Let $p \in \mathbb{P}$ throughout this problem set. Let $n \in \mathbb{N}$. We will write $\mathbb{F}_{p^n}$ for the finite field of $p^n$ elements constructed in Theorem 21 in the lectures.

1. The following are to be performed only with a straightedge and a compass. Prove your answers.

(a) Is it possible to trisect an angle of $90^\circ$?

Solution. Yes. $30^\circ$ is constructible since $\cos 30^\circ = \sqrt{3}/2$ and $\sin 30^\circ = 1/2$ are both constructible numbers: $(\cos 30^\circ)^2 = 3/2 \in \mathbb{Q}$ and $\sin 30^\circ = 1/2 \in \mathbb{Q}$. We can therefore construct a line segment of length $\sqrt{3}/2$ and a second line segment of length $1/2$ perpendicular to the first and meeting at the end points. The line through the two non-meeting end points of the two line segments would then make an angle of $30^\circ$ with the first line segment.

(b) Is it possible to construct a square whose area equals that of a circle of unit radius?

Solution. No. A circle of unit radius has area $\pi$. To construct a square of area $\pi$ requires constructing a line segment of length $\sqrt{\pi}$, which is impossible since $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ and thus not algebraic of degree a power of 2.

(c) Is it possible to construct the roots of $ax^2 + bx + c$ where $a, b, c$ are constructible numbers?

Solution. Yes. If $a = 0$ and $b \neq 0$, then the only root is $x = -c/b$ and is constructible since the constructible numbers form a field. If $a \neq 0$, then $x = -b \pm \sqrt{b^2 - 4ac}/2a$ is constructible since square roots (which may be complex valued — in which case constructibility means both the real and imaginary parts have constructible magnitudes) of constructible numbers are constructible.

2. Show that if $E$ is a finite field, then $E \cong \mathbb{F}_{p^n}$ for some $p \in \mathbb{P}$ and $n \in \mathbb{N}$.

Solution. Since $E$ is a finite field, Theorem 1 in the lectures implies that the prime field of $E$ must be isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for some $p \in \mathbb{P}$. We will identify the prime field of $E$ with $\mathbb{F}_p$. Since $E$ is a finite, it must be a finite extension over $\mathbb{F}_p$. Let $[E : \mathbb{F}_p] = n$ and $e_1, \ldots, e_n \in E$ be a basis. Then every element in $E$ can be written uniquely as

$$\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_p$. Since there are $p$ choices for each $\alpha_i$, $i = 1, \ldots, n$, $E$ contains exactly $p^n$ elements. By Problem 5, $E^\times$ is cyclic. Let $\alpha \in E^\times$ be a generator. Then clearly $E = \mathbb{F}_p(\alpha)$ and by Theorem 2 in the lectures,

$$E \cong \mathbb{F}_p[x]/\langle f^\alpha_{\mathbb{F}_p}(x) \rangle.$$ 

Since the order of $\alpha$ is $|E^\times| = p^n - 1$, we must have $f^\alpha_{\mathbb{F}_p}(x) = x^{p^n-1} - 1$. Hence

$$E \cong \mathbb{F}_p[x]/\langle x^{p^n-1} - 1 \rangle.$$ 

Note that this argument applies to any field with $p^n$ elements and so in particular the field $\mathbb{F}_{p^n}$ constructed in Theorem 21 in the lectures must also satisfy

$$\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/\langle x^{p^n-1} - 1 \rangle.$$
3. Let \( \alpha \) and \( \beta \in \mathbb{F}_2 \) be zeroes of \( x^3 + x^2 + 1 \) and \( x^3 + x + 1 \in \mathbb{F}_2[x] \) respectively. Show that \( \mathbb{F}_2(\alpha) = \mathbb{F}_2(\beta) \).

**Solution.** Since both the given polynomials are irreducible over \( \mathbb{F}_2 \), both \( \mathbb{F}_2(\alpha) \) and \( \mathbb{F}_2(\beta) \) are extension of \( \mathbb{F}_2 \) of degree 3 and thus are subfields of \( \mathbb{F}_2 \) containing \( 2^3 = 8 \) elements. By our construction in the proof of Theorem 21 in the lectures, both of these fields must consist precisely of the zeros in \( \overline{\mathbb{F}}_2 \) of the polynomial \( x^8 - x \). Thus the fields are the same.

4. Show that every irreducible polynomial in \( \mathbb{F}_p \) is a divisor of \( x^{p^n} - x \) for some \( n \in \mathbb{N} \).

