

$C_3 = \{1, x, x^2\}$. $\mathbb{F}_2C_3 = \{a.1 + b.x + c.x^2 \mid a, b, c \in \mathbb{F}_2\}$. There are 2 choices for $a \in \{0, 1\}$, 2 choices for $b \in \{0, 1\}$ and there are 2 choices for $c \in \{0, 1\}$ so there are $2 \cdot 2 \cdot 2 = 8$ elements in \mathbb{F}_2C_3 .

Now $3 \leq |\mathbb{F}_2C_3| \leq 8$ and $C_3 \triangleleft \mathcal{U}(\mathbb{F}_2C_3)$. By Lagrange's theorem $|C_3|$ divides $|\mathcal{U}(\mathbb{F}_2C_3)|$ so $3 \mid |\mathcal{U}(\mathbb{F}_2C_3)|$ and $|\mathcal{U}(\mathbb{F}_2C_3)| \leq 8$, therefore $|\mathcal{U}(\mathbb{F}_2C_3)| = 3$ or 6 .

Lemma 1.35 *Let R be a ring of order m and G a group of order n . Then RG is a finite group ring of size $|R|^{|G|} = m^n$.*

Proof. $RG = \{\sum_{g \in G} a_g g \mid a_g \in R\}$. For each g , there are m choices for a_g . So there are $\underbrace{m \cdot m \cdot \dots \cdot m}_{|G|=n}$ -elements in RG . i.e. $m^n = |R|^{|G|}$. ■

Example 1.36 $|\mathbb{F}_2C_2| = |\mathbb{F}_2|^{|C_2|} = 2^2 = 4$. The group $(\mathbb{F}_2C_2, +)$ has order 4 so it is isomorphic to either C_4 or $C_2 \times C_2$. If $a \in \mathbb{F}_2C_2$, then $2.a = 0.a = 0$. So every element of \mathbb{F}_2C_2 has order ≤ 2 . Thus $\mathbb{F}_2C_2 \not\cong C_4$ (since C_4 has an element of order 4). $\therefore (\mathbb{F}_2C_2, +) \cong C_2 \times C_2$ (Klein-4-group).

Question : Is $\mathbb{F}_2C_2 \cong \mathbb{Z}_4$ (isomorphic as rings) ? **Answer :** No. What is the additive group of \mathbb{Z}_4

\mathbb{Z}_4				
+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

So $(\mathbb{Z}_2, +) \cong C_2$

Thus \mathbb{F}_2C_2 and \mathbb{Z}_4 have non-isomorphic additive groups. So they are not