Computational Algebra: Lecture 8 Exercise

Manuel Arcedo Saiz

Exercise: Prove that for a prime power q and $n \in \mathbb{N}$ with $\gcd(q, n) = 1$, a finite field $\mathbb{F}_q$ with q elements contains a primitive nth root of the unity if and only if n divides $q-1$.

P/ First of all, we can note that $\mathcal{U}^{(n)}$ (the set of all nth roots of the unity in $\mathbb{F}_q$) is a subgroup under $\cdot$. In fact, suppose $\alpha, \beta \in \mathcal{U}^{(n)}$ $(\alpha\beta)^n = \alpha^n \beta^n$ and $(\alpha^{-1})^n = (\alpha^n)^{-1} = 1$. Moreover, if n not a unit in $\mathbb{F}_q$ being a primitive nth root of the unity and having $w^l \neq 1$ for $0 < l < n$ (equivalently having order n) are equivalent statements since a field does not contain zero divisors.
Furthermore, ~~[illegible]~~ $\varphi: \mathbb{Z}_n \to \mathcal{U}^{(n)}$, $m \mapsto w^m$ defines an isomorphism, since by the latter, being w a nth primitive root implies φ to be injective and by def $w \in \mathcal{U}^{(n)}$ is a solution (root) of $x^n - 1$ which will have at most n and thus φ surjective too.

1 – Therefore, $\mathcal{U}^{(n)} = \langle x \rangle$ cyclic subgroup of order n. Moreover, we are going to use the classical fact that ~~under the hypothesis~~ $\mathbb{F}_q^*$ is a cyclic group of order $q-1$ under multiplication. By Lagrange's theorem $|\mathcal{U}^{(n)}| \mid |\mathbb{F}_q^*| \Rightarrow n \mid q-1$. (Recall that we were assuming n ~~[illegible]~~ to be a unit) $\circledast$

2 – Moreover if ~~[illegible]~~ $n \mid q-1$ $n \leq q-1$ and so $\exists m \in \mathbb{N}$ st $q-1 = nm$, and so since $\mathbb{F}_q^* = \langle x \rangle$ is cyclic of order $q-1$, x^m is going to be an nth ~~prim~~ root of the unity in $\mathbb{F}_q^*$ and by the equivalence mentioned above a nth primitive root of the unity (n is a unit since $n \mid q-1$).

$\circledast$ n not a unit in $\mathbb{F}_q \Rightarrow \operatorname{char}(\mathbb{F}_q) \mid n$, say ~~[illegible]~~ $\exists m \in \mathbb{N}$, $m < n$ st $n = cm$. Suppose $w \in \mathbb{F}_q$ nth root of the unity then $(w^m - 1)^c = w^n - 1 = 0$ so $w^m - 1$ is a zero div and not a primitive nth root of unity. Therefore in 1 assuming ~~not~~ the existence of nth primitive root of unity implies n unit, so this solves our assumption $\circledast$