MATH 6140 HOMEWORK 12

COLTON GRAINGER
APRIL 16, 2019

1. 14.2.1. The minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2}+\sqrt{5}$ is $x^4 - 14x^2 + 9$.

Proof. Noting that $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ is a subfield of the Galois extension $\mathbb{Q}(\sqrt{2},\sqrt{5})$, it suffices to find the monic polynomial $m(x) \in \mathbb{Q}[x]$ of minimal degree such that $\mathbb{Q}[x]/\langle m(x)\rangle$ contains the four elements $\sqrt{2} \pm \sqrt{5}$ and $\pm\sqrt{2}+\sqrt{5}$. (These elements are the *distinct* conjugate pairs of $\sqrt{2}+\sqrt{5}$, and the Galois group $\operatorname{Gal}\left\{\mathbb{Q}(\sqrt{2}+\sqrt{5})\right\}$ necessarily permutes the conjugate elements.) Consider then the product

$$\prod_{\text{conjugates}} \left(x - \left(\pm\sqrt{2} \pm \sqrt{5}\right)\right) = \left(x^2 - \left(2 + 2\sqrt{10} + 5\right)\right)\left(x^2 - \left(2 - 2\sqrt{10} + 5\right)\right) \tag{1.1}$$

$$= x^4 - 14x^2 - 9. \tag{1.2}$$

We conclude $m(x) = x^4 - 14x^2 - 9$ is minimal, because any product of 3 or fewer linear factors in (1.1) is not a polynomial in $\mathbb{Q}[x]$. ∎

2. 14.2.4. Let p be an odd[1] prime. Then the Galois group of $x^p - 2$ over $\mathbb{Q}$ is the semidirect product of cyclic groups

$$\operatorname{Gal}\left(\mathbb{Q}\left(\zeta, \sqrt[p]{2}\right)/\mathbb{Q}\right) \cong C_p \rtimes_\psi C_{p-1}$$

where ζ is a primitive pth root of unity, $\sqrt[p]{2}$ is the real pth root of 2, and $\psi\colon C_{p-1} \xrightarrow{\cong} \operatorname{Aut} C_p$ is an isomorphism from C_{p-1} to the $p-1$ automorphisms of C_p.

Proof. Because $\operatorname{chr}\mathbb{Q} = 0$, the polynomial $x^p - 2$ is separable, with roots

$$\left\{\zeta^k \sqrt[p]{2} \quad \text{such that} \quad 0 \le k \le p-1\right\} \subset \mathbb{C}.$$

We see the splitting field of $x^p - 2$ is generated by $\zeta, \sqrt[p]{2} \in S$. Hence the extension $F = \mathbb{Q}\left(\zeta, \sqrt[p]{2}\right)/\mathbb{Q}$ is the splitting field of a separable polynomial, and so F is Galois. To see that $[F : \mathbb{Q}] = (p-1)p$, note p and $p-1$ are coprime, and recall the (partial) Hasse diagram:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[p]{2}, \zeta) \arrow[dl, dash, "p-1"'] \arrow[dr, dash, "p"] & \\
\mathbb{Q}(\sqrt[p]{2}) \arrow[dr, dash, "p"'] & & \mathbb{Q}(\zeta) \arrow[dl, dash, "p-1"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Now, the Galois group is determined by its action on the (fixed) generators $\sqrt[p]{2}, \zeta$, which gives the possibilities

$$\zeta \longmapsto \zeta^k, \qquad k = 1, \ldots, p-1, \tag{2.1}$$

$$\sqrt[p]{2} \longmapsto \zeta^\ell \sqrt[p]{2}, \qquad \ell = 0, \ldots, p-1. \tag{2.2}$$

[1]The case $p = 2$ with $x^2 - 2$ has Galois group C_2 and automorphisms $\sqrt{2} \mapsto \pm\sqrt{2}$.

By order considerations, as the degree of $F/\mathbb{Q}$ is $p(p-1)$, the automorphisms in (2.1) form a complete list. Now let m be an integer $1 < m < p-1$ that is coprime to $p-1$ (we need a generator for the cyclic group of order $p-1$). Then define $\sigma, \tau \in \operatorname{Gal}(F/\mathbb{Q})$ by

$$\sigma = \begin{cases} \zeta \mapsto \zeta^m \\ \sqrt[p]{2} \mapsto \sqrt[p]{2} \end{cases} \qquad \text{and} \quad \tau = \begin{cases} \zeta \mapsto \zeta \\ \sqrt[p]{2} \mapsto \zeta \sqrt[p]{2} \end{cases} .$$

Because p is prime and $\operatorname{ord} \zeta = p$, it is visible that $\operatorname{ord} \tau = p$. We deduce that $\operatorname{ord} \sigma = p - 1$ from both $(m, p-1) = 1$ and the fact that "$\sigma \in \operatorname{Aut} \langle \zeta \rangle \cong C_{p-1}$" is a cyclic group.

