Tutorial 1 – Algebra 2019

The field with nine elements is obtained from $\mathbb{Z}$ in two steps: first, take the quotient by the equivalence relation generated by $3 \sim 0$, then adjoin the imaginary number i subject to the relation $i \times i = -1$. We will make proper sense of this with a formal definition in class. For now, play around with these rules to fill in the addition and multiplication table for the field with nine elements.

$+$	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
0	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
1	1	2	0	$i+1$	$i+2$	i	$2i+1$	$2i+2$	$2i$
2	2	0	1	$i+2$	i	$i+1$	$2i+2$	$2i$	$2i+1$
i	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$	0	1	2
$i+1$	$i+1$	$i+2$	i	$2i+1$	$2i+2$	$2i$	1	2	0
$i+2$	$i+2$	i	$i+1$	$2i+2$	$2i$	$2i+1$	2	0	1
$2i$	$2i$	$2i+1$	$2i+2$	0	1	2	i	$i+1$	$i+2$
$2i+1$	$2i+1$	$2i+2$	$2i$	1	2	0	$i+1$	$i+2$	i
$2i+2$	$2i+2$	$2i$	$2i+1$	2	0	1	$i+2$	i	$i+1$

$\times$	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
2	0	2	1	$2i$	$2i+2$	$2i+1$	i	$i+2$	$i+1$
i	0	i	$2i$	2	$i+2$	$2i+2$	1	$i+1$	$2i+1$
$i+1$	0	$i+1$	$2i+2$	$i+2$	$2i$	1	$2i+1$	2	i
$i+2$	0	$i+2$	$2i+1$	$2i+2$	1	i	$i+1$	$2i$	2
$2i$	0	$2i$	i	1	$2i+1$	$i+1$	2	$2i+2$	$i+2$
$2i+1$	0	$2i+1$	$i+2$	$i+1$	2	$2i$	$2i+2$	i	1
$2i+2$	0	$2i+2$	$i+1$	$2i+1$	i	2	$i+2$	1	$2i$

Familiarize yourself with the field axioms for instance here: `http://people.reed.edu/~mayer/math112.html/html1/node16.html` and check that they hold for the tables you wrote down. Which ones have (consciously or unconciously) influenced your construction? Probably all of them apart from the existence of units, which were already given in $\mathbb{Z}$, and inverses. Which is the hardest to check? Typically the existence of multiplicative inverses. These can be read off from the multiplication table and account for the fact that each of its non-zero rows and each columns contains every element exactly once.

There is an element $\alpha \neq 0$ whose powers give all the non-zero elements. Find α and compute its powers. There are two choices:

α	α^2	α^3	α^4	α^5	α^6	α^7	α^8
$i+1$	$2i$	$2i+1$	2	$2i+2$	i	$i+2$	1

and $i+2 = (i+1)^{-1}$. For each number n from zero to ten, decide whether or not a field with n elements exists. If the answer is "yes", construct this field.

(1) No such field, since $0 \neq 1$ implies that any field contains at least two distinct elements.

(2) The field with two elements, $\mathbb{F}_2$, is isomorphic to the ring $\mathbb{Z}/2\mathbb{Z}$,

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

(3) The field with three elements, $\mathbb{F}_3$, is isomorphic to the ring $\mathbb{Z}/3\mathbb{Z}$,

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(4) The field with two elements, $\mathbb{F}_4$, is not isomorphic to the ring $\mathbb{Z}/4\mathbb{Z}$ – the latter has zero divisors. It turns out that the additive group needs to be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the tables are constructed explicitly as:

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\times$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

This was a bit harder but still feasible just by playing around from first principles.

(5) The field with five elements, $\mathbb{F}_5$, is isomorphic to the ring $\mathbb{Z}/5\mathbb{Z}$.

(6) There is no field with six elements: the only abelian group with six elements is $\mathbb{Z}/6bbZ$ with the usual addition. Playing around with the axioms, you can see that once the additive group is cyclic, the multiplication is forced to be the multiplication inherited from $\mathbb{Z}$. Again, there are zero divisors.

(7) The field with seven elements, $\mathbb{F}_7$, is isomorphic to the ring $\mathbb{Z}/7\mathbb{Z}$,

(8) Up to isomorphism, there is one field with eight elements, and I will be impressed if you managed to construct it from first principles. Here it is:

$+$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
1	1	0	$b+1$	b	b^2+1	b^2	b^2+b+1	b^2+b
b	b	$b+1$	0	1	b^2+b	b^2+b+1	b^2	b^2+1
$b+1$	$b+1$	b	1	0	b^2+b+1	b^2+b	b^2+1	b^2
b^2	b^2	b^2+1	b^2+b	b^2+b+1	0	1	b	$b+1$
b^2+1	b^2+1	b^2	b^2+b+1	b^2+b	1	0	$b+1$	b
b^2+b	b^2+b	b^2+b+1	b^2	b^2+1	b	$b+1$	0	1
b^2+b+1	b^2+b+1	b^2+b	b^2+1	b^2	$b+1$	b	1	0

$\times$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	0	0	0	0	0	0	0
1	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
b	0	b	b^2	b^2+b	$b+1$	1	b^2+b+1	b^2+1
$b+1$	0	$b+1$	b^2+b	b^2+1	b^2+b+1	b^2	1	b
b^2	0	b^2	$b+1$	b^2+b+1	b^2+b	b	b^2+1	1
b^2+1	0	b^2+1	1	b^2	b	b^2+b+1	$b+1$	b^2+b
b^2+b	0	b^2+b	b^2+b+1	1	b^2+1	$b+1$	b	b^2
b^2+b+1	0	b^2+b+1	b^2+1	b	1	b^2+b	b^2	$b+1$

(9) You constructed the field with nine elements above. It is unique up to (non-unique) isomorphism.

(10) The same argument we used for six shows that there is no field with ten elements.