V. Fields and Galois Theory

V.8. **Cyclotomic Extensions.**

2. Establish the following properties of the Euler function φ.

a) If p is prime and $n > 0$, then $\varphi(p^n) = p^n\left(1 - \frac{1}{p}\right) = p^{n-1}(p-1)$.

p prime $\implies$ $\varphi(p) = p - 1$, so we enumerate those numbers which are not relatively prime to p^n:

$$\begin{array}{cccccc} p & 2p & 3p & \dots & (p-1)p & p\cdot p \\ (p+1)p & (p+2)p & (p+3)p & \dots & (p^2-1)p & p^2\cdot p \\ (p^2+1)p & (p^2+2)p & (p^2+3)p & \dots & (p^3-1)p & p^3\cdot p \\ \vdots & & & & & \\ (p^{n-2}+1)p & (p^{n-2}+2)p & (p^{n-2}+3)p & \dots & (p^{n-1}-1)p & (p^{n-1})p \end{array}$$

Since there are p^{n-1} elements in the list above, there must be

$$p^n - p^{n-1} = p^{n-1}(p-1)$$

numbers which are less than p^n and relatively prime to it, i.e.,

$$\varphi(p^n) = p^{n-1}(p-1).$$

b) If $(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Note that $\varphi(m) = |\mathbb{Z}_m^\times|$ and $\varphi(n) = |\mathbb{Z}_n^\times|$. Define an isomorphism

$$\gamma : \mathbb{Z}_{mn}^\times \to \mathbb{Z}_m^\times \oplus \mathbb{Z}_n^\times \qquad \text{by} \qquad \gamma : x \mapsto (x \bmod m, x \bmod n)$$

to get $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \oplus \mathbb{Z}_n^\times$, so $\varphi(m,n) = |\mathbb{Z}_{mn}^\times|$.

c) If $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ (p_i are distinct primes, $k_i \in \mathbb{N}$), then

$$\varphi(n) = n\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\cdots\left(1-\tfrac{1}{p_r}\right).$$

Since powers of distinct primes are always relatively prime, we have

$$\varphi(n) = \varphi\left(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\right) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p_r^{k_r}\right) \quad \text{by (b)}$$

But then

$$\varphi\left(p_i^{k_i}\right) = p_i^{k_i}\left(1-\tfrac{1}{p_i}\right) \quad \text{by (a)}$$

shows that

$$\begin{aligned}\varphi(n) &= p_1^{k_1}\left(1-\tfrac{1}{p_1}\right)\cdot p_2^{k_2}\left(1-\tfrac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\tfrac{1}{p_r}\right) \\ &= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\cdots\left(1-\tfrac{1}{p_r}\right) \\ &= n\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\cdots\left(1-\tfrac{1}{p_r}\right)\end{aligned}$$

d) Prove that $\sum_{d|n} \varphi(d) = n$.

$$\begin{aligned} n &= \deg(x^n - 1) \\ &= \deg\left(\prod_{d|n} g_d(x)\right) && \text{by 8.2(i)} \\ &= \sum_{d|n} \deg(g_d(x)) && \text{by III.6.1} \\ &= \sum_{d|n} \varphi(d) && \text{by 8.2(iii)} \end{aligned}$$

■

e) Show that $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$, where μ is the Moebius function defined by

$$\mu(n) = \begin{cases} 1 & \text{if n=1} \\ (-1)^t & \text{if n is the product of } t \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

First, we use the simple identity $n = \frac{n}{d} d$ to note that $d|n \iff \frac{n}{d}|n$, which allows us to simplify the given formula by substituting d for $\frac{n}{d}$:

$$\varphi(n) = \sum_{\frac{n}{d}|n} \mu(d) \tfrac{n}{d} = \sum_{d|n} \mu(d) \tfrac{n}{d} = n \sum_{d|n} \tfrac{\mu(d)}{d}$$

We break apart the latter sum as follows:

$$\begin{aligned} n \sum_{d|n} \tfrac{\mu(d)}{d} &= n\left(\tfrac{\mu(1)}{1} + \sum_i \tfrac{\mu(p_i)}{p_i} + \sum_{i<j} \tfrac{\mu(p_i p_j)}{p_i p_j} + \ldots + \tfrac{\mu(p_1 p_2 \cdots p_k)}{p_1 p_2 \cdots p_k}\right) \\ &= n\left(1 - \sum_i \tfrac{1}{p_i} + \sum_{i<j} \tfrac{1}{p_i p_j} - \ldots + \tfrac{(-1)^k}{p_1 p_2 \cdots p_k}\right) \\ &= n\left(\prod_{i=1}^k \left(1 - \tfrac{1}{p_i}\right)\right) && \text{by (c)} \\ &= \varphi(n) \end{aligned}$$

■

3. Let φ be the Euler-phi function.

a) $\varphi(n)$ is even for $n > 2$.

