Homework

Frederick Robinson

24 May 2010

1 Chapter 14 Section 4

1.1 Problem 1

1.1.1 Question

Determine the Galois closure of the field $\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$ over $\mathbb{Q}$.

1.1.2 Answer

The Galois closure is merely the splitting field for the minimal polynomial of $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$. The minimal polynomial is just $f(x) = (x^2-1)^2 - 2 = x^4 - 2x^2 - 1$. So, since the roots of this polynomial are

$$x = -i\sqrt{-1+\sqrt{2}} \quad x = i\sqrt{-1+\sqrt{2}} \quad x = -\sqrt{1+\sqrt{2}} \quad x = \sqrt{1+\sqrt{2}}$$

the splitting field (and therefore the Galois closure) is just $\mathbb{Q}(i, \sqrt{1+\sqrt{2}})$

1.2 Problem 2

1.2.1 Question

Find a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

1.2.2 Answer

A primitive generator for the given extension is $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$.

Proof. This is a member of the given extension, so clearly $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Moreover, α is not fixed by any of the 8 Galois automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and therefore $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\alpha)$ which gives us equality, as claimed. $\square$

1.3 Problem 3

1.3.1 Question

Let F be a field contained in the ring of $n \times n$ matrices over $\mathbb{Q}$. Prove that $[F : \mathbb{Q}] \leqslant n$. (Note that, by Exercise 19 of Section 13.2, the ring of $n \times n$ matrices over $\mathbb{Q}$ does contain fields of degree n over $\mathbb{Q}$.)

1.3.2 Answer

Proof. As $\mathbb{Q}$ is of characteristic 0, F is a simple extension over $\mathbb{Q}$ and $F = \mathbb{Q}(\theta)$ for some primitive element θ. Let $m(x)$ be the minimal polynomial of θ over $\mathbb{Q}$ and note that $[F : \mathbb{Q}] = \deg m(x)$.

Since θ is an $n \times n$ matrix, its characteristic polynomial $f(x)$ is of degree n, and $f(\theta) = 0$. So $\deg m(x) = [F : \mathbb{Q}] \leqslant n$, and $f(\theta) = 0$. So $\deg m(x) = [F : \mathbb{Q}] \leqslant n$, or else there would be a polynoimal of lesser degree $(f(x))$ which had θ as a root. □

2 Chapter 14 Section 5

2.1 Problem 1

2.1.1 Question

Determine the minimal polynomials satisfied by the primitive generators given in the text for the subfields of $\mathbb{Q}(\zeta_{13})$

2.1.2 Answer

One can easily verify that the minimal polynomials are (in order of degree)

Generator	Polynomial
ζ	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$
	$+x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12}$
$\zeta + \zeta^{-1}$	$-1 + 3x + 6x^2 - 4x^3 - 5x^4 + x^5 + x^6$
$\zeta + \zeta^3 + \zeta^9$	$3 - 4x + 2x^2 + x^3 + x^4$
$\zeta + \zeta^5 + \zeta^8 + \zeta^{12}$	$1 - 4x + x^2 + x^3$
$\zeta + \zeta^3 + \zeta^4 + \zeta^9 + \zeta^{10} + \zeta^{12}$	$-3 + x + x^2$

2.2 Problem 3

2.2.1 Question

Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5^{th} root of unity ζ_5. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicitly solve for the 5^{th} root of unity.

2.2.2 Answer

It is easy to check that α satisfies the quadratic x^2+x-1 and that the quadratic $x^2-\alpha x+1$ is satisfied by ζ_5. Now, by the quadratic equation we have one of

$$\alpha = \frac{-1 \pm \sqrt{1+4}}{2}.$$

However, since α is positive (ζ_5 and ζ_5^{-1} both have positive real part) we must have in particular that

$$\alpha = \frac{-1+\sqrt{5}}{2}.$$

By the quadratic equation again we get one of

$$\zeta_5 = \frac{\alpha \pm \sqrt{\alpha^2-4}}{2}.$$

Since the imaginary component of ζ_5 is positive we know that

$$\zeta_5 = \frac{\alpha + \sqrt{\alpha^2-4}}{2}.$$

Substituting, expanding we have

$$\zeta_5 = -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{2} i \sqrt{4 - \frac{1}{4}\left(-1+\sqrt{5}\right)^2}.$$

