MATH 421
Lecture notes

Roots of unity with special emphasis on finite fields [pp 67 – 70]

These notes differ considerably from Rotman’s presentation.

**Lemma 68**: As per Rotman. Note in particular the observation immediately following this note.

**Recall**: For any \( n \in \mathbb{N} \) and field \( F \), we know \( \{ \alpha \in F \mid \alpha^n = 1 \} \) is a cyclic subgroup of \( F^* \) by Corollary 63.

**Definition**: Let \( n \in \mathbb{N} \) and \( \alpha \in F \). We say \( \alpha \) is a **primitive nth root of unity** if \( \alpha \) generates all of the distinct roots of the polynomial \( x^n - 1 \).

**Note 1**: 1 is a primitive 1st root of unity. For the rest of our discussion we’ll assume \( n > 1 \).

**Note 2**: For any \( n \) and field \( F \), there is an extension \( E/F \) containing a primitive \( nth \) root of unity. That is, for any field, we can find a primitive \( nth \) root of unity [in a field] over \( F \).

**Note 3**: Let \( \text{char}(F) = p \) and \( \alpha \) be a primitive \( nth \) root of unity over \( F \).

- If \( p = 0 \) or \( p \) does not divide \( n \), then \( x^n - 1 \) has exactly \( n \) distinct roots and \( |<\alpha>| = n \).
- If \( p \) divides \( n \), write \( n = p^m d \) where \((d,p) = 1\). Then \( x^n - 1 \) has exactly \( d \) distinct roots and \( |<\alpha>| = d \).

This is an important observation and will be used to adjust many of Rotman’s statements. In particular, note that any primitive 12th root of unity over a field of characteristic 3 is actually a primitive 4th root of unity. Also, 1 is the primitive 8th root of unity in any field having characteristic 2.

**Theorem 69’**: Let \( F \) be a field with \( \text{char}(F) = p \) and \( E = F(\alpha) \) where \( \alpha \) is a primitive \( nth \) root of unity [over \( F \)]. Letting \( G \) denote \( \text{Gal}(E/F) \) we have

(i) If \( p = 0 \) or \( p \) does not divide \( n \), then \( G \) is isomorphic to a subgroup of \( U(\mathbb{Z}_n) \).
(ii) If \( p \) divides \( n \), write \( n = p^m d \). Then \( G \) is isomorphic to a subgroup of \( U(\mathbb{Z}_d) \).

In either case, we see \( G \) is an abelian group.
Proof: (i) Note $E = F(\alpha)$ is a splitting field for the polynomial $f(x) = x^n - 1$. Let $q(x)$ denote the irreducible polynomial of $\alpha$ in $F[x]$. Since $q(x)$ must divide $f(x)$, we know that $r = \partial(q) \leq n$. Further $\{1, \alpha, \ldots, \alpha^r\}$ is a basis for $E$ over $F$.

Now, since $\{1, \alpha, \ldots, \alpha^r\}$ is a basis for $E$ over $F$, we see that any $\sigma \in \text{Gal}(E/F)$ is completely determined by $\sigma(\alpha)$. But $\sigma$ permutes the $n$ roots of unity in $E$, which are all generated by $\alpha$, so $\sigma(\alpha) = \alpha^i$ for a unique $i$ modulo $n$. But since $\langle \sigma(\alpha) \rangle = \langle \alpha \rangle$, $\alpha^i$ must be a generator of $\langle \alpha \rangle$. Thus $(i, n) = 1$. With this, we have a well-defined function $\psi: \text{Gal}(E/F) \to U(\mathbb{Z}_n)$. Note $\psi$ is a homomorphism to this multiplicative group and it’s injective by Exercise 73.

For (ii) replace every “$n$” in the argument with “$d$.”