**Solution.** Let \( f(x) \) be irreducible of degree \( m \) in \( \mathbb{F}_p[x] \). Let \( K \) be a finite extension of \( \mathbb{F}_p \), with \( \mathbb{F}_p \leq K \leq \mathbb{F}_p \), obtained by adjoining to \( \mathbb{F}_p \) all the zeros of \( f(x) \) in \( \mathbb{F}_p \). Then \( K \) is a finite field of order \( p^n \) for some positive integer \( n \), and consists precisely of all zeros of \( x^{p^n} - x \) in \( \mathbb{F}_p \) by our construction in the proof of Theorem 21 in the lectures. Now \( f(x) \) factors into linear factors in \( K[x] \), and these linear factors are among the linear factors of \( x^{p^n} - x \) in \( K[x] \). Thus \( f(x) \) is a divisor of \( x^{p^n} - x \).

5. Let \( K \) be a field, not necessarily finite. Show that if \( G \) is any finite multiplicative subgroup of the multiplicative group \( K^\times \), then \( G \) is cyclic. In particular, this shows that \( \mathbb{F}_p^\times \), is cyclic. [Hint: use the Fundamental Theorem of Finitely Generated Abelian Group from Math 113.]

**Solution.** Let \( G \leq K^\times \) be finite and \( |G| = n \). Since \( K^\times \) is abelian, so is \( G \). By the Fundamental Theorem of Finitely Generated Abelian Group (Theorem 38.12 in Fraleigh), every finitely generated abelian group is isomorphic to a group of the form

\[
\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^s
\]

where \( m_i \mid m_{i+1} \) for \( i = 1, \ldots, r - 1 \) and \( s \in \mathbb{N} \cup \{0\} \). Since \( G \) is finite abelian, \( s = 0 \) and

\[
G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_r}
\]

where \( m_i \mid m_{i+1} \) for \( i = 1, \ldots, r - 1 \). To show that \( G \) is cyclic, it suffices to show that \( m_r = n \) (and so \( r = 1 \)) and therefore \( G \cong \mathbb{Z}_n \). Suppose not, \( m_r < n \). Since \( m_i \mid m_r \) for all \( i = 1, \ldots, r - 1 \), we must have

\[
g^{m_r} = 1 \quad \text{for all } g \in G.
\]

In other words, the polynomial \( x^{m_r} - 1 \in K[x] \) has \( n \) distinct roots — a contradiction. Hence \( m_r = n \) and so \( G \) is cyclic.

6. Let \( K \) be a field, not necessarily finite. Let \( \operatorname{char}(K) = p \neq 0 \).

(a) Show that the set \( K^p = \{ \alpha^p \mid \alpha \in K \} \) is a subfield of \( K \).

**Solution.** Since \( \operatorname{char}(K) = p \), and \( p \mid (\begin{pmatrix} p \\ k \end{pmatrix}) \) for \( k = 1, \ldots, p - 1 \),

\[
(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k} = \alpha^p + \beta^p.
\]

Clearly for \( \beta \neq 0 \),

\[
(\alpha \beta^{-1})^p = \alpha^p (\beta^{-1})^p.
\]

So for \( \alpha^p, \beta^p \in K^p \), \( \alpha^p \pm \beta^p \in K^p \) and \( \alpha^p (\beta^{-1})^p \in K^p \) if \( \beta \neq 0 \). Hence \( K^p \) is a field and so \( K^p \leq K \).

(b) Let \( K^p \leq L \leq K \). Show that if \( [L : K^p] < \infty \), then \( [L : K^p] = p^n \) for some \( n \in \mathbb{N} \).

**Solution.** If \( [L : K^p] < \infty \), there exist \( \alpha_1, \ldots, \alpha_n \in L \) such that

\[
L = K^p(\alpha_1, \ldots, \alpha_n).
\]

WLOG, we will assume that \( \alpha_i \notin K^p(\alpha_1, \ldots, \alpha_{i-1}) \) for \( i = 1, \ldots, n \). Since

\[
\alpha_i^p \in K^p \subseteq K^p(\alpha_1, \ldots, \alpha_{i-1})
\]
and
\[ \alpha_i \notin K^p(\alpha_1, \ldots, \alpha_{i-1}), \]
the polynomial \( x^p - \alpha_i^p \in K^p(\alpha_1, \ldots, \alpha_{i-1})[x] \) is irreducible over \( K^p(\alpha_1, \ldots, \alpha_{i-1}) \). Hence
\[
[K^p(\alpha_1, \ldots, \alpha_i) : K^p(\alpha_1, \ldots, \alpha_{i-1})] = \deg f_{K^p(\alpha_1, \ldots, \alpha_{i-1})}^\alpha(x) = \deg(x^p - \alpha_i^p) = p.
\]
It follows that
\[
[L : K^p] = [K^p(\alpha_1, \ldots, \alpha_n) : K^p]
= \prod_{i=1}^{n} [K^p(\alpha_1, \ldots, \alpha_i) : K^p(\alpha_1, \ldots, \alpha_{i-1})]
= p^n.
\]