Exercise [16.05]

An element ε of a finite field $\mathbb{F}_n$ with the property that the sequence $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-2}$ enumerates all elements of the field except 0 (and repeats for higher powers, i.e. $\varepsilon^{n-1}=1$) is called a *primitive element* (or a *generator* of the multiplicative group of the field). By expressing each nonzero element of the field as a power of ε, multiplication can be reduced to addition (of powers) modulo n-1. It is known that all finite fields have at least one primitive element. (I won't prove it here).

In the case of $\mathbb{F}_8$, $n-1=7$ is prime, and in that case, *all* elements except 0 and 1 are primitive. To see this, either manually check that the sequences $\varepsilon^n, (\varepsilon^2)^n, \ldots, (\varepsilon^6)^n$ (for $n=1$ through 6 in each case) each enumerate the same set of elements (just in different orders), or else note that the numbers 2 through 6 are all relatively prime to 7, and see my solution to [16.04].

To solve this exercise, though, we need to *both add and multiply* elements of $\mathbb{F}_8$, which means we need a complete specification of this field. In the text, we are using $\mathbb{F}_8$ as a field derived from the vector space $\mathbb{F}_2\times\mathbb{F}_2\times\mathbb{F}_2$. Addition in this space is defined as usual for vector addition; it is the multiplication rule that we must define to turn this space into a field… and component-wise multiplication *doesn't* work. (Consider, e.g.: $(0,0,1)\times(1,0,0)$ which would give $(0,0,0)$).

When we added an extra element **i** to the reals $\mathbb{R}$, we obtained $\mathbb{C}$, isomorphic to $\mathbb{R}^2$ under addition. Similarly, if we extend the rational numbers $\mathbb{Q}$ by appending the cube root of 2 to them, we get the number system:

$$\{x(\sqrt[3]{2})^2 + y(\sqrt[3]{2}) + z:\quad x, y, z \in \mathbb{Q}\}$$

isomorphic to $\mathbb{Q}^3$ under addition. In both cases, addition and multiplication rules follow logically from the definition of the appended element. So to find a "multiplication rule" for the vector space $(\mathbb{F}_p)^n$ that turns it into the field $\mathbb{F}_{p^n}$ (where p must be prime), we simply extend $\mathbb{F}_p$ by appending some element $\sigma \notin \mathbb{F}_p$ with the property that $\sigma, \sigma^2, \ldots, \sigma^{n-1}$ are all linearly independent non-elements of $\mathbb{F}_p$, but where σ^n is not. i.e. where σ is a solution of some polynomial equation:

$$\sigma^n + a_{n-1}\sigma^{n-1} + \ldots + a_2\sigma^2 + a_1\sigma + a_0 \;=\; 0 \qquad\qquad a_i \in \mathbb{F}_p$$

with no solution in $\mathbb{F}_p$, and where the LHS can't be factorized into any smaller polynomials with coefficients in $\mathbb{F}_p$ (i.e. the LHS is a polynomial that is *irreducible* over $\mathbb{F}_p$). (Not being factorizable guarantees all powers of σ less than n are linearly independent). *Any* such polynomial will do, and it is always possible to find one. Then we can interpret a vector $(x_0, x_1, \ldots, x_{n-1})$ in $(\mathbb{F}_p)^n$ as the element:

$$x_0 + x_1\sigma + \ldots + x_{n-1}\sigma^{n-1}$$

of our "extended" number system. Addition and multiplication are defined accordingly. Addition is just componentwise (vector) addition, and multiplication is just the same as normal polynomial multiplication, after which we get rid of higher powers of σ by repeated substitution of:

$$\sigma^n \;=\; -a_{n-1}\sigma^{n-1} - \ldots - a_2\sigma^2 - a_1\sigma - a_0$$

Note that although there is only one finite field $\mathbb{F}_{p^n}$ for each choice of n and (prime) p, different choices of irreducible polynomial may result in different multiplication rules for the particular vector representation being used. These different representations of $\mathbb{F}_{p^n}$ will all be isomorphic to each other, however. For an example of what this means, swapping the positions of the first two components in each vector would also yield one such isomorphism, as a different multiplication rule would result.

Now back to the particular problem at hand: Defining a multiplication rule on $(\mathbb{F}_2)^3$ to turn it into $\mathbb{F}_8$. We need to find an order 3 irreducible polynomial over $\mathbb{F}_2$. Given that the only possible coefficients are 0 and 1, this is very easy to do by inspection. There are only two:

$$\sigma^3 + \sigma + 1 \qquad \text{and} \qquad \sigma^3 + \sigma^2 + 1$$

(Obviously neither 0 nor 1 is a root of either of these, as they evaluate to 1 when σ is set to either value). Using the first polynomial gives us the simplification rule: $\sigma^3 = \sigma + 1$

(Uniquely in $\mathbb{F}_2$ we have $+1=-1$, so there's no minus signs when we rearrange the equation!)

