MATH 6140 HOMEWORK 12

COLTON GRAINGER
APRIL 15, 2019

1. 14.2.1. The minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2}+\sqrt{5}$ is:

2. 14.2.4. Let p be a prime. The elements of the Galois group of x^p-2 over $\mathbb{Q}$ are:

3. 14.2.5. The Galois group of x^p-2 (as in problem 2) is isomorphic to the matrix group

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

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

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

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

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

(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 $p^n - 1$. □