_2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$$

From 5a,

$$L_1L_2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)$$

Applying Vieta gives:

$$L_1L_2 = -3p$$

b) Computation gives:

$$(L_1 + L_2)^3 = L_1^3 + 3L_1^2L_2 + 3L_1L_2^3 + L_2^3$$

$$(L_1 + L_2)^3 - 3L_1(-3p) - 3L_2(-3p) = L_1^3 + L_2^3$$

$$(\alpha_1 - \alpha_2 - \alpha_3)^3 - 3L_1(-3p) - 3L_2(-3p) = L_1^3 + L_2^3$$

$$(2\alpha_1)^3 + 9p(L_1 + L_2) = L_1^3 + L_2^3$$

$$(2\alpha_1)^3 + 9p(2\alpha_1 - \alpha_2 - \alpha_3) = L_1^3 + L_2^3$$

$$(2\alpha_1)^3 + 27p(\alpha_1) = L_1^3 + L_2^3$$

$$8\alpha_1^3 + 27p\alpha_1 = L_1^3 + L_2^3$$