This rule allows us to define multiplication as follows:

$(a_0, a_1, a_2) \times (b_0, b_1, b_2)$

$= (a_0b_0) + (a_0b_1+a_1b_0)\sigma + (a_1b_1+a_0b_2+a_2b_0)\sigma^2 + (a_1b_2+a_2b_1)\sigma^3 + (a_2b_2)\sigma^4$

$= (a_0b_0+a_1b_2+a_2b_1) + (a_0b_1+a_1b_0+a_1b_2+a_2b_1+a_2b_2)\sigma + (a_1b_1+a_0b_2+a_2b_0+a_2b_2)\sigma^2$ (applying the rule)

$= (a_0b_0+a_1b_2+a_2b_1,\ \ a_2b_2+a_0b_1+a_1b_0+a_1b_2+a_2b_1,\ \ a_1b_1+a_2b_2+a_0b_2+a_2b_0)$

(Note that if we'd chosen the 2nd polynomial, we'd have gotten

$(a_0b_0+a_2b_2+a_1b_2+a_2b_1,\ \ a_2b_2+a_0b_1+a_1b_0,\ \ a_1b_1+a_2b_2+a_0b_2+a_2b_0+a_1b_2+a_2b_1)$ instead).

Hence:

$(a_0, a_1, a_2)^2 = (a_0,\ \ a_2,\ \ a_1+a_2)$

$(a_0, a_1, a_2)^3 = (a_0+a_1+a_2+a_1a_2,\ \ a_1+a_0a_1+a_0a_2,\ \ a_2+a_0a_1)$

$(a_0, a_1, a_2)^4 = (a_0,\ \ a_1+a_2,\ \ a_1)$

$(a_0, a_1, a_2)^5 = (a_0+a_1+a_2+a_1a_2,\ \ a_1+a_2+a_0a_2,\ \ a_1+a_0a_1+a_0a_2)$

$(a_0, a_1, a_2)^6 = (a_0+a_1+a_2+a_1a_2,\ \ a_2+a_0a_1,\ \ a_1+a_2+a_0a_2)$

$(a_0, a_1, a_2)^7 = (a_0+a_1+a_2+a_0a_1+a_0a_2+a_1a_2+a_0a_1a_2,\ \ 0,\ \ 0)$

Note that $(a_0, a_1, a_2)^7$ is $(0,0,0)$ if $a_0=a_1=a_2=0$, and $(1,0,0)$ otherwise, as expected.

Now, the problem asks us to prove that for each primitive element ε of $\mathbb{F}_8$, one of the following two identities holds:

$$\varepsilon^a+\varepsilon^b+\varepsilon^c = 0 \qquad \text{or} \qquad \varepsilon^{3a}+\varepsilon^{3b}+\varepsilon^{3c} = 0$$

where a, b, c are any three numbers pointed to by the magic disk's arrows. We can divide each equation by its leftmost term; then (w.l.o.g) taking a, b, c anticlockwise from the right of the figure as shown, we have the constants $(b-a)=1$, $(c-a)=3$ (mod 7) irrespective of the disk's rotation, and (using the fact that $\varepsilon^7=1$) the identities thus become:

$$1+\varepsilon+\varepsilon^3 = 0 \qquad \text{or} \qquad 1+\varepsilon^3+\varepsilon^2 = 0$$

Using the vector representation of $\mathbb{F}_8$ just derived, these equations become:

(A) $((a_1+1)(a_2+1),\ a_0(a_1+a_2),\ a_0a_1) \ = \ (0,0,0)$

or

(B) $((a_1+1)(a_2+1),\ (a_0+1)(a_1+a_2),\ (a_0+1)a_1) \ = \ (0,0,0)$

By inspection, (A) holds for $\varepsilon = (0,1,0)$, $(0,0,1)$, or $(0,1,1)$, and (B) holds for $\varepsilon = (1,1,0)$, $(1,0,1)$, or $(1,1,1)$; the other two elements of $\mathbb{F}_8$ in this representation are $(0,0,0)$ and $(1,0,0)$, but they are not primitive elements (they are 0 and 1 respectively). Thus one of the two identities given holds for each primitive element of $\mathbb{F}_8$, as required, and the exercise is complete.

■