Recall the notion of a Principal Ideal Domain, and that \( \mathbb{Z} \) and \( F[x] \) are ones.

**Gaussian integers.** Here is one more example of a PID.

Recall the complex numbers: \( \mathbb{C} = \{ a + bi \mid a, b \in \mathbb{R} \} \), where \( i^2 = -1 \). The Gaussian integers are the subset
\[
\mathbb{Z}[i] := \{ a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z} \}.
\]

If you plot them in the complex plane, you get the integer lattice.

It is not hard to see that \( \mathbb{Z}[i] \) is a domain (it is a subset of a field closed under addition, negation, and multiplication, and contains 0 and 1.)

This is in fact a PID: this is not obvious.

**Divisibility in PIDs.** Assume \( D \) is a PID. Definitions and propositions:

- Given \( f, g \in D \), say that \( g \) divides \( f \) if there exists \( d \in D \) such that \( fd = g \). Write "\( g \) divides \( f \)" for "\( g \) divides \( f \)".
  
  (Example: In \( D = \mathbb{R}[x] \), \( x + 1 \) divides \( x^2 + 4x + 3 \).) We also say "\( g \) is a factor of \( f \)."

- For \( f, g \in D \), a greatest common divisor is a \( d \in D \) which is a common divisor of \( f, g \) such that every common divisor of \( f, g \) divides \( d \).

  Note that \( Dg = (g) \), the ideal generated by \( g \), is exactly the set of elements which are divisible by \( g \). So

  \[
  g \mid f \iff f \in (g).
  \]

**Proposition.** Let \( D \) be a PID. For all \( f, g \in D \), a GCD \( d \) exists. Furthermore, there exist \( m, n \in D \) such that \( d = mf + ng \).

**Proof.** Because \( I = (f, g) \) is a principal ideal, there exists \( d \) such that \( I = (d) \), which implies \( d = mf + ng \), and also that \( d \) is a common factor of \( f \) and \( g \). We will show that \( d \) must be a GCD.

Since \( f, g \in I = Dd \), there exist \( s, t \) such that \( d = sf = tg \), so \( d \) is a common divisor of \( f, g \). If \( q \mid f \) and \( q \mid g \) is another common divisor, then \( q \mid mf + ng = d \): that is, if \( f, g \in Dq \), then \( d = mf + ng \in (q) \), so \( q \) divides \( d \). \( \square \)

*Date:* April 25, 2016.
Example. Let $f = x^2 + 2x + 1$ and $g = x^2 + 3x + 2$ in $\mathbb{R}[x]$. Then the GCD $d$ is any generator of the ideal $(f,g)$. I claim that we can take $d = x + 1$. In fact, it is clear that this is a common factor, since $f = (x + 1)^2$ and $g = (x + 1)(x + 2)$. To show that $x + 1$ is the GCD, note that
\[ d = (1)f - (1)g. \]
Therefore any common factor of $f, g$ also divides $d$.

Note: $3x + 3$ is also a GCD. GCDs aren’t quite unique.

- An element $f \in D$ is a unit if it has a multiplicative inverse in $D$. Exercise. $f \in F[x]$ is a unit if and only if it is a non-zero constant polynomial. I’ll write $\text{Units}(D)$ for the subset of units in $D$.

Example. $\text{Units}(\mathbb{Z}) = \{ \pm 1 \}$.

Example. $\text{Units}(F[x]) = \{ f \in F[x] \mid \deg f = 0 \} = F \setminus \{ 0 \}$, the set of non-zero constant polynomials.

Example. $\text{Units}(\mathbb{Z}[i]) = \{ \pm 1, \pm i \}$. This can be proved using the complex norm $N(a + bi) := a^2 + b^2$ and the fact that $N(\alpha \beta) = N(\alpha)N(\beta)$.

Exercise: if $u$ is a unit and $f \mid u$, then $f$ is also a unit: if $u = fg$, then $f(gu^{-1}) = 1$, so $f$ has a multiplicative inverse.

Proposition. If $D$ is a PID, then $(d) = (d')$ if and only if there exists a unit $u$ such that $d' = ud$.

Proof. We have $d = fd'$ and $d' = gd$, so $d = fgd$ and $d' = fgd'$, whence $d(1 - fg) = 0 = d'(1 - fg)$. Either $fg = 1$, whence $f$ and $g$ are both units; otherwise, we must have $d = 0 = d'$.

In particular, the GCD of two elements is only defined up to multiplication by a unit.

Say that $f, g \in D$ are relatively prime if $1$ is a GCD. In other words, the only common factors of

Irreducible elements. We still take $D$ to be a PID.

- An element $f \in D$ is reducible if it can be written $f = gh$ with $g, h$ both not units. An element $f \in D$ is irreducible if (i) it is not 0 or a unit, and (ii) $f = gh$ implies that either $g$ or $h$ is a unit.

Example. In $D = \mathbb{Z}$, this is almost exactly what we meant by prime, except primes in $\mathbb{Z}$ were assumed positive. For each prime $p$ in $\mathbb{Z}$, we get two irreducible elements $\pm p$.

Example. An element $f \in F[x]$ is irreducible if it is not constant, and cannot be factored into a product of polynomials of smaller degree.

For instance, in $\mathbb{R}[x]$, every linear polynomial $f = ax - b$ is irreducible ($a \neq 0$). Also, some quadratic polynomials $f = ax^2 + bx + c$ are irreducible ($a \neq 0$). Which ones?

Non-obvious fact: these are the only irreducible polynomials in $\mathbb{R}[x]$.