Polynomials with rational number coefficients

Key fact from previous class: *The ideal $(p(x)) \subseteq F[x]$ is maximal iff $p(x)$ is irreducible*
Will help us construct extension fields of F. Example: $\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$.

So we need to understand irreduciblity of polynomials.

A little easier if we can reduce it to irreducibility over $\mathbb{Z}$. In fact we will show the following:

Gauss' lemma: *If a polynomial cannot be factored with integer coefficients, then it cannot be factored with rational coefficients*

(Usually stated in the contrapositive: If it can be factored in rational coefficients, then it can be factored with integer coefficients).

Example: $x^3 + 6x - 7$

Eisenstein's irreducibility criterion: If $f(x) \in \mathbb{Z}[x]$ has $f(x) = x^n + a_1 x^{n-1} + ... + a_n$ and the prime p divides all the a_i but p^2 does not divide a_n then f is irreducible over $\mathbb{Q}[x]$.

Need the following lemmata:

Lemma 4.6.1 If $f(x) \in \mathbb{Q}[x]$ then

$$f(x) = \frac{u}{m}(a_0 x^n + a_1 x^{n-1} + ... + a_n)$$

where $u, m, a_0, a_1, ..., a_n$ are integers and the integers $a_0, a_1, ..., a_n$ have gcd = 1 and u, m are also relatively prime.

Lema 4.6.2 If R is any ring and I is an ideal of R then $I[x]$ is an ideal of $R[x]$ and $R[x]/I[x] \simeq R/I[x]$.

Applying this to $\mathbb{Z}$ and the ideal $p\mathbb{Z}$ we get that the ring of polynomials obtained by reducing coefficients of integer polynomials mod p is the same as the polynomials over $\mathbb{Z}/p\mathbb{Z}$.

Use these to prove Gauss' lemma and Eisenstein's criterion. Can do Gauss' lemma without the lemma 4.6.2 but it is nicer with it.

Key role played in proof of Gauss' lemma by the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field (hence an integral domain).

Proof of Eisenstein's criterion Suppose $f(x) = g(x)h(x)$ where $g, h \in \mathbb{Z}[x]$. (by Gauss' lemma). Using the hypothesis, we get that $f(x) \equiv x^n \ mod\ p\mathbb{Z}[x]$. Now suppose $g(x) = x^r + A(x) \in \mathbb{Z}[x]/p\mathbb{Z}[x]$ and $h(x) = x^s + B(x) \in \mathbb{Z}[x]/p\mathbb{Z}[x]$ where $r + s = n$. Now multiplying we get $f(x) = g(x)h(x) \implies x^n \equiv (x^r + A(x))(x^s + B(x)) \in \mathbb{Z}[x]/p\mathbb{Z}[x] \simeq \mathbb{Z}/p\mathbb{Z}[x]$. This gives $A(x)x^s + B(x)x^r + A(x)B(x) \equiv 0 \ mod\ p\mathbb{Z}[x]$

Clearly the degree of the LHS is less than n. From this we can show that $A(x), B(x)$ are the zero polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$. Will need to use the fact that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Ash's book has a proof that gives the details better.

What would go wrong if we replaced p with any integer n (possibly composite) in Eisenstein's criterion? You could get a product of two polynomials that are not monomials equal to x^n in $\mathbb{Z}/n\mathbb{Z}[x]$.

Note on problem 21 in 4.5: Had to use at least 3 basic requirements for Euclidean domain. Look at polynomial ring to get an idea of how it will work.

Example for irreducible polynomial: cyclotomic polynomial for primes.

$$\frac{x^p - 1}{x - 1} = 1 + x + x^2 + ... + x^{p-1}.$$

Other examples: $x^n - p$, $x^5 - 4x + 22$.

HW6:

4.5: 15,16,18,20,21.

4.6: 2,3,4,6,7,8,12,13.

Exercise before class: Prove that unit element in a any ring is unique, if it exists.

4.7: Please read it at home.