HOMEWORK #3
SOLUTIONS TO SELECTED PROBLEMS

Problem 3.3. (a) Use Eisenstein's criterion with the prime 7. 7 does not divide the highest coefficient, does divide all other coefficients and 7^2 does not divide the constant term.

(b) Use the following lemma:

Lemma. *Let F be a field and let $a, b \in F$ such that $a \neq 0$. Let $f(t) \in F[t]$ be a polynomial and set $g(t) = f(at+b)$. Then f is irreducible if and only if g is irreducible.*

Proof. If $f(t) = f_1(t)f_2(t)$ is a non-trivial factorization then $g(t) = f(at + b) = f_1(at+b)f_2(at+b)$ is a non-trivial factorization of g. Conversely, note that $f(t) = g((t-b)/a)$ so applying the first part gives the result. $\square$

So instead of $f(t) = t^{p-1} + \cdots + t + 1$ we consider $g(t) = f(t+1)$, Then by $f(t) = (t^p - 1)/(t-1)$ we have $g(t) = ((t+1)^p - 1)/t = \sum_{i=1}^{p} \binom{p}{i} t^{i-1} = t^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} t^{i-1}$. Since $\binom{p}{i}$ is divisible by p for $0 < i < p$ and $p^2 \nmid p$, we can apply the Eisenstein's criterion for $g(t)$ with the prime p and get that $g(t)$ is irreducible in $\mathbb{Q}[t]$.

Problem 3.4. (a) By Lemma 3.5 (see Lecture Notes), in order to show that $t^p - x \in K[t]$ is irreducible, it is enough to show that x has no p-th root in K. Indeed, an element of K has the form $f(x,y)/g(x,y)$ for polynomials $f, g \in \mathbb{F}_p[x,y]$. Now, $f(x,y)^p = f(x^p, y^p)$ (because $a^p = a$ for $a \in \mathbb{F}_p$), so that $x = (f/g)^p$ means $xg(x^p, y^p) = f(x^p, y^p)$ which is impossible because all monomials in $f(x^p, y^p)$ have their x degree divisible by p, and in the LHS all monomials have their x degree congruent to 1 modulo p.

(b) Note that one can think of L as $\mathbb{F}_p(x^{1/p}, y)$, i.e. rational functions over $\mathbb{F}_p$ in $x^{1/p}$ (a new variable whose p-th power equals x) and y.

Denote by α a p-th root of x. One can construct an explicit isomorphism $L = K(\alpha) \to \mathbb{F}_p(x^{1/p}, y)$ by

$$(f_0/g_0) + (f_1/g_1)\alpha + \ldots (f_{p-1}/g_{p-1})\alpha^{p-1} \mapsto$$
$$(f_0/g_0) + (f_1/g_1)x^{1/p} + \ldots (f_{p-1}/g_{p-1})x^{(p-1)/p}$$

It is surjective since $\mathbb{F}_p(x^{1/p}, y)$ is an extension of $\mathbb{F}_p(x,y)$ of degree p (it is a simple extension obtained by adjoining $x^{1/p}$ whose minimal polynomial is of degree p).

Now the proof that $t^p - y$ is irreducible in $L[t]$ is the same as in (a), one should consider the y degree in each monomial of the polynomials.

(c) As in (b), one can see that M is isomorphic to $\mathbb{F}_p(x^{1/p}, y^{1/p})$ (a field of rational functions in two variables whose p powers are the original x and y). Any element of M has the form f/g for $f, g \in \mathbb{F}_p[x^{1/p}, y^{1/p}]$, so its p-th power is $f((x^{1/p})^p, (y^{1/p})^p)/g((x^{1/p})^p, (y^{1/p})^p) = f(x,y)/g(x,y)$ a rational function in x, y hence in K.

(d) The extension M/K is not simple since the number of intermediate subfields is infinite. Indeed, for any $f \in K$, consider the subfield $M_f := K(fx^{1/p} + y^{1/p})$ of M. We have $(fx^{1/p} + y^{1/p})^p = f^p x + y \in K$ thus $[M_f : K] \leq p$.

