Some “Higher Arithmetic”

Lemma 1: Suppose $F$ is a field and $P(X) \in F[X]$ is an irreducible (over $F$) polynomial of degree $n \geq 1$. If $K \supseteq F$ is another field and $\zeta \in K$ is a root of $P$, then $1, \zeta, \ldots, \zeta^{n-1}$ are linearly independent over $F$.

Proof: Suppose we have some linear combination

$$a_0 \cdot 1 + a_1 \cdot \zeta + \cdots + a_{n-1} \cdot \zeta^{n-1} = 0$$

with $a_0, \ldots, a_{n-1} \in F$. Then $\zeta$ is a root of the polynomial $Q(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \in F[X]$ of degree strictly less than $n$. Suppose for the moment that $Q(X) \neq 0$. Since $P$ is irreducible and the degree of $Q \neq 0$ is less than the degree of $P$, the greatest common divisor of $P$ and $Q$ is 1 and we may write (via the Euclidean algorithm)

$$A(X)P(X) + B(X)Q(X) = 1,$$

where $A(X), B(X) \in F[X]$. But now evaluating at $\zeta$ gives us the impossible equation $0 = 1$. Thus $Q = 0$ and our powers of $\zeta$ are linearly independent over $F$.

Application: Suppose $P(X) \in \mathbb{Z}[X]$ is monic and irreducible over $\mathbb{Q}$ (which as we’ve seen is the same as saying it’s irreducible over $\mathbb{Z}$) of degree $n > 1$. Let $\zeta$ be a root of $P$ and set

$$\mathbb{Z}[\zeta] = \{a_0 + a_1 \zeta + \cdots + a_{n-1} \zeta^{n-1} : a_i \in \mathbb{Z} \text{ for all } i\}.$$ 

Add and multiply elements here in the obvious manner. Then this set is closed under addition (obviously) and multiplication (using $P(\zeta) = 0$ allows us to rewrite all powers of $\zeta$ in terms of $1, \zeta, \ldots, \zeta^{n-1}$). Moreover, by the lemma above every element here is uniquely represented as a $\mathbb{Z}$-linear combination of $1, \ldots, \zeta^{n-1}$. Notice how $\mathbb{Z} \subseteq \mathbb{Z}[\zeta]$.

Basic arithmetic in $\mathbb{Z}[\zeta]$ will work the same as $\mathbb{Z}$, meaning we have the usual properties of addition and multiplication (though not necessarily the fancier stuff like the Euclidean algorithm or unique factorization). In particular, given a non-zero modulus $\mu \in \mathbb{Z}[\zeta]$ and two $\alpha, \beta \in \mathbb{Z}[\zeta]$, we say $\alpha$ is congruent to $\beta$ modulo $\mu$ if $\mu$ divides their difference, i.e., $\mu \gamma = \alpha - \beta$ for some $\gamma \in \mathbb{Z}[\zeta]$. This is an equivalence relation, just as it is over $\mathbb{Z}$, and the modular arithmetic works as usual.
Lemma 2: With the notation as above, if \( m \) is a positive integer and \( a, b \in \mathbb{Z} \) are congruent modulo \( m \) in \( \mathbb{Z}[\zeta] \), then \( a \equiv b \mod m \) as a regular congruence of integers.

Proof: We have \( m\gamma = a - b \) for some \( \gamma \in \mathbb{Z}[\zeta] \). Writing \( \gamma = a_0 + \cdots + a_{n-1}\zeta^{n-1} \), we have

\[
ma_0 + ma_1\zeta + \cdots + ma_{n-1}\zeta^{n-1} = a - b
\]

\[
(b - a + ma_0) + ma_1\zeta + \cdots + ma_{n-1}\zeta^{n-1} = 0.
\]

Since the powers of \( \zeta \) here are linearly independent over \( \mathbb{Q} \), we must have \( a_1 = \cdots = a_{n-1} = 0 \), i.e. \( \gamma \in \mathbb{Z} \).