First consider the primes p. $\varphi(2) = 1$ and since every prime $p > 2$ is odd, p odd $\implies p - 1 = \varphi(p)$ is even, $\forall p > 2$.
Now consider powers of primes p^r. $\varphi(p^r) = p^{r-1}(p-1)$, as shown in 2(a), and $(p-1)$ is even, as mentioned above, so $\varphi(p^r)$ is even.
Now consider the general case, where $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, so

$$\begin{aligned} \varphi(n) &= \varphi\left(\prod_{i=1}^k p_i^{r_i}\right) \\ &= \prod_{i=1}^k \varphi\left(p_i^{r_i}\right) && \text{by 2(b)} \end{aligned}$$

where the second equality follows because powers of distinct primes are always relatively prime. Since each factor on the right is even by the previous remarks, the entire product $\varphi(n)$ contains factors of 2 and is hence even. ■

b) Find all $n > 0$ such that $\varphi(n) = 2$.

First note that 3 is the smallest $n \in \mathbb{N}$ for which $\varphi(n) = 2$, by inspection.
Now considering powers of primes, we know $\varphi(p^r) = p^{r-1}(p-1)$ by 2(a), so $p^{r-1}(p-1) = 2$ would imply either $p = 2, r = 2$, or $p > 2, r = 1$. Any other options would force $p^{r-1}(p-1) > 2$. So the only powers of primes p^r with $\varphi(p^r) = 2$ are 4 and 3, respectively.
Now consider the general case, where $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Then

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{r_i}\right) = \prod_{i=1}^k \varphi\left(p_i^{r_i}\right) = 2$$

only if $\varphi\left(p_i^{r_i}\right) = 2$ for exactly one i, and for all other factors, $\varphi\left(p_j^{r_j}\right) = 1$. Now note that the only number for which $\varphi\left(p_j^{r_j}\right) = 1$ is $p_j = 2$ (and in this case, $r_j = 1$). This leaves the possibilities

$$p_1^{r_1} = 2^2, p_2^{r_2} = 2^1 \qquad \text{or} \qquad p_1^{r_1} = 3^1, p_2^{r_2} = 2^1$$

but note that the first is not a list of distinct primes.
Thus, only $\varphi(3), \varphi(4), \varphi(6) = 2$. ■

c) Find all pairs (n, p) where $n, p > 0$, p is prime, and $\varphi(n) = \frac{n}{p}$.

5. If $f(x) = \sum_{i=0}^{n} a_i x^i$, let $f(x^s)$ be the polynomial $f(x^s) = \sum_{i=0}^{n} a_i x^{is}$.
Establish the following properties of the cyclotomic polynomials $g_n(x)$ over $\mathbb{Q}$.

a) If p is prime and $k \geqslant 1$, then $g_{p^k}(x) = g_p(x^{p^k - 1})$.

Proceed by induction on k.
Consider g_{p^2}. We know that $x^n - 1 = \prod_{d|n} g_d(x)$ by 8.2(i), and the only numbers dividing p^2 are $p^2, p, 1$, so

$$\begin{aligned} x^{p^2} - 1 &= \prod_{d|p^2} g_d(x) \\ &= g_{p^2}(x) g_p(x) g_1(x) \\ &= g_{p^2}(x)\left(x^p - 1\right), \end{aligned}$$

which implies $g_{p^2}(x) = \frac{x^{p^2}-1}{x^p-1}$. Now make the substitution $u = x^p$ (so that $u^p = (x^p)^p = x^{p^2}$) to see that this expression becomes

$$\begin{aligned} g_{p^2}(x) &= \tfrac{u^p-1}{u-1} \\ &= 1 + u + u^2 + \ldots + u^{p-1} \\ &= 1 + x^p + x^{2p} + \ldots + x^{p^2-p} \\ &= g_p(x^p) \end{aligned}$$

where the final equality follows from the definition of g_p as

$$g_p(x^p) = \tfrac{x^p-1}{x-1} = 1 + x + x^2 + \ldots + x^{p-1}.$$

■

b) If $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where the p_i are distinct primes and $k \in bN$, then

$$g_n(x) = g_{p_1 p_2 \cdots p_k}\left(x^{p_1^{r_1-1} p_2^{r_2-1} \cdots\, p_k^{r_k-1}}\right)$$

6. Let F_n be a cyclotomic extension of $\mathbb{Q}$ of order n; i.e.,
F_n is a splitting field over $\mathbb{Q}$ of $x^n - 1$.

a) Determine $\mathrm{Aut}_{\mathbb{Q}} F_5$ and all intermediate fields.