Any two such fields are distinct; if $M_f = M_g$ then $fx^{1/p} + y^{1/p}, gx^{1/p} + y^{1/p} \in M_f$ hence their difference $(f - g)x^{1/p} \in M_f$ thus $x^{1/p} \in M_f$ and $y^{1/p} = (fx^{1/p} + y^{1/p}) - fx^{1/p} \in M_f$, so that $M_f = M$. But this is impossible since $[M : K] = [M : L][L : K] = p^2$ but $[M_f : K] \leq p$.

Since there are infinite elements in $K = \mathbb{F}_p(x, y)$, we get infinite number of intermediate fields $K \subset M_f \subset M$.

Problem 3.5. (a) We can scale any quadratic equation over K to the form $x^2 + bx + c = 0$ where $b, c \in K$. If $\operatorname{char} K \neq 2$, we can "complete the square", i.e. write $x^2 + bx + c = (x + b/2)^2 + (c - b^2/4)$, so x is the solution to the original equation if and only if $x + b/2$ is a solution to the equation $t^2 = b^2/4 - c$. Since by assumption the latter equation has a solution in K, we deduce that the original equation has a solution in K.

(b) If $\operatorname{char} K = 2$, we cannot proceed as in the previous case. Instead, let $x^2 + bx + c = 0$ be a quadratic equation with $b, c \in K$. We distinguish between two cases:

(1) $b = 0$. In this case we have $x^2 = -c$ and a solution x exists by our assumption.
(2) $b \neq 0$. In this case we can write $x = bt$ and then $b^2t^2 + b \cdot bt + c = 0$, or $t^2 + t = -c/b^2$, and the latter equation has a solution by our assumption.

Problem 3.6. Let L/K be a field extension with $[L : K] = 2$ and assume that $\operatorname{char} K \neq 2$. Pick any $\alpha \in L \setminus K$. Then by $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ we get that $L = K(\alpha)$. Since $[K(\alpha) : K] = 2$, the minimal polynomial of α over K has degree 2, i.e. of the form $x^2 + bx + c = 0$ for $b, c \in K$. As in Problem 3.5(a), setting $\beta = \alpha + b/2$ we see that $\beta^2 = b^2/4 - c \in K$ and $K(\beta) = K(\alpha)$. We conclude that $L = K(\beta)$ with β a square root of an element of K.

(a) It follows that it is enough to consider extensions of the form $\mathbb{F}_5(\sqrt{a})$ for $a \in \mathbb{F}_5$ which is not a square. The only possible values of a are $a = 2, 3$. Let's construct an isomorphism $\mathbb{F}_5(\sqrt{2}) \simeq \mathbb{F}_5(\sqrt{3})$.

Elements of $\mathbb{F}_5(\sqrt{3})$ are of the form $c + d\sqrt{3}$ for $c, d \in \mathbb{F}_5$. Since $(2\sqrt{2})^2 = 4 \cdot 2 = 3$, we define

$$c + d\sqrt{3} \mapsto c + 2d\sqrt{2}$$

It is easy to verify that this defines the required isomorphism.

We conclude that there is only one quadratic extension of $\mathbb{F}_5$, up to isomorphism.

(b) Since α is the sum of $\sqrt{2}, \sqrt{3} \in L$, obviously $\mathbb{Q}(\alpha) \subseteq L$. For the opposite inclusion, note that $(\sqrt{3}-\sqrt{2})(\sqrt{3}+\sqrt{2}) = 1$, hence $\sqrt{3}-\sqrt{2} = 1/\alpha$. We see that $\sqrt{3} = (\alpha + 1/\alpha)/2 \in \mathbb{Q}(\alpha)$ and $\sqrt{2} = (\alpha - 1/\alpha)/2 \in \mathbb{Q}(\alpha)$, hence $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$.