MATH 210B. HOMEWORK 1

1. Let $L = \mathbb{Q}(\alpha, \beta)$ with $\alpha^2 = 2$ and $\beta^2 = -1$. Prove that $[L : \mathbb{Q}] = 4$ and prove that $\gamma := \alpha + \beta$ is a primitive element (i.e., $L = \mathbb{Q}(\gamma)$) by considering the possibilities for $[\mathbb{Q}(\gamma) : \mathbb{Q}]$. (Do *not* try to argue by brute force that $\{1, \gamma, \gamma^2, \gamma^3\}$ is linearly independent over $\mathbb{Q}$.)

2. Prove that $f = X^4 - 5$ is irreducible over $\mathbb{Q}$ with a splitting field of degree 8, and exhibit a $\mathbb{Q}$-basis for the splitting field in terms of a root of f and a root of $X^2 + 1$.

3. Choose a prime number p and let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the field with p elements. Consider the field $L = \mathbb{F}_p(X, Y)$ and its subfield $k = \mathbb{F}_p(X^p, Y^p)$.

(i) For $x = X^p$ and $y = Y^p$ in k, prove that L/k is a splitting field of $(T^p - x)(T^p - y)$ over k. Prove that $[L : k] = p^2$.

(ii) Prove that every $\alpha \in L$ satisfies $\alpha^p \in k$, and deduce that L/k does *not* admit a primitive element.

(iii) Construct *infinitely many* distinct subfields of L of degree p over k.

4. Choose $a \in \mathbb{F}_p$, and consider $f_a(T) = T^p - T - a \in \mathbb{F}_p[T]$.

(i) If $a = 0$, show that $f_a = \prod_{r \in \mathbb{F}_p}(T - r)$.

(ii) Assume $a \neq 0$, and let $k/\mathbb{F}_p$ be a splitting field of f_a (so k depends on a). If r, r' are roots of f_a in k, show that $r - r' \in \mathbb{F}_p$. (Hint: compute $(r - r')^p$ and use (i).)

(iii) Deduce from (ii) that if $a \neq 0$ then f_a is irreducible in $\mathbb{F}_p[T]$.

(iv) Using Gauss' Lemma and (iii), show that $T^p - T - 4$ is irreducible over $\mathbb{Q}$, with p any prime.

5. Prove that $f = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$ is irreducible but that for all $c \in \mathbb{Z}$ the polynomial $f(X + c)$ is not Eisenstein with respect to any prime p (i.e., f has no "Eisenstein translate"). In particular, Eisenstein's criterion cannot be used to prove the irreducibility of f. What is the degree over $\mathbb{Q}$ of a splitting field of f?

6. Describe an algorithm that will factor any polynomial $f \in \mathbb{Q}[X]$ into irreducibles in a finite time.