Theorem 4.15 *The unit group of any finite field $\mathbb{F}_{p^n}$ (with p a prime) is cyclic of order $p^n - 1$. So $\mathcal{U}(\mathbb{F}_{p^n}) \cong C_{p^n-1}$. So any element of $\mathbb{F}_{p^n}$ has (multiplicative) order dividing $p^n - 1$.*

Example 4.16 *Consider $\mathbb{F}_5$. $1 = 1$. $2^2 = 4$, $2^3 = 3$, $2^4 = 1$. $3^2 = 4$, $3^3 = 2$, $3^4 = 1$. $4^2 = 1$. Therefore the elements of $\mathcal{U}(\mathbb{F}_5)$ have order $1, 4, 4, 2$. These all divide $5 - 1 = 4$.*

Thus $\mathcal{U}(\mathbb{F}_3C_2) \cong \mathcal{U}(\mathbb{F}_3) \times \mathcal{U}(\mathbb{F}_3) = C_2 \times C_2$ or $\mathcal{U}(\mathbb{F}_3C_2) \cong \mathcal{U}(\mathbb{F}_{3^2}) = C_{3^2-1} = C_8$. However (by homework 1) $\mathcal{U}(\mathbb{F}_3C_2) \cong C_2 \times C_2$. So $\mathbb{F}_3C_2 \not\cong \mathbb{F}_{3^2}$ so

$$\mathbb{F}_3C_2 \cong \mathbb{F}_3 \oplus \mathbb{F}_3$$

(Alternatively, note that $\mathcal{U}(\mathbb{F}_3C_2)$ and $\mathbb{F}_3 \oplus \mathbb{F}_3$ contain zero divisors but $\mathbb{F}_{3^2}$ does not).

Theorem 4.17 *Let G be a finite group and K a field such that char $K \nmid |G|$. Then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i) \cong K \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i)$$

(i.e. the field itself appears at least once as a direct summand in the Wedderburn-Artin decomposition).

Proof. Later ■

Lemma 4.18 *Let K be a finite field. Then if char $K \nmid |G| < \infty$, then*

$$KG \cong \oplus_{i=1}^{s} M_{n_i}(K_i)$$

where the K_i are fields (i.e. all the division rings appearing are fields).

Proof. Clearly $KG \cong \oplus_{i=1}^{s} M_{n_i}(D_i)$ where the D_i are division rings. But D_i is a division ring such that $dim_K D_i < \infty$ (since G is finite). Now Wedderburn's theorem implies that D_i must be a field. ■

Example 4.19 *Consider $\mathbb{F}_5S_3$. $\mathbb{F}_5S_3 \cong \oplus_{i=1}^{s} Mn_i(D_i) \cong \mathbb{F}_5 \oplus \oplus_{i=1}^{s-1} M_{n_i}(D_i) \cong \mathbb{F}_5 \oplus \oplus_{i=1}^{s-1} M_{n_i}(K_i)$.*