Theorem 8.1

Let \( n \in \mathbb{N} \) and let \( \alpha \in \mathbb{C} \) be a primitive root of unity in \( \mathbb{C} \) of order \( n \). Then the cyclotomic extension of \( \mathbb{Q} \) of degree \( n \) is a finite field, and it is isomorphic to the cyclic field of \( \mathbb{Z}/n\mathbb{Z} \).
We prove the first statement by (the Strong Principle of Induction).

\[
(x)^p \prod_{u > p, |u| \mid p} (x)^u \equiv (x)^p \prod_{u \geq p, |u| \mid p} = K - u^x
\]

\[
(\prod_{u \geq p, |u| \mid p} (x)^u)^{p=\mid u\mid \mid p} \cdot \prod_{\mid u\mid \mid p} (x)^u \equiv (x)^p \prod_{\mid u\mid \mid p} = (x)^p \prod_{\mid u\mid \mid p} = K - u^x
\]

Then, the coefficients are actually integers.

Therefore, for each divisor \(d\) of \(n\) by the definition of \(\mathbf{g}(\mathbb{F}_p)\), there is no cyclic extension of \(\mathbb{F}_p\) of order \(m\).

Theorem V.8.2. Let \(n \in \mathbb{N}\). Let \(\mathbb{F}_n\) be an extension of \(\mathbb{F}_p\) that has \(\mathbb{F}_n\) as a cyclic extension of \(\mathbb{F}_p\).

Proof (continued). (i) Assume that \(\mathbb{F}_n\) is true for all \(k\). Then, for \(p > k\), let \(\mathbb{F}_n\) be a cyclic extension of \(\mathbb{F}_p\) of order \(m\). Then, \(\mathbb{F}_n\) is a cyclic extension of \(\mathbb{F}_p\).

Theorem V.8.2 (continued)
But the number of such \( i \) is by definition precisely

\[ \langle u, \zeta \rangle = \langle u, \zeta \rangle \]

root of unity (i.e., a generator of \( G \) that and only if \( \gcd(i, \zeta) \subseteq \langle \zeta \rangle \)). By Theorem 1.3.6,\( \langle \zeta \rangle \subseteq \langle \zeta \rangle \). Since \( \langle \zeta \rangle \subseteq \langle \zeta \rangle \) and that every other primitive root is a power of \( \zeta \), there is exactly one primitive root.

**Proof (continued).** (iii) By the definition of \( \gcd(g, \zeta) \), the following hold:

- The following hold:

**Theorem V.8.2.** Let \( u \in \mathbb{N} \). Let \( \mathcal{K} \) be a field such that \( \mathcal{K} \langle \zeta \rangle \) does not divide \( u \) and let \( \mathcal{G}(x) \) be the monic cyclotomic polynomial over \( \mathcal{K} \). Then

\[ \langle u, \zeta \rangle = \langle u, \zeta \rangle \]

But as above, this implies \( u = 0 \) and \( \langle u, \zeta \rangle = \langle u, \zeta \rangle \) if \( \gcd(u, \zeta) \subseteq \langle \zeta \rangle \). Since \( \langle \zeta \rangle \subseteq \langle \zeta \rangle \) and \( \langle \zeta \rangle \subseteq \langle \zeta \rangle \) with the above notation, By the Division Algorithm V.3.1, A. As argued above, B. \( \mathcal{G}(x) \) is a divisor of \( \mathcal{G}(x) \) in \( \mathcal{K} \langle \zeta \rangle \). Let \( \mathcal{H} \subseteq \mathcal{K} \langle \zeta \rangle \) be a prime field. Then the coefficients are actually integers.

**Theorem V.8.2.** Let \( u \in \mathbb{N} \). Let \( \mathcal{K} \) be a field such that \( \mathcal{K} \langle \zeta \rangle \) does not divide \( u \) and let \( \mathcal{G}(x) \) be the monic cyclotomic polynomial over \( \mathcal{K} \). Then

\[ \langle u, \zeta \rangle = \langle u, \zeta \rangle \]