FIELDS – MATH 5405
SPRING 2016

Recall a *field* is a commutative ring with unity where every element has a multiplicative inverse ($aa^{-1} = 1$). Recall the following result from class.

Lemma: *Suppose R is an integral domain[1] with finitely many elements. Then R is a field.*

Proof. Suppose $0 \neq x \in R$. Consider the set $\{x, x^2, x^3, \ldots\} \subseteq R$. This set must have some repeats since R has finitely many elements. Suppose $m > n \geq 1$ and $x^m = x^n$. Then

$$x^n \cdot x^{m-n} = x^m = x^n = x^n \cdot 1$$

and so $x^{m-n} = 1$ by the cancellation property for integral domains. But now

$$xx^{m-n-1} = 1$$

and so $x^{m-n-1} = x^{-1}$ is the inverse for x. We just proved that every nonzero element has an inverse and so finite integral domains are fields as claimed. □

We talked about the next fact in class, but didn't write it down formally.

Lemma: *Suppose that F is a field. Then $F[x]$ is an integral domain.*

Proof. Remember that $F[x]$ is the polynomials in x with coefficients in F. It is easy to see that these form a commutative ring with unity under $+$ and $\cdot$ for polynomials. So suppose that $a(x) \cdot b(x) = 0$. Suppose for a contradiction that $a(x) \neq 0 \neq b(x)$. In that case we see that the degree of $a(x) \cdot b(x)$ is $\deg(a(x)) + \deg(b(x))$.[2] But that is impossible since 0 has degree $-\infty$ (the usual convention). We conclude that $a(x) = 0$ or $b(x) = 0$ which completes the proof. □

Here's another lemma.

Lemma: *Suppose that F is a field. Then either F contains a subfield which looks like $\mathbb{Q}$, or F contains a subfield that looks like $\mathbb{Z}/p$ for some prime p.*

Proof. Suppose first that the characteristic of F is $n > 0$. This means that $0 = n \cdot 1 = 1+1+\cdots+1 = \sum_{i=1}^{n}$ and n is the smallest integer > 0 satisfying this property. If n is composite $n = ab$ with $a, b > 1$. Then $0 = n \cdot 1 = ab \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$. Since fields are integral domains, either $a \cdot 1 = 0$ or $b \cdot 1 = 0$ but this contradicts the minimality of our choice of n. This proves that the characteristic $n = p$ of F is prime. Consider the set $\{0, 1, 2 \cdot 1 \cdots, (p-1) \cdot 1\}$. I claim this is a subfield of F that looks just like $\mathbb{Z}/p$. But this is easy, the addition and multiplication is just done mod p.

Now suppose that the characteristic of F is 0, which means that $n \cdot 1$ is never zero unless n is zero. The same argument above implies that F contains a subring that looks just like $\mathbb{Z}$. But once you are a field and you contain $\mathbb{Z}$, you also have to have inverses of all your elements, so you have elements that look like $\frac{1}{n}$. But then you have $m \cdot \frac{1}{n}$ too so you have a subfield of F that looks just like $\mathbb{Q}$. □

Now, suppose that $f(x) \in F[x]$ is a polynomial of degree > 0. We say that $f(x)$ is *irreducible in $F[x]$* if whenever we write $f(x) = g(x) \cdot h(x)$ with $g(x), h(x) \in F[x]$, then either $\deg(g(x)) = 0$ or $\deg(h(x)) = 0$. Note that $x^2 - 3$ is irreducible in $\mathbb{Q}[x]$ but it is not irreducible in $\mathbb{R}[x]$.

[1] This means if $ab = 0$ then $a = 0$ or $b = 0$ and if $ab = ac$ then $b = c$ as long as $a \neq 0$.

[2] If F is an arbitrary ring, this isn't always true. Notice that in $(\mathbb{Z}/4)[x]$, $(2x) \cdot (2x) = 0$.

Theorem: *If F is a field and $q(x) \in F[x]$ is an irreducible polynomial, then $(F[x])/q(x)$ is a field.*

Proof. We first show that $(F[x])/q(x)$ is an integral domain. Indeed, suppose $a(x), b(x) \in (F[x])/q(x)$ and that $a(x) \cdot b(x) = 0$. Just like for the integers modulo an integer, this means that $q(x)|(a(x) \cdot b(x))$. Since $q(x)$ is irreducible, this implies that $q(x)|a(x)$ or $q(x)|b(x)$. Implicitly we are using that we can factor polynomials uniquely, or alternately that irreducible polynomials are "prime". The proof though, is essentially the same as it was for the integers. Returning to the proof, if $q(x)|a(x)$ then $a(x) = 0 \in (F[x])/q(x)$. Likewise if $q(x)|b(x)$ then $b(x) = 0 \in (F[x])/q(x)$. Either way, we are done.

Now we prove that $(F[x])/q(x)$ is a field. We will restrict to the special case that F is a finite field since that's the case that will interest us this semester. Then we know that all the elements of $(F[x])/q(x)$ are represented as polynomials with coefficients in F of degree $< \deg q(x)$. There are only finitely many of those (see the first problem on worksheet #2). Thus $(F[x])/q(x)$ is a finite integral domain and hence a field. □