Error-Correcting Codes: Existence of generators

LEMMA Let $\alpha \in GF(q)^*$ with $\text{ord}(\alpha) = t$. Then $\text{ord}(\alpha^i) = t/\gcd(t,i)$.

Proof. Let $d = \gcd(t,i)$. The order of α^i is the smallest positive integer s such that $\alpha^{is} = 1$. Now,

$$\alpha^{is} = 1 \;\Leftrightarrow\; t \mid is \;\Leftrightarrow\; \frac{t}{d} \mid \frac{i}{d}s \;\Leftrightarrow\; \frac{t}{d} \mid s.$$

Since the smallest positive integer s satisfying $\frac{t}{d} \mid s$ is $s = \frac{t}{d}$, we have $\text{ord}(\alpha^i) = \frac{t}{d}$. $\square$

LEMMA Let $\alpha, \beta \in GF(q)^*$, with $\text{ord}(\alpha) = m$ and $\text{ord}(\beta) = n$. If $\gcd(m,n) = 1$ then $\text{ord}(\alpha\beta) = mn$.

Proof. Let $t = \text{ord}(\alpha\beta)$. Now,

$$(\alpha\beta)^{mn} = \alpha^{mn}\beta^{mn} = 1,$$

so $t \mid mn$. Also,

$$1 = (\alpha\beta)^{tn} = \alpha^{tn}\beta^{tn} = \alpha^{tn},$$

so $m \mid tn$. And, since $\gcd(m,n) = 1$, we have $m \mid t$. Similarly,

$$1 = (\alpha\beta)^{tm} = \alpha^{tm}\beta^{tm} = \beta^{tm},$$

so $n \mid tm$. And, since $\gcd(m,n) = 1$, we have $n \mid t$. Hence, since $\gcd(m,n) = 1$, we have $mn \mid t$. Thus $t = mn$. $\square$

THEOREM Every finite field $GF(q)$ has a generator.

Proof. Let α be an element of highest order in $GF(q)^*$; say $\text{ord}(\alpha) = t$. Suppose that $t < (q-1)$.
If the order of every element in $GF(q)^*$ were to divide t then the equation $y^t - 1 = 0$ would have $q-1$ roots in $GF(q)$, which is impossible since $(q-1) > t$. Hence there exists an element $\beta \in GF(q)^*$ whose order b does not divide t.
Now, let ℓ be a prime such that the highest power of ℓ which divides b (say ℓ^e) is greater than the highest power of ℓ which divides t (say ℓ^f) — such a prime ℓ must exist since b does not divide t.
Consider the field elements $\alpha' = \alpha^{\ell^f}$ and $\beta' = \beta^{b/\ell^e}$. We have

$$\text{ord}(\alpha') = \frac{t}{\gcd(t,\ell^f)} = \frac{t}{\ell^f}$$

and

$$\text{ord}(\beta') = \frac{b}{\gcd(b, b/\ell^e)} = \frac{b}{b/\ell^e} = \ell^e.$$

Since $\gcd(t/\ell^f, \ell^e) = 1$, we have $\text{ord}(\alpha'\beta') = (t/\ell^f)(\ell^e) = t\ell^{e-f} > t$. This contradicts the hypothesis that the highest order of any element in $GF(q)^*$ is t. Hence the hypothesis that $t < (q-1)$ is wrong, and so $t = q-1$. Thus α is a generator of $GF(q)^*$. $\square$