5 is prime, so $\deg g_5 = \deg\left(1 + x + x^2 + x^3 + x^4\right) \implies [F_5 : \mathbb{Q}] = 4$.
Now $\mathrm{Aut}_{\mathbb{Q}} F_5 \cong \mathbb{Z}_5^{\times}$ by 8.3(iii), so $|\mathrm{Aut}_{\mathbb{Q}} F_5| = 4$, which implies that

$$\mathrm{Aut}_{\mathbb{Q}} F_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \text{or} \qquad \mathrm{Aut}_{\mathbb{Q}} F_5 \cong \mathbb{Z}_4$$

But $\mathrm{Aut}_{\mathbb{Q}} F_5$ is cyclic and Galois, by 5.10, so $\mathrm{Aut}_{\mathbb{Q}} F_5 \cong \mathbb{Z}_4$. We determine the intermediate fields of $F_5 : \mathbb{Q}$ by examining the subgroups of $\mathrm{Aut}_{\mathbb{Q}} F_5$: $1, \mathbb{Z}_2, \mathbb{Z}_4$.
Since $\mathcal{F}(\mathbb{Z}_4) = \mathbb{Q}$ and $\mathcal{F}(\{1\}) = F_5$, it suffices to consider $\mathcal{F}(\mathbb{Z}_2)$.
Take ζ to be a primitive 5th root of unity, so that $Z_2 \cong \{\sigma_0, \sigma_1\}$ where

$$\sigma_0 : \mathbb{Q}(\zeta) \xrightarrow{id} \mathbb{Q}(\zeta) \quad \text{and} \quad \sigma_1 : \mathbb{Q}(\zeta) \longrightarrow \mathbb{Q}(\zeta) \text{ by } \sigma(\xi) = \xi^3$$

$\mathcal{F}(\mathbb{Z}_2) = \{u \in \mathbb{Q}(\zeta) \vdots \sigma(u) = u\}$, so pick a $u \in \mathbb{Q}(\zeta)$. If

$$u = 1 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 + q_4\zeta^4,\ q_i \in \mathbb{Q}$$

is in the fixed field, then

$$\sigma(u) = 1 + q_1\zeta^3 + q_2\zeta^1 + q_3\zeta^4 + q_4\zeta^2 = u$$

implies that $q_1 = q_2, q_2 = q_4, q_4 = q_3,$ and $q_3 = q_1$. Thus, the fixed field is

$$\mathcal{F}(\mathbb{Z}_2) = \{1 + q\left(\zeta + \zeta^2 + \zeta^3 + \zeta^4\right) \vdots q \in Q\}.$$

■

b) Determine $\text{Aut}_{\mathbb{Q}} F_8$ and all intermediate fields.

Let ζ be a primitive 8th root of unity. Using 8.3(ii) and #2(a), we derive

$$[F_8 : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(8) = \varphi\left(2^3\right) = 2^2(2-1) = 4,$$

so we must have

$$\text{Aut}_{\mathbb{Q}} F_8 \cong \mathbb{Z}_4 \qquad \text{or} \qquad \text{Aut}_{\mathbb{Q}} F_8 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

We also have that $\text{Aut}_{\mathbb{Q}} F_8 \leqslant \mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. Noticing that

$$\begin{aligned}
|3| &= 2 &&\text{because } 9 = 8 + 1 \equiv_8 1\\
|5| &= 2 &&\text{because } 25 = 24 + 1 \equiv_8 1\\
|7| &= 2 &&\text{because } 49 = 48 + 1 \equiv_8 1\\
|9| &= 2 &&\text{because } 81 = 80 + 1 \equiv_8 1,
\end{aligned}$$

we see that $\text{Aut}_{\mathbb{Q}} F_8$ has no elements of order 4, and hence $\text{Aut}_{\mathbb{Q}} F_8 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Since $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ has two subgroups isomorphic to $\mathbb{Z}_2$, the field extension $F_8 : \mathbb{Q}$ has two intermediate fields. Consider these two subgroups of $\text{Aut}_{\mathbb{Q}} F_8$:

$$\begin{aligned}
\mathbb{Z}_2 &\cong \{1, \sigma\} = G_1 &&\text{where } \sigma(\xi) = \xi^3\\
\mathbb{Z}_2 &\cong \{1, \tau\} = G_2 &&\text{where } \tau(\xi) = \xi^5
\end{aligned}$$

To determine $\mathcal{F}(G_1)$, consider that for $u = 1 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 \in \mathbb{Q}(\zeta)$,

$$\sigma(u) = 1 + q_1\zeta^3 - q_2\zeta^2 + q_3\zeta^1$$

So $q_2 = -q_2 \implies q_2 = 0$, and we have

$$u \in \mathcal{F}(G_1) \iff u = 1 + q(\zeta + \zeta^3) \quad \text{for some } q \in \mathbb{Q}.$$

To determine $\mathcal{F}(G_2)$, consider that for $u = 1 + q_1\zeta + q_2\zeta^2 + q_3\zeta^3 \in \mathbb{Q}(\zeta)$,

$$\begin{aligned}
\tau(u) &= 1 + q_1\zeta^5 + q_2\zeta^2 + q_3\zeta^7\\
&= 1 - q_1\zeta^3 + q_2\zeta^2 - q_3\zeta
\end{aligned}$$

So $u \in \mathcal{F}(G_2) \iff u = 1 + q\zeta + r\zeta^2 - q\zeta^3 \quad$ for some $q, r \in \mathbb{Q}$. ■