1) Let $\alpha_1 \overset{\text{def}}{=} 8 - 8i$, $\alpha_2 \overset{\text{def}}{=} 10 + 15i$ and $\beta \overset{\text{def}}{=} 2 - 3i$, and let $I \overset{\text{def}}{=} (\beta)$ be the principal ideal of $\mathbb{Z}[i]$ generated by $\beta$.

(a) Compute the quotient and remainders of the divisions of $\alpha_1$ and $\alpha_2$ by $\beta$?

Solution. We divide $\alpha_1$ by $\beta$:

$$\frac{8 - 8i}{2 - 3i} = \frac{(8 - 8i)(2 + 3i)}{(2 - 3i)(2 + 3i)} = \frac{40 + 8i}{13} = \frac{3 + i + 1 - 5i}{q_1}.$$ 

Hence, $\alpha_1 = \beta \cdot q_1 + r_1$, where $r_1 = (8 - 8i) - (2 - 3i)(3 + i) = -1 - i$. So,

$$(8 - 8i) = (2 - 3i)(3 + i) + (-1 - i).$$

[Note $|r_1|^2 = 2 < |2 - 3i|^2 = 13$.]

We divide $\alpha_2$ by $\beta$:

$$\frac{10 + 15i}{2 - 3i} = \frac{(10 + 15i)(2 + 3i)}{(2 - 3i)(2 + 3i)} = \frac{-25 + 60i}{13} = \frac{-2 + 5i + 1 - 5i}{q_2}.$$ 

Hence, $\alpha_2 = \beta \cdot q_2 + r_2$, where $r_2 = (10 + 15i) - (2 - 3i)(-2 + 5i) = -1 - i$. So,

$$(10 + 15i) = (2 - 3i)(-2 + 5i) + (-1 - i).$$

[Note $|r_2|^2 = 2 < |2 - 3i|^2 = 13$.]

(b) Is $\alpha_1 \equiv \alpha_2 \pmod{I}$?

Solution. Yes. Since $r_1 = r_2 = -1 - i$, we have $\alpha_1 - \alpha_2 = (2 - 3i)(3 + i) + r_1 - (2 - 3i)(-2 + 5i) + r_2 = (2 - 3i)((3 + i) - (-2 + 5i)) = (2 - 3i)(5 - 4i)$. Hence, $\alpha_1 - \alpha_2 \in I$, i.e., indeed $\alpha_1 \equiv \alpha_2 \pmod{I}$. 

\square
2) Let $\zeta_{11} \overset{\text{def}}{=} e^{2\pi i/11}$. Prove that there are exactly four intermediate extension of $\mathbb{Q}[\zeta_{13}]/\mathbb{Q}$ [including $\mathbb{Q}$ and $\mathbb{Q}[\zeta_{13}]$. [You do not have to find them.]

Proof. As seen in class, for all prime $p$, we have $\mathbb{Q}[\zeta_{p}]/\mathbb{Q}$ is Galois, with $G(\mathbb{Q}[\zeta_{p}]/\mathbb{Q}) \cong C_{p-1}$. Hence, since $G \overset{\text{def}}{=} G(\mathbb{Q}[\zeta_{11}]/\mathbb{Q}) \cong C_{10}$ is cyclic, it has exactly one subgroup [which is in fact also cyclic] for each divisor of the order, i.e., one subgroup of order 1 [i.e., $\{\text{id}\}$], one subgroup of order 2, one subgroup of order 5, and one subgroup of order 10 [i.e., $G$].

By the Main Theorem of Galois Theory [since $\mathbb{Q}[\zeta_{11}]/\mathbb{Q}$ is Galois], there is a one-to-one correspondence between subgroups of $G$ and intermediate extensions of $\mathbb{Q}[\zeta_{11}]/\mathbb{Q}$. Since there are four subgroups, there are four intermediate fields, with degree equal to the indices: 1 [i.e., $\mathbb{Q}[\zeta_{11}]$], 2, 5, and 10 [i.e., $\mathbb{Q}$].
3) Let $R$ be a ring [which you can assume is commutative with identity, but it is not necessary] and $a \in R$. Let $\phi : R \to R'$ be a homomorphism such that $a \in \ker \phi$. Prove that the map $\psi : R/(a) \to R'$, defined by $\psi(b + (a)) \overset{\text{def}}{=} \phi(b)$ gives a well-defined [you have to prove that it is well-defined] ring homomorphism.