2.3 Problem 5

2.3.1 Question

Let p be a prime and let $\epsilon_1, \epsilon_2, \ldots, \epsilon_{p-1}$ denote the primitive p^{th} roots of unity. Set $p_n = \epsilon_1^n + \epsilon_2^n + \cdots + \epsilon_{p-1}^n$, the sum of the n^{th} powers of the ϵ_i. Prove that $p_n = -1$ if p does not divide n and that $p_n = p-1$ if p does divide n. [One approach: $p_1 = -1$ from $\Phi_p(x)$; show that p_n is a Galois conjugate of p_1 for p not dividing n, hence is also -1.]

2.3.2 Answer

Proof. Since $\Phi_p = x^{p-1} + x^{p-2} + \cdots + 1$ we have $\Phi(\zeta_p) = 0 = p_1 + 1 \Rightarrow p_1 = -1$. The members of the cyclotomic Galois group are defined by $\sigma_a(\zeta_p) = \zeta_p^a$ with p not dividing a. Thus, $\sigma_a(p_1) = p_a$ and so for p not dividing a we have $p_a = -1$ as well.

If p does divide a then $\epsilon_i^a = (\epsilon_i^p)^m = 1^m = 1 \Rightarrow p_a = p-1$. □

2.4 Problem 7

2.4.1 Question

Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of n^{th} roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n +$

ζ_n^{-1}) is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the *maximal real subfield of K.*

2.4.2 Answer

The complex conjugate of a root of unity ζ_n is just ζ_{-n}. Therefore, σ_{-1} takes members of $\mathbb{Q}(\zeta_n)$ to their complex conjugates.

An element of some field is real if and only if it is fixed by complex conjugation. Thus, in particular, the subfield of all real elements of $\mathbb{Q}(\zeta_n)$ is precisely that subfield which is fixed by complex conjugation, or equivalently, by σ_{-1}. So, K^+ is the subfield which is fixed by the subgroup of the Galois group $H = \{\sigma_{-1}, 1\}$.

One such element is $\zeta_n + \zeta_n^{-1} = \alpha$. Now, observe that for every automorphism $\sigma_a \notin H$ we have $\sigma_a(\alpha) = \zeta_n^a + \zeta_n^{-a} \neq \alpha$ (This lack of equality follows from the fact that the real part of such a power of ζ_n is not the same as the real part of ζ_n). Hence, α generates the entire fixed field.

2.5 Problem 12

2.5.1 Question

Let σ_p denote the Frobenius automorphism $x \mapsto x^p$ of the finite field $\mathbb{F}_q$ of $q = p^n$ elements. Viewing $\mathbb{F}_q$ as a vector space V of dimension n over $\mathbb{F}_p$ we can consider σ_p as a linear transformation of V to V. Determine the characteristic polynomial of σ_p and prove that the linear transformation σ_p is diagonalizable over $\mathbb{F}_p$ if and only if n divides $p-1$, and is diagonalizable over the algebraic closure of $\mathbb{F}_p$ if and only if $(n,p) = 1$.

2.5.2 Answer

Since for all $x \in \mathbb{F}_{p^n}$, $x^{p^n} - x = 0$ we have that σ_p satisfies $x^n - 1$. Since this is a degree n polynomial it is the characteristic polynomial.

Recall that σ_p is diagonalizable if and only if the characteristic polynomial splits completely in $\mathbb{F}_p$.

Proof. Observe that σ_p is diagonalizable if and only if $\mathbb{F}_p$ contains all the nth roots of unity, if and only if $\mathbb{F}_p^\times$ contains a copy of $\mathbb{Z}/n\mathbb{Z}$. By fundamental theorem of cyclic groups this is the case if and only if $n|(p-1)$.

The linear transformation is diagonalizable over the closure of $\mathbb{F}_p$ if and only if $x^n - 1$ is separable. This is true if and only if it is relatively prime to the derivative nx^{n-1} but this is in turn true if and only if $nx^{n-1} \neq 0 \Leftrightarrow p \nmid n$. $\square$