Day 18

Gauss's Lemma

In the proof that $R[x]$ is a UFD if R is one, we need the following fact, which is often called "Gauss's Lemma."

Theorem: Let R be a UFD. Then if a polynomial $p(x) \in R[x]$ is reducible in $K(R)[x]$, it is reducible in $R[x]$.

If $R = \mathbb{Z}$, then what this is saying is that if a polynomial can be factored in a nontrivial way in $\mathbb{Q}[x]$ – meaning using polynomial factors whose coefficients have denominators – then it can be factored in $\mathbb{Z}[x]$, meaning without denominators. More precisely, if $p(x) \in R[x]$ and

$$p(x) = A(x)B(x)$$

where $A(x)$ and $B(x)$ are in $K(R)[x]$, then there are elements a and b in R such that $aA(x)$ and $bB(X)$ are in $R[x]$ and $abA(X)B(X) = p(x)$.

To see that there is some content to this, let $R = \mathbb{Z}[\sqrt{-3}]$. Consider the polynomial $x^2 - x + 1 \in R[x]$. This polynomial factors in $Q(\sqrt{-3})[x]$ as

$$x^2 - x + 1 = (x - \rho)(x - \bar{\rho})$$

where

$$\rho = \frac{1 + \sqrt{-3}}{2}.$$

So this polynomial factors in $K(R)[x]$. But it cannot factor in $R[x]$ because it's monic and the roots don't lie in $R[x]$.

This means R is not a UFD and in fact the idea generated by 2 and $1 + \sqrt{-3}$ is not principal.

However, the ring $\mathbb{Z}[\rho]$ *is* a PID.

Proof of Gauss's Lemma: Given $p(x)$ in $R[x]$, where R is a UFD, assume $p(x) = a(x)b(x)$ where both factors are in $K(R)[x]$. Let d be a common denominator so $dp(x) = a_1(x)b_1(x)$ where a_1 and b_1 are in $R[x]$. Now, since R is a UFD, we can factor d into a product of irreducibles π_i. Formally speaking the proof is on the number of irreducible factors of d. If d is a unit, then our factorization is already over $R[x]$, so suppose our result is true for d with at most

n irreducible factors. In other words, if we have $dp(x) = a(x)b(x)$ with d having at most n irreducible factors, then there is an expression $p(x) = a'(x)b'(x)$ with a' and b' in $R[x]$. Now suppose we have an expression $dp(x) = a_1(x)b_1(x)$ where d has $n+1$ factors. Let π be one them.

Since R is a UFD, the ideal πR is prime and therefore $(R/\pi R)[x]$ is an integral domain. Since $a_1(x)b_1(x) \equiv 0 \pmod{\pi R[x]}$, one of them must be zero; say $a_1(x)$. That means all the coefficients of $a_1(x)$ are divisible by π so we can divide $a_1(x)$ by π and get a_2 which still has cofficients in $R[x]$. Now we have $(d/\pi)p(x) = ((a(x))/\pi)b(x)$. By induction we get the factorization of $p(x)$ over R.

Remark: A polynomial $p(x)$ over $\mathbb{Z}$ is called primitive if its coefficients are relatively prime. This theorem is sometimes expressed over $\mathbb{Z}$ by saying that the product $p(x)q(x)$ of two *primitive* polynomials is primitive.

Eisenstein's Criterion

Theorem: Suppose R is an integral domain. If $f(x) = a_0 + a_1x + \ldots + x^n \in R[x]$ is a monic polynomial and P is a prime ideal of R such that $a_i \in P$ for $i = 0, \ldots, n-1$, and if $a_0 \notin P^2$, then $f(x)$ is irreducible.

Proof: Suppose $f(x) = a(x)b(x)$. Then $f(x) \equiv x^n \equiv a(x)b(x) \pmod{P}$, This means that the constant terms of $a(x)$ and $b(x)$ have product zero mod P so must be in P. But then the constant term of f would be in P^2.