Note: To see that Rotman’s proof is flawed as presented, consider $p = 3$, $n = 12$ and the proof’s second sentence (p.68). Since $\alpha$ is actually a 4th root of unity, $\alpha^3 = \alpha^9$. However $[5] \neq [9] \mod 12$! The upshot would be, in this case, that one could not construct a well-defined function to $U(\mathbb{Z}_{12})$. However, everything is fine if we work modulo 4.

Example 27: As per Rotman, noting that the $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic of order $p - 1$.

Theorem 70': Let $F$ be a field with $\text{char}(F) = p$; $\alpha \in F$ a primitive $n$th root of unity; $f(x) = x^n - c \in F[x]$; and $E/F$ a splitting field of $f(x)$ over $F$. Letting $G$ denote $\text{Gal}(E/F)$ we have:

(i) If $p = 0$ or $p$ does not divide $n$, then there is an injection $\varphi: G \to (\mathbb{Z}_n, +)$.
(ii) If $p$ divides $n$, write $n = p^md$. Then there is an injection $\varphi: G \to (\mathbb{Z}_d, +)$.

In case (i): $f(x)$ is irreducible if and only if $\varphi$ is surjective.
In case (ii): If $f(x)$ is irreducible, then $\varphi$ is surjective.

Proof: (i) As per Rotman. For (ii) again replace “$n$” by “$d$.”

Note: Once again Rotman’s presentation is flawed if $p = 3$ and $n = 12$, as the function he wants to construct is not well-defined in this case. Also check that $F = \mathbb{Z}_3$ and $f(x) = x^3 - 2$ can be used to show that the converse of the last statement is false.

Corollary 71': Let $p$ be a prime; let $F$ be a field with $\text{char}(F) \neq p$ and containing a primitive $p$th root of unity; and let $f(x) = x^n - c \in F[x]$ with splitting field $E$. Then either $f(x)$ splits in $F[x]$ and $\text{Gal}(E/F) = 1$ or it is irreducible and $\text{Gal}(E/F)$ is isomorphic to $\mathbb{Z}_p$.

Proof [adapted from Rotman]: First note that since $\text{char}(F)$ does not divide $p$ we have an injective map $\text{Gal}(E/F) \to (\mathbb{Z}_p, +)$ by Theorem 70'. If $f(x)$ splits, then $E = F$
and \( \text{Gal}(E/F) = 1 \). So we may assume \( f(x) \) does not split. Note that \( f(x) \) is separable in \( F[x] \) (since \( (f(x), f'(x)) = 1 \), \( f(x) \) has no repeated roots in \( E \)). Thus, by Theorem 56, \( |\text{Gal}(E/F)| = [E:F] > 1 \). Thus the image of the map is a non-trivial subgroup of \( \mathbb{Z}_p \). But \( \mathbb{Z}_p \) has no proper non-trivial subgroups, so the map must be surjective and \( f(x) \) must be irreducible.

Note: If one omits the underlined hypothesis above, the statement is false. Here’s a counterexample that relates to Example 21. Let \( F = \mathbb{Z}_p(t) \) and consider \( f(x) = x^p - t \in F[x] \). Note that 1 is a primitive pth root of unity in \( F \). [In any field of characteristic \( p \), there is only one pth root of unity!] Letting \( E \) denote the splitting field of \( f(x) \), we have seen \( f(x) = (x - t^{1/p})^p \) in \( E[x] \). That is \( f(x) \) has only one [repeated] root in \( E: t^{1/p} \). Consequently \( |\text{Gal}(E/F)| = 1 \) by Theorem 55 (since \( \text{Gal}(E/F) \) has to be isomorphic to a subgroup of \( S_1 \), the trivial group).

We see that \( f(x) \) is irreducible in \( F[x] \), so it can’t split, yet \( \text{Gal}(E/F) \) is not isomorphic to \( \mathbb{Z}_p \).

Corollary 72: As per Rotman.

Ironically, Rotman correctly observes this proof can be adapted to handle the case where \( \text{char}(F) \) does not divide \( p \). He should have observed this important condition in his other theorems!