**Proof.**

1. **Well-defined**: Let $b' \in R$ such that $b + (a) = b' + (a)$. Then, we have that there is $ra \in (a)$ [with $r \in R$], such that $b' = b + ra$. Then

   $\psi(b' + (a)) = \phi(b') = \phi(b + ra)$ \hspace{1cm} [defn. of $\psi$]
   $= \phi(b) + \phi(r)\phi(a)$ \hspace{1cm} [$\phi$ is a homom.]
   $= \phi(b) + 0_R = \phi(b)$ \hspace{1cm} [$a \in \ker \phi$]
   $= \psi(b + (a))$ \hspace{1cm} [defn. of $\psi$]

2. **Takes $1_{R/(a)}$ to $1_{R'}$**: We have:

   $\psi(1_{R/(a)}) = \psi(1_R + (a))$
   $= \phi(1_R)$ \hspace{1cm} [defn. of $\psi$]
   $= 1_{R'}$ \hspace{1cm} [$\phi$ is a homom.]

3. **Additive**: We have:

   $\psi((b + (a)) + (c + (a))) = \psi((b + c) + (a))$ \hspace{1cm} [addition in $R/(a)$]
   $= \phi(b + c)$ \hspace{1cm} [defn. of $\psi$]
   $= \phi(b) + \phi(c)$ \hspace{1cm} [$\phi$ is a homom.]
   $= \psi(b + (a)) + \psi(c + (a))$ \hspace{1cm} [defn. of $\psi$]

4. **Multiplicative**: We have:

   $\psi((b + (a)) \cdot (c + (a))) = \psi((bc) + (a))$ \hspace{1cm} [mult. in $R/(a)$]
   $= \phi(bc)$ \hspace{1cm} [defn. of $\psi$]
   $= \phi(b) \cdot \phi(c)$ \hspace{1cm} [$\phi$ is a homom.]
   $= \psi(b + (a)) \cdot \psi(c + (a))$ \hspace{1cm} [defn. of $\psi$]

\[\square\]
4) Prove that if $F$ is a field and $F[[x]]$ represents formal power series over $F$ [as in the second extra-credit problem], then all non-zero ideals of $F[[x]]$ are of the form $(x^n)$ where $n$ is a non-negative integer. [You can use any fact in the statement of the extra-credit problem.]

Proof. Since $F[[x]]$ is an Euclidean domain [by the extra credit problem], it is a PID. So, if $I$ be a non-zero ideal of $F[[x]]$, there is $a \in F[[x]] - \{0\}$ such that $I = (a)$.

By part (b) of the extra credit problem, we can write $a = x^na'$ [$n \overset{\text{def}}{=} \sigma(a)$ in the extra credit problem] where $a'$ is a unit. Then, $a$ and $x^n$ are associates, and hence $(a) = (x^n)$. \qed
5) Construct a field with 8 elements. [Hint: Extend some known field.]

Solution. Let \( f = x^3 + x + 1 \in \mathbb{F}_2[x] \). Then, \( f(0) = 1, f(1) = 1 \), and \( f \) has no root in \( \mathbb{F}_2 \).

Since \( f \) has degree 3, this means that \( f \) is irreducible. Hence, \( F = \mathbb{F}_2[x]/(x^3 + x + 1) \) is an extension field of \( \mathbb{F}_2 \) of degree 3.

Thus, if \( \alpha \overset{\text{def}}{=} \bar{x} \in F \), we have that \( F = \mathbb{F}_2[\alpha] \), with \( \mathbb{F}_2 \)-basis \( \{1, \alpha, \alpha^2\} \), and hence \( F \) has 8 elements: \( \{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\} \). \( \square \)
Let $F$ be a field of characteristic $p \neq 0$, for which the polynomial $f(x) \overset{\text{def}}{=} x^p - x - a \in F[x]$ is irreducible. Let $\alpha$ be a root of $f(x)$ [in some extension of $F$].

(a) Prove that $\alpha + 1$ is also a root of $f(x)$.

\textit{Proof.} Since we are in characteristic $p$, we have that $(a + b)^p = a^p + b^p$. So, $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = f(\alpha) = 0$ [since $\alpha$ is a root of $f$ by hypothesis].

(b) Prove that $F[\alpha]$ is the splitting field of $f(x)$ over $F$. \textbf{[Hint:} Use (a) to find all roots of $f$.\textbf{]}

\textit{Proof.} Repeating the argument above, we have that since $\alpha + 1$ is a root, then $\alpha + 2$ is a root. In this way, we have that $\alpha, \alpha + 1, \ldots, \alpha + (p - 1)$ are roots. [Note that $\alpha + p = \alpha$.] Since these gives us $p$ distinct roots of $f$, and $\deg f = p$, these are all roots of $f$. But, $\alpha + i \in F[\alpha]$. So, $F[\alpha]$ is the splitting field.

(c) Prove that $G(F[\alpha]/F) \cong C_p$.

\textit{Solution.} Since $F[\alpha]$ is a splitting field of $f(x)$ over $F$, we have that $F[\alpha]/F$ is Galois. Hence, $|G(F[\alpha]/F)| = [F[\alpha] : F]$. But since $f$ is monic and irreducible [by hypothesis] and $f(\alpha) = 0$, we have that $f = \min_{\alpha,F}$, and so $|G(F[\alpha]/F)| = [F[\alpha] : F] = \deg f = p$. Since $p$ is prime, and $G(F[\alpha]/F) \cong C_p$ [every group of prime order is cyclic].
7) Let $K \overset{\text{def}}{=} \mathbb{Q}[\sqrt[4]{2}, i]$.

(a) Find $[K : \mathbb{Q}]$.

Solution. We have that $[K : \mathbb{Q}] = [K : \mathbb{Q}[\sqrt[4]{2}]] \cdot [\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}]$.

Since $x^4 - 2$ is irreducible [by a Eisenstein’s criterion], we have that $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] = 4$.

Moreover, since $\mathbb{Q}[\sqrt[4]{2}] \subseteq \mathbb{R}$, but $K \not\subseteq \mathbb{R}$, we have $K \neq \mathbb{Q}[\sqrt[4]{2}]$. Hence, $[K : \mathbb{Q}[\sqrt[4]{2}]] \geq 2$, and since $i$ is a root of $x^2 + 1$, we must have $[K : \mathbb{Q}[\sqrt[4]{2}]] \leq 2$. So, $[K : \mathbb{Q}[\sqrt[4]{2}]] = 2$.

Therefore, $[K : \mathbb{Q}] = 2 \cdot 4 = 8$.

(b) Give a $\mathbb{Q}$-basis for $K$ [as a vector space over $\mathbb{Q}$].

Solution. We have that $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\sqrt[4]{2}]$. Also, $\{1, i\}$ is a $\mathbb{Q}[\sqrt[4]{2}]$-basis of $K$. Hence, a $\mathbb{Q}$-basis of $K$ is $\{1 \cdot 1, 1 \cdot \sqrt[4]{2}, 1 \cdot \sqrt[4]{4}, 1 \cdot \sqrt[4]{8}, i \cdot 1, i \cdot \sqrt[4]{2}, i \cdot \sqrt[4]{4}, i \cdot \sqrt[4]{8}\} = \{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}, i, i \cdot \sqrt[4]{2}, i \cdot \sqrt[4]{4}, i \cdot \sqrt[4]{8}\}$.

(c) Prove that $K/\mathbb{Q}$ is Galois.

Proof. Since $f \overset{\text{def}}{=} x^4 - 2 = (x - \sqrt[4]{2})(x - i\sqrt[4]{2})(x - (-\sqrt[4]{2}))(x - (-i\sqrt[4]{2}))$, the splitting field of $f$ is $L \overset{\text{def}}{=} \mathbb{Q}[\sqrt[4]{2}, i\sqrt[4]{2}]$. Clearly $L \subseteq K$ [since $i, \sqrt[4]{2} \in K$]. But since $\sqrt[4]{2}, i\sqrt[4]{2} \in L$, then $i \overset{\text{def}}{=} (i\sqrt[4]{2})/\sqrt[4]{2} \in L$. Hence, $K = L$.

