Notes[1]

For any integer $n \geq 1$ we can make the "integers modulo n", which I call $\mathbb{Z}_n$. The elements of $\mathbb{Z}_n$ are $\{0, \ldots, n-1\}$. For example, $\mathbb{Z}_{10} = \{0, \ldots, 9\}$.

$\mathbb{Z}_n$ has operations of $+$, $-$, and $\cdot$, which I'll explain below. These operations have the properties you have come to expect—all the field properties except the existence of multiplicative inverses.

However, if n is prime, then you *do* get multiplicative inverses. So there is a finite field of each prime size p, namely $\mathbb{Z}_p$. In other words, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, etc., are fields.

A more general fact is that there is one finite field of each prime-power size, called the Galois field of that size, or $\mathrm{GF}(p^n)$. So $\mathrm{GF}(p) = \mathbb{Z}_p$.

Focus on one integer n. To understand $+$, $-$ and $\cdot$ in $\mathbb{Z}_n$, it's helpful first to get used to "congruences modulo n". (n is called the *modulus.*) We say that two integers a, b are *congruent modulo* n if n divides their difference $a - b$. In other words, they are a multiple of n apart. In that case we write $a \equiv b \pmod{n}$. For example, if we have chosen $n = 10$, then $4 \equiv 24 \pmod{10}$ and also $4 \equiv -6 \pmod{10}$. Congruences are important because when you stick to one modulus, congruences have nice compatibility with $+$, $-$, and $\cdot$ (which we won't go into now).

For addition, subtraction, and multiplication in $\mathbb{Z}_n$, do the operation in $\mathbb{Z}$ first. If the answer is outside the range $0, \ldots, n-1$, replace the answer by the integer in that range that is congruent to the answer modulo n.

So in $\mathbb{Z}_{10}$, $6 + 7 = 3$, $6 - 7 = 9$, and $6 \cdot 7 = 2$. In the case $n = 10$, for $+$ and $\cdot$, this is the same as writing out an addition or multiplication and then erasing all digits of the answer except the last one. (If you are familiar with number bases, for other values of n, working in Z_n is the same as working with last digits in base n.)

You will find that $\mathbb{Z}_{10}$ is *not* a field: If you look for multiplicative inverses, you will find that only the elements $1, 3, 7, 9$ have them (the elements with no factor of 2 or 5).

$\mathbb{Z}_{12}$ is also not a field, but the operations of addition and subtraction are the familiar "clock arithmetic", as when you ask what time is 7 hours ahead of 6:00. (But instead of 12 we should write 0, to be within the range $0, \ldots, 11$.)

$\mathbb{Z}_{11}$ *is* a field, since 11 is prime. For example, the multiplicative inverse of 5 is 9, since $5 \cdot 9 = 45 \equiv 1 \pmod{11}$.

[1] Originally posted after lecture 1-M, October 1. This version is slightly edited.

Your homework problem about $\{0,1\}$ is really talking about $\mathbb{Z}_2$. Here all the even integers are congruent to each other modulo 2, and all the odd integers are congruent to each other modulo 2.