Math 121, Winter 2023, Homework 6 Solutions

Section 14.4

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

Solution. $\alpha := \sqrt{1+\sqrt{2}}$ is a root of the polynomial $f(x) = x^4 - 2x^2 - 1$. This is irreducible since $f(x+1) = x^4 + 4x^3 + 4x^2 - 2$, which is irreducible by Eisenstein's criterion with prime 2.

f has roots $\pm\alpha$ and $\pm\beta$ where $\beta = \sqrt{1-\sqrt{2}}$. By Theorem 13, since f is separable, an extension field K of $\mathbb{Q}(\alpha)$ is Galois if and only if it is the splitting field for f. Therefore the Galois closure of $\mathbb{Q}(\alpha)$ is $L := \mathbb{Q}(\alpha, \beta)$, but this is not a particularly nice way of writing the extension.

Since $\mathbb{Q}(\alpha) \subset \mathbb{R}$ and $\beta \notin \mathbb{R}$, $\mathbb{Q}(\alpha)$ is strictly contained in L. Now, $\alpha^2\beta^2 = (1+\sqrt{2})(1-\sqrt{2}) = -1$, so $\beta = \frac{\sqrt{-1}}{\alpha^2}$, and so $L = \mathbb{Q}(\alpha, i)$.

Problem 3. *Let F be a field contained in the ring of $n \times n$ matrices over $\mathbb{Q}$. Prove that* $[F : \mathbb{Q}] \leq n$.

Solution. (Note that $\mathbb{Q}$ is a subset of $n \times n$ matrices by identifying $q \in \mathbb{Q}$ with the diagonal matrix with all diagonal entries equal to q.)

Since char $F = 0$, the primitive element theorem tells us that $F = \mathbb{Q}(\alpha)$ for some element $\alpha \in F$. Let $f(x)$ be the characteristic polynomial for the matrix α. Then $\deg f = n$, and $f(\alpha) = 0$ by the Cayley-Hamilton theorem. Therefore, $[F : \mathbb{Q}] = \deg \alpha \leq \deg f = n$.

Section 14.5

Problem 3. *Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5th 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 5th root of unity.*

Solution. Let $\zeta := \zeta_5$. $\alpha^2 = \zeta^2 + \zeta^{-2} + 2 = 1 - \zeta - \zeta^{-1} = 1 - \alpha$ since the sum of all nth roots of unity is zero. Therefore, α is a root of the polynomial $x^2 + x - 1 \in \mathbb{Q}[x]$, and using the quadratic formula, $\alpha = \frac{-1\pm\sqrt{5}}{2}$

As is true for all n, ζ and ζ^{-1} are the roots of the polynomial $x^2 - \alpha x + 1 \in \mathbb{Q}(\alpha)[x]$, since the sum of ζ and ζ^{-1} is α, and their product is 1. Therefore, using the quadratic formula gives

$$\zeta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} = \frac{\frac{-1\pm\sqrt{5}}{2} \pm \sqrt{(\frac{-1\pm\sqrt{5}}{2})^2 - 4}}{2} = \frac{-1 \pm \sqrt{5} \pm \sqrt{-10 \mp 2\sqrt{5}}}{4}.$$

Here, the first $\pm$ and the $\mp$ must have opposite signs, and the two choices from this, plus the two choices from the second $\pm$, give all four primitive 5th roots of unity.

Problem 7. *Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of nth roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the maximal real subfield of K.*

Solution. Let $\zeta := \zeta_n$ Since $|\zeta| = 1$, $\overline{\zeta} = \zeta^{-1}$. Since ζ is primitive over $\mathbb{Q}$, by the lemma in the previous homework solutions there exists an automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ sending $\zeta \mapsto \zeta^{-1}$, and this determines σ_{-1}. This means that complex conjugation restricted to $\mathbb{Q}(\zeta)$ must equal σ_{-1}, since they match on $\mathbb{Q}$ and ζ.

Now, $\zeta + \zeta^{-1} = \zeta + \overline{\zeta} = 2\mathrm{Re}\,\zeta \in \mathbb{R}$, so $K^+ = \mathbb{Q}(\zeta + \zeta^{-1}) \subset \mathbb{R}$. On the other hand, $[K : K^+] = 2$ since ζ is a root of the polynomial $x^2 - (\zeta + \zeta^{-1})x + 1$, so there is no intermediate field strictly between K^+ and K. Since $K \not\subseteq \mathbb{R}$, K^+ is the maximal subfield of K, contained in $\mathbb{R}$, so it must equal the field $K \cap \mathbb{R}$ of all real elements of K.

Problem 10. *Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.*

Solution. Since $\mathbb{Q}(\sqrt[3]{2})$ has one, but not all of the roots of the separable polynomial $x^3 - 2$, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

By Theorem 26, every cyclotomic field over $\mathbb{Q}$ is an abelian (Galois) extension of $\mathbb{Q}$, and since every subgroup of an abelian group is normal, by the Fundamental Theorem of Galois theory, every subfield of a cyclotomic field is a Galois (and abelian) extension of $\mathbb{Q}$.

