ABSTRACT ALGEBRA 2 COURSE NOTES, LECTURE 1: EUCLIDEAN DOMAINS AND PRINCIPAL IDEAL DOMAINS.

ANDREW SALCH

Remember that a principal ideal domain, or PID for short, is an integral domain in which every ideal is principal.

Example 0.1. Every field is a PID, since fields have no zero divisors, so they are integral domains, and since the only ideals in a field \( k \) are \((0)\) and \((1) = k\), both of which are, of course, principal.

The ring of integers \( \mathbb{Z} \) is a PID. If \( k \) is a field, then the polynomial ring \( k[x] \) is a PID. (I prove both of these claims below, in Theorem 1.5.)

Example 0.2. The ring \( \mathbb{Z}[x] \) is an example of an integral domain that is not a principal ideal domain. Here is a proof: I claim that the ideal \((p, x)\), for any prime number \( p \in \mathbb{Z}\), is not principal. Suppose on the contrary that \((p, x)\) is principal, i.e., \((p, x) = (f)\) for some \( f \in \mathbb{Z}[x]\). Since the degree of \( p \) is zero (since it is a constant polynomial), the degree of \( f \) must be zero as well. So \( f \) must be a constant polynomial. But \((p, x) = (f)\), so \( x = fg \) for some \( g \in \mathbb{Z}\). So \( g = \pm x \) and \( f = \pm 1 \). So either \( f = 1 \) or \( f = -1 \), and either way, \((f) = \mathbb{Z}[x]\), not \((p, x)\). So \((p, x)\) is not principal.

Another good example of a commutative ring that is not a principal ideal domain is \( k[x, y] \) for any field \( k \) (see the exercise below), or indeed, \( R[x, y] \) for any commutative ring \( R \). Indeed, \( k[x_1, x_2, \ldots, x_n] \) is not a principal ideal domain unless \( n = 1 \).

1. Euclidean domains.

Definition 1.1. An integral domain \( R \) is called a Euclidean domain if there exists a function
\[ \delta : R \setminus \{0\} \to \mathbb{N} \]
such that, for all \( a, b \in R \setminus \{0\}, \delta(ab) \geq \delta(a) \) and there exist \( q, r \in R \) such that \( a = bq + r \) and either \( r = 0 \) or \( \delta(r) < \delta(b) \). We call the function \( \delta \) a Euclidean norm on \( R \).

The \( q \) and \( r \) in Definition 1.1 stand for “quotient” and “remainder,” and a Euclidean norm is exactly what you need in order to run the “Euclidean algorithm,” which we will talk about in class.

Example 1.2. The most familiar examples of Euclidean domains are \( \mathbb{Z} \), with norm given by the absolute value, and \( k[x] \) for \( k \) a field, with norm given by the degree of a polynomial.

Proposition 1.3. Let \( R \) be a Euclidean domain with norm \( \delta \). Then the group of units \( R^\times \) in \( R \) is exactly the set
\[ \{ r \in R : \delta(r) = \delta(1) \}. \]

Proof. Suppose \( x \in R \). Then \( \delta(x) = \delta(x1) \geq \delta(1) \), so no elements of \( R \) have smaller norm than 1 does.

Date: January 2016.
Now let \( x \in R \) be a unit. Then there exists some \( y \in R \) such that \( xy = 1 \). Then 
\[
\delta(1) = \delta(xy) \geq \delta(x).
\]
But we have already shown that \( \delta(x) \geq \delta(1) \) for all \( x \in R \). So 
\[
\delta(x) = \delta(1) \quad \text{for all } x \in R^\times.
\]
Conversely, suppose that \( \delta(x) = \delta(1) \). Then there exists some \( q, r \) such that \( 1 = xq + r \) with either \( r = 0 \) or \( \delta(r) < \delta(x) \). But we have already shown that \( \delta(r) < \delta(1) \) is impossible, so \( r = 0 \). So \( 1 = xq \). So \( x \in R^\times \).

**Example 1.4.** By Proposition 1.3, the units in \( \mathbb{Z} \) are the nonzero elements with norm 1, i.e., \( \mathbb{Z}^\times = \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z} \). Similarly, the units in \( k[x] \) are the nonzero polynomials of degree zero, i.e., the nonzero constant polynomials, i.e., \( k[x]^\times \cong k^\times \).

**Theorem 1.5.** Let \( R \) be a Euclidean domain. Then \( R \) is a principal ideal domain.

**Proof.** Choose a Euclidean norm \( \delta \) on \( R \). Let \( I \subseteq R \) be an ideal, and choose an element \( i \in R \) with minimal norm, i.e., \( \delta(i) \leq \delta(i') \) for all \( i' \in I \).

I claim that \( I = \langle i \rangle \). Clearly \( \langle i \rangle \subseteq I \), since \( i \in I \) and \( I \) is an ideal. Conversely, if \( j \in I \), then 
\[
\delta(j) \geq \delta(i),
\]
and there exists some \( q, r \) such that \( j = iq + r \) and either \( r = 0 \) or \( \delta(r) < \delta(i) \). We solve for \( r \) to get \( r = j - iq \), and since \( j \) and \( iq \) are both in \( I \), so is \( r \). So \( \delta(r) < \delta(i) \) is impossible, since \( i \) was assumed to have minimal norm among the elements of \( I \). So \( r = 0 \). So \( j = iq \). So \( j \in \langle i \rangle \). So \( I \subseteq \langle i \rangle \).

Hence every ideal in \( R \) is principal. \( \square \)

**Example 1.6.** Clearly \( \mathbb{Z} \) and \( k[x] \), for \( k \) a field, are principal ideal domains, