Set 7. Please study the following Problems 61–70 by March 1 (Friday).
This time, you prove quadratic reciprocity law and related things.

61. Let $K$ be a commutative field whose characteristic is not 2 and which contains a primitive 8-th root $\zeta_8$ of 1 (a primitive $n$-th root of 1 is an element $\alpha$ such that $\alpha^n = 1$ and $\alpha^i \neq 1$ for $1 \leq i < n$).
Prove that $\zeta_8 + \zeta_8^{-1}$ is a square root of 2.

62. Let $p$ be a prime number which is not 2. In Problem 61, take the algebraic closure of $\mathbb{F}_p$ as $K$. By using the fact $\mathbb{F}_p = \{ x \in K \mid x^p = x \}$ and by using Problem 61, prove the formula \( \left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}} \), that is, a square root of 2 exists in $\mathbb{F}_p$ if and only if $p \equiv 1, 7 \text{ mod } 8$ and does not exist if $p \equiv 3, 5 \text{ mod } 8$.

63. Let $K$ be a commutative field whose characteristic is not 3 and which contains a primitive cubic root $\zeta_3$ of 1. Prove that $\zeta_3 - \zeta_3^2$ is a square root of $-3$. Let $p$ be a prime number which is not 2, 3. By taking the algebraic closure of $\mathbb{F}_p$ as $K$ and using the fact $\mathbb{F}_p = \{ x \in K \mid x^p = x \}$, prove that $\left( \frac{-3}{p} \right)$ is 1 if and only if $p \equiv 1 \text{ mod } 3$.

The following Problems 64 and 65 are preparations for Problem 66 which is a generalization of Problem 63.

64. Let $N \geq 1$ be an integer, let $K$ be a commutative field, and assume that $K$ contains a primitive $N$-th root $\zeta_N$ of 1. For a function $f : \mathbb{Z}/N\mathbb{Z} \to K$, define the Fourier transform $\mathcal{F}(f)$ of $f$ as the function $\mathbb{Z}/N\mathbb{Z} \to K$ defined by
\[
(\mathcal{F}(f))(x) = \sum_{y \in \mathbb{Z}/N\mathbb{Z}} f(y) \zeta_N^{xy}.
\]
(This is an analogue of the Fourier transform of a function on $\mathbb{R}$.) Let $g = \mathcal{F}(\mathcal{F}(f))$. Prove $g(x) = Nf(-x)$.

65. In Problem 64, in the case $N$ is a prime number $q$ and $f : \mathbb{F}_q = \mathbb{Z}/q\mathbb{Z} \to K$ is defined by $f(x) = (\frac{x}{q})$ if $x \neq 0$ and $f(0) = 0$, prove that $\mathcal{F}(f) = G \cdot f$ where $G = \sum_{a \in \mathbb{F}_q^\times} (\frac{a}{q}) \zeta_q^a$.

66. Let $K$ be a commutative field and let $q$ be a prime number which is different from 2. Assume that the characteristic of $K$ is not 2, $q$, and assume that $K$ contains a primitive $q$-th root $\zeta_q$ of 1. Let $q^* = q$ if $q \equiv 1 \text{ mod } 4$, and let $q^* = -q$ if $q \equiv 3 \text{ mod } 4$. Using Problems 64 and 65, prove that
\[
\sum_{a \in \mathbb{F}_q^\times} (\frac{a}{q}) \zeta_q^a \text{ is a square root of } q^*.
\]
(For Problems 66 and 67, please use the fact $\left( \frac{-1}{p} \right) = (-1)^{\frac{p^2+1}{2}}$ freely.)
67. Let $p$ and $q$ be prime numbers which are not 2 and assume $p \neq q$. In Problem 66, take the algebraic closure of $\mathbb{F}_p$ as $K$. By using the fact $\mathbb{F}_p = \{ x \in K \mid x^p = x \}$ and by using Problem 66, prove the formula

$$\left( \frac{q}{p} \right) = \left( \frac{p}{q} \right).$$

From this, deduce the quadratic reciprocity law

$$\left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

68. By using Problem 64 and Problem 65 taking the algebraic closure of $\mathbb{Q}$ as $K$, prove that if $L$ is a quadratic field (an extension of $\mathbb{Q}$ of degree 2), then $L \subset \mathbb{Q}(\zeta_N)$ for some $N \geq 1$. Here $\zeta_N$ denotes a primitive $N$-th root of 1.

69. Let $K$ be a commutative field whose characteristic is not 7 and which contains a primitive 7-th root $\zeta_7$ of 1. Prove that for $a = 1, 2, 3$, $\zeta_7^a + \zeta_7^{-a}$ are solutions of $x^3 + x^2 - 2x - 1 = 0$.

Let $p$ be a prime number which is not 7. By taking the algebraic closure of $\mathbb{F}_p$ as $K$ and by using the fact $\mathbb{F}_p = \{ x \in K \mid x^p = x \}$, prove that $x^3 + x^2 - 2x - 1 = 0$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \mod 7$.

70. Let $p$ be a prime number which is not 7. Let $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ and let $O_F$ be the integer ring of $F$. Prove that if $p \equiv \pm 1 \mod 7$, there are three maximal ideals $\mathfrak{p}$ of $O_F$ such that $pO_F \subset \mathfrak{p}$. Prove that for other $p$, $pO_F$ is a maximal ideal.

(Please use the fact

$$\mathbb{Z}[T]/(T^3 + T^2 - 2T - 1) \cong O_F ; \ T \mapsto \zeta_7 + \zeta_7^{-1}.$$ )