Moreover, as σ and τ have coprime orders, by Lagrange's theorem, they generate the Galois group. We conclude that, as a set, $\operatorname{Gal}(F/\mathbb{Q}) = \langle \tau \rangle \times \langle \sigma \rangle = C_p \times C_{p-1}$. The group structure $\operatorname{Gal}(F/\mathbb{Q}) \cong C_p \rtimes_\psi C_{p-1}$ follows from the isomorphism $\psi \colon \langle \sigma \rangle \to \langle \tau \rangle$ defined by

$$\psi(\sigma).\tau = \sigma^{-1} \tau \sigma.$$

□

3. 14.2.5. The Galois group $\operatorname{Gal}(F/\mathbb{Q})$ of $x^p - 2$ (as in problem 2) is isomorphic to the matrix group

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \quad \text{given} \quad a, b \in \mathbb{F}_p \quad \text{and} \quad a \neq 0 \right\}.$$

Proof. Fix a, a generator of the group of units $\mathbb{F}_p^\times$, and define a group homomorphism $f \colon \operatorname{Gal}(F/\mathbb{Q}) \to H$ by

$$\sigma \underset{f}{\longmapsto} \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \tau \underset{f}{\longmapsto} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Because H has order $p(p-1)$ and f is surjective (by choice of generator a), we have a surjective homomorphism between finite groups, and thus an isomorphism. □

4. 14.2.8. Suppose K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. There are Galois extensions of F contained in K of degrees p and p^{n-1}.

5. 14.2.11. Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group S_4 over $\mathbb{Q}$. Let θ be a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Then K is an extension of Q of degree 4 which has no proper subfields. We determine if there are any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields.

6. 14.2.13. If the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3, then all the roots of the cubic are real.

7. 14.3.1. The factors of $x^8 - x$ as irreducibles in $\mathbb{Z}[x]$ and $\mathbb{F}_2[x]$, respectively, are:

8. 14.3.3. An algebraically closed field is infinite.

9. 14.3.7.

(a) One of 2, 3, or 6 is a square in $\mathbb{F}_p$ for every prime p.

(b) Therefore, for every prime p, the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = \big(x^2 - 2\big)\big(x^2 - 3\big)\big(x^2 - 6\big) \tag{9.1}$$

has a root modulo p.

(c) However, the polynomial (9.1) is irreducible over $\mathbb{Z}$.

10. 14.3.8. We exhibit an *Artin–Schreier extension.*

(a) The splitting field E of the polynomial $x^p - x - a$ over $\mathbb{F}_p$, where $a \neq 0$ and $a \in \mathbb{F}_p$, is:

(b) For a root α of $x^p - x - a$, the map $\alpha \mapsto \alpha + 1$ induces an automorphism of E fixing $\mathbb{F}_p$.

(c) Therefore, the Galois group of $x^p - x - a$ over $\mathbb{F}_p$ is cyclic.

11. 14.3.9. Let $q = p^m$ be a power of the prime p and let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Then let $\sigma_q = \sigma_p^m$ be the mth power of the Froebenius automorphism σ_p, called the *q-Froebenius automorphism.*

(a) The q-Froebenius automorphism σ_q fixes $\mathbb{F}_q$.

(b) Every finite extension of $\mathbb{F}_q$ of degree n is the splitting field K of $x^{q^n} - x$ over $\mathbb{F}_q$, hence unique.

(c) For $K/\mathbb{F}_q$ the unique degree n extension of $\mathbb{F}_q$, we have

$$\operatorname{Gal}(K/\mathbb{F}_q) = \langle \sigma_q \rangle .$$

(d) Hence, there's a bijective correspondence

$$\left\{ \begin{matrix} \text{subfields } E \\ K \geq E \geq F \end{matrix} \right\} \leftrightsquigarrow \left\{ \begin{matrix} \text{divisors } d \\ 1 \mid d \mid n \end{matrix} \right\}.$$

12. 14.3.10. Let φ be the Euler totient function, p a prime, and n a natural number. Then

$$n \quad \text{divides} \quad \varphi(p^n - 1).$$

Proof. Observe that $\varphi(p^n - 1)$ is the order of the group of automorphisms of a cyclic group of order $p^n - 1$. $\square$