Section 14.6

Problem 2a. *Determine the Galois group of the polynomial $f(x) = x^3 - x^2 - 4$*

Solution. It turns out $f(x) = (x-2)(x^2+x+2)$ is reducible (should probably have checked for that before I assigned this problem...), so the Galois group of f is the same as the Galois group of $g(x) = x^2 + x + 2$. Now, g is irreducible by Eisenstein's criterion with the prime 2, which means that the splitting field of g and therefore g is a degree 2 extension of $\mathbb{Q}$, and therefore the Galois group is the only group of order 2, $\mathbb{Z}/2\mathbb{Z}$.

For good measure, we compute the discriminant of g, which is $D = -7$. Since $\sqrt{D} = \sqrt{-7} \notin \mathbb{Q}$, this means that the Galois group of g is not contained in $A_2 = 1$, so must equal $S_2 = \mathbb{Z}/2\mathbb{Z}$.

Problem 22. *Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \dots, \alpha_n$. Let s_i be the elementary symmetric function of degree i in the roots and define $s_i = 0$ for $i > n$. Let $p_i = \alpha_1^i + \cdots + \alpha_n^i, i \geq 0$, be the sum of the ith powers of the roots of $f(x)$ Prove Newton's formulas:*

$$p_n - s_1 p_{n-1} + s_2 p_{n-2} + \cdots + (-1)^{n-1} s_{n-1} p_1 + (-1)^n \cdot n s_n = 0.$$

.

Solution. [See solution to extra problem below first.] Multiply the desired equation by $(-1)^n$ and move everything but the last term onto the opposite side of the equation. This becomes

$$n s_n = \sum_{r=1}^{n} (-1)^{r-1} p_r s_{n-r}. \tag{1}$$

The right side of (1) is the coefficient of t^{n-1} in $P(-t)E(t)$since

$$P(-t)E(t) = \sum_{r=0}^{\infty} p_r (-t)^{r-1} \sum_{m=0}^{\infty} s_m t^m = \sum_{r,m \geq 0} (-1)^{r-1} p_r s_m t^{r-1+m} = \sum_{n \geq 0} \left(\sum_{r \geq 0} (-1)^{r-1} p_r s_{n-r} \right) t^{n-1}.$$

On the other hand, using the extra problem below, we have

$$\begin{aligned}
\frac{d}{dt} \ln E(t) &= \frac{d}{dt} \ln \prod_{i=1}^{n} (1 + x_i t) \\
&= \sum_{i=1}^{n} \frac{d}{dt} \ln(1 + x_i t) \\
&= \sum_{i=1}^{n} \frac{d}{dt} \left(-\ln \frac{1}{1 + x_i t} \right) \\
&= \sum_{i=1}^{n} \frac{d}{d(-t)} \left(\ln \frac{1}{1 + x_i t} \right) = P(-t).
\end{aligned}$$

Using the chain rule,

$$P(-t) = \frac{d}{dt} \ln E(t) = \frac{E'(t)}{E(t)},$$

so

$$P(-t)E(t) = E'(t) = \sum_{n=0}^{\infty} n s_n t^{n-1},$$

and the coefficient of t^{n-1} is the left side of (1)

Extra Problem. *Let* $p_k(x_1, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$. *Let*

$$E(t) = \sum_{r=0}^{\infty} s_r(x_1, \ldots, x_n) t^r, \qquad P(t) = \sum_{r=1}^{\infty} p_r(x_1, \ldots, x_n) t^{r-1}.$$

Prove that

$$E(t) = \prod_{i=1}^{n} (1 + x_i t), \qquad P(t) = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t} = \sum_{i=1}^{n} \frac{d}{dt} \ln \frac{1}{1 - x_i t}.$$

Solution. We won't worry much about convergence here, but notice that if $x_1, \ldots, x_n \in \mathbb{C}$ since there are finitely many x_i, we may choose some $t \in \mathbb{C}, t \neq 0$ such that $|tx_i| < 1$ for all i. Therefore, all the relevant series converge.

First, the elementary symmetric functions. We have

$$\begin{aligned} E(t) &= \sum_{r=0}^{\infty} s_r(x_1, \ldots, x_n) t^r \\ &= \sum_{r=0}^{\infty} \sum_{i_1 < \ldots < i_r} x_{i_1} \cdots x_{i_r} t^r \\ &= \sum_{r=0}^{\infty} \sum_{i_1 < \ldots < i_r} (x_{i_1} t) \cdots (x_{i_r} t) \\ &= \sum_{I \subseteq \{1,2,\ldots,n\}} \prod_{i \in I} x_i t. \end{aligned}$$

Expanding the product $\prod_{i=1}^{n} (1 + x_i t)$ using the distributive law gives the same expression; the term $\prod_{i \in I} x_i t$ corresponds to choosing $x_i t$ from the factor $1 + x_i t$ when $i \in I$, and choosing 1 when $i \notin I$.

Next, the power sum symmetric functions. We have

$$P(t) = \sum_{r=1}^{\infty} p_r(x_1, \ldots, x_n) t^{r-1} = \sum_{r=1}^{\infty} \sum_{i=1}^{n} x_i^r t^{r-1} = \sum_{i=1}^{n} \sum_{r=1}^{\infty} x_i^r t^{r-1} = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t},$$

summing the geometric series in the last step. For the second equality, using the chain rule,

$$\frac{d}{dt}\ln\frac{1}{1-x_it} = -\frac{d}{dt}\ln(1-x_it) = \frac{x_i}{1-x_it}.$$