Math 3140 — Fall 2012

Handout #16

Exercise 1. Is there is a field with 6 elements?

Solution. Suppose that F is a field with 6 elements. Then consider the element $1 \in F$. Let $E \subset F$ be the set of all integer multiples of 1. If $a \cdot 1, b \cdot 1 \in E$ then $a \cdot 1 + b \cdot 1 = (a+b) \cdot 1$ and $a \cdot 1 - b \cdot 1 = (a-b) \cdot 1$ and $ab \cdot 1 = (a \cdot 1)(b \cdot 1)$ are all in E. Therefore E is a ring.

Since F is finite, there must be a smallest n such that $n \cdot 1 = 0$ in F. (Here is the reason: eventually we must have $n \cdot 1 = m \cdot 1$ so $(n-m) \cdot 1 = 0$.) Therefore $E \cong \mathbf{Z}/n\mathbf{Z}$. But if n is not prime then we could find two factors a and b of n. Then $(a \cdot 1)(b \cdot 1) = 0$ in E. This means that E contains zero divisors. But E is contained in F so this means F also contains zero divisors, so F can't be a field.

The n that appeared above is the order of 1 in the additive group of F. Since F has 6 elements, this means that n must be a divisor of 6. Therefore F contains either $\mathbf{F}_2$ or $\mathbf{F}_3$.

Suppose that F contains $\mathbf{F}_3$. Pick some $x \in F$ that is not in $\mathbf{F}_3$. Then consider all of the elements of F of the form $ax + b$ with $a, b \in \mathbf{F}_3$. There are 9 expressions like this and only 6 elements in F, so we must have $ax + b = a'x + b'$ for some choices of $a, b \in \mathbf{F}_3$ and $a', b' \in \mathbf{F}_3$. But then $(a - a')x + (b - b') = 0$, which means $x = -(a-a')^{-1}(b-b')$. But that means $x \in \mathbf{F}_3$: contradiction!

Now suppose that F contained $\mathbf{F}_2$. Pick some $x \in F$ that is not in $\mathbf{F}_2$. Then look at all $a + bx \in F$ with $a, b \in \mathbf{F}_2$. There can only be 4 of these and F has 6 elements, so there must be some $y \in \mathbf{F}_2$ that can't be expressed as $a + bx$ for any $a, b \in \mathbf{F}_2$. Then look at all $a + bx + cy \in F$ with $a, b, c \in \mathbf{F}_2$. There are 8 such expressions and 6 elements, so there must be two choices a, b, c and a', b', c' in $\mathbf{F}_2$ with

$$a + bx + cy = a' + b'x + c'y.$$

Then

$$(a - a') + (b - b')x + (c - c')y = 0.$$

We can't have $c = c'$, because then $x = -(b-b')^{-1}(a-a')$ is in $\mathbf{F}_2$. But then $y = (c-c')^{-1}(a-a') + (c-c')^{-1}(b-b')x$ can be expressed as a combination of 1 and x. Either way, it's a contradiction! $\square$