HOMEWORK, DUE FRIDAY MARCH 17TH

1. Let $K = \mathbb{F}_p$ and $L = \overline{\mathbb{F}}_p$. Describe the lattice of inclusions of all intermediary fields.
2. Suppose we want to describe the field extension $L = \mathbb{F}_{27}/\mathbb{F}_3 = K$. One way to do this, the best way in fact, is simply to say that this is a splitting field for $x^{27} - x$. However if we use this method, we don't see how to explicitly add and multiply elements of L.
(a) Let L/K be a splitting field for any irreducible cubic $f(x) \in \mathbb{F}_3[x]$. Show that $L \simeq \mathbb{F}_{27}$.
(b) Let α be a root of $f(x)$. Show that $L = K(\alpha)$.
(c) Now write down an explicit such polynomial $f(x)$.
(d) Describe the additive and multiplicative structure of L/K in terms of α and $f(x)$.
(e) Show how to compute inverses in L.
3. Let $L = K(x)$, where x is an indeterminate. Let $\alpha = f(x)/g(x)$ and let $M = K(\alpha)$. Recall that L/M is algebraic and the degree of x over M is the maximum degree of $f(x)$ and $g(x)$.
(a) Show that every automorphism of L/K is of the form

$$x \longrightarrow \frac{ax + b}{cx + d},$$

where $ad - bc \neq 0$.
(b) Show that the group of automorphisms of L/K is equal to $\mathrm{PGL}(2, K)$, the group of invertible 2×2 matrices, with entries in K, modulo the subgroup of matrices of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

4. Suppose that the monic polynomial $f(x) \in K[x]$ splits as

$$x^n - a_{n-1}x^{n-1} + \cdots + a_0 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\ldots(x - \alpha_n).$$

Expanding this product we get polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_n$, known as the elementary symmetric polynomials.
(a) Write down all the elementary symmetric polynomials in the case $n \leq 4$.
(b) Show that any polynomial in $\alpha_1, \alpha_2, \ldots, \alpha_n$ which is symmetric under the action of S_n, is a rational function in the symmetric polynomials (challenge problem: show that they are in fact polynomials in

the symmetric polynomials, which are integer polynomials in the case the original polynomial is integral).
(c) Work this out in the case $n = 3$ for the polynomial

$$\alpha^2 + \beta^2 + \gamma^2.$$

(d) If

$$f(x) = x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma),$$

express

$$\alpha^2 + \beta^2 + \gamma^2,$$

in terms of a, b and c.
5. (a) Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$$

be a general monic polynomial of degree n. Show that if the characteristic is coprime to n, then there is an automorphism of $K[x]$, such that the image of $f(x)$ has vanishing term in x^{n-1}.
In the case of a cubic,

$$f(x) = x^3 + ax^2 + bx + c,$$

find the transformed cubic

$$g(x) = x^3 + px + q.$$

(b) Find the discriminant of $g(x)$.
6. Find $\Phi_6(x)$, $\Phi_{10}(x)$, $\Phi_{30}(x)$.
7. Compute the Galois groups of $x^7 - 1$, $x^{20} - 1$ and $x^{60} - 1$ over $\mathbb{Q}$.
8. Give an example of a polynomial which is solvable by radicals, but whose splitting field is not an extension by radicals.
9. Suppose that the characteristic of K is p and that $f(x) = x^p - x - a \in K[x]$, with splitting field L/K. Show that if α is a root of $f(x)$, then the roots of $f(x)$ are

$$\beta, \quad \beta + 1, \quad \beta + 2, \quad \dots, \quad y\beta + p - 1.$$

Show that either $f(x)$ splits in K or that L/K has a cyclic Galois group of order p.
Challenge Problems: 10. Let L/K be a Galois extension with Galois group G. If $\alpha \in L$ the **trace** of α is

$$f(x) = \sum_{\sigma \in G} \sigma(\alpha).$$

Show that the trace is a K-linear map

$$f \colon L \longrightarrow K.$$

Show that the map f is non-zero.

11. Suppose that L/K is a Galois extension of degree p with Galois group G, generated by σ over a field of characteristic p. Let β be an element of L with trace one, and let

$$\alpha = (p-1)\beta + (p-2)\sigma(\beta) + \cdots + 2\sigma^{p-3}(\beta) + \sigma^{p-2}(\beta).$$

Show that $\sigma(\alpha) - \alpha = 1$ and that $a = \alpha^p - \alpha$ is an element of K. Show that $f(x) = x^p - x - a$ is irreducible over K, that L/K is a splitting field for $f(x)$ and that $L = K(\alpha)$.

12. (Hilbert's Theorem 90). Let L/K be a Galois extension of degree n with cyclic Galois group G generated by σ. The Norm of an element $\alpha \in L$ is the product

$$N(\alpha) = \prod_{\phi \in G} \phi(\alpha).$$

(i) Suppose that $\alpha = \beta/\sigma(\beta)$. Show that $N(\alpha) = 1$.

(ii) Conversely suppose that $N(\alpha) = 1$. Show that there is a β such that

$$\alpha = \frac{\beta}{\sigma(\beta)}.$$