Since $K$ is a splitting field over $\mathbb{Q}$, we have that $K/\mathbb{Q}$ is Galois.

(d) If $\sigma \in G(K/\mathbb{Q})$, then what are the possible values of $\sigma(\sqrt[4]{2})$ and $\sigma(i)$?

Solution. Since $\sigma$ fixes $\mathbb{Q}$ and $\sqrt[4]{2}$ and $i$ are roots of $x^4 - 2$ and $x^2 + 1$, respectively, both of which have coefficients in $\mathbb{Q}$, then $\sigma$ must take $\sqrt[4]{2}$ to another root of $x^4 - 2$, namely, $\pm \sqrt[4]{2}$ or $\pm i\sqrt[4]{2}$, and $i$ to another root of $x^2 + 1$, namely $\pm i$.
8) In this problem we will show that if \( R \) is commutative ring with identity, and \( a \in R \) is such that \( a^n = 0 \) for some positive integer \( n \), then \( a \) is in every maximal ideal of \( R \). [Note that if \( a \neq 0 \), then \( R \) is not an integral domain!]

(a) Let \( I \) be an ideal and \( a \in R \). Prove that
\[
(I, a) \overset{\text{def}}{=} \{x + ra : x \in I \text{ and } r \in R\}
\]
is an ideal of \( R \) that contains \( I \) and \( a \).

Proof. 1. Non-empty (and containment): Clearly, \( 0 + 1 \cdot a = a \in (I, a) \). Also, for all \( x \in I \), \( x = x + 0 \cdot a \in (I, a) \). So, \( I \subseteq (I, a) \).

2. Additive: Let \( x + ra, y + sa \in (I, a) \) [with \( x, y \in I \) and \( r, s \in R \)]. Then \((x + ra) + (y + sa) = (x + y) + (r + s)a \). Since \( I \) and \( R \) are closed under addition, we have that \((x + y) \in I \) and \((r + s) \in R \). Thus, \((x + ra) + (y + sa) \in (I, a) \).

3. Multiplicative: Let \( s \in R \) and \( x + ra \in (I, a) \) [with \( x \in I \) and \( r \in R \)]. Then \( s(x + ra) = sx + (sr)a \). Since \( R \) is closed under multiplication, we have \( sr \in R \), and since \( I \) is an ideal, and \( x \in I \), \( sx \in I \). Thus, \( s(x + ra) \in (I, a) \).

(b) Prove that if \( M \) is a maximal ideal and \( a^n = 0 \) [and you can assume \( a^{n-1} \neq 0 \)] for some positive integer \( n \), with \( a \notin M \), then \( a^{n-1} \in M \). [Hint: Start by proving that \( 1_R \in (M, a) \), and then use (a).]

Proof. Since \( M \subseteq (M, a) \) [from (a)] and \( a \notin (M, a) \) but \( a \notin M \), we have \( M \not
subseteq (M, a) \subseteq R \). Since \( M \) is a maximal [and \( (M, a) \) is an ideal], we have \( (M, a) = R \). Therefore, \( 1 \in (M, a) \). So, there are \( x \in M \) and \( r \in R \) such that \( 1 = x + ra \). Multiplying by \( a^{n-1} \) we have \( a^{n-1} = a^{n-1}x + ra^{n-1} = a^{n-1}x \) [since \( a^n = 0 \)]. Since \( x \in M \) [an ideal] and \( a^{n-1} = a^{n-1}x \in M \), we have that \( a^{n-1} \in M \). [Note that since we might no be in a domain, we cannot cancel the \( a^{n-1} \) above!]

(c) Prove that since \( a^{n-1} \in M \), we actually have \( a \in M \) [which is then a contradiction to the fact that \( a \notin M \)].

Proof. Since \( M \) is maximal, it is a prime ideal. Since \( M \) is prime, and \( a^{n-1} \in M \), we have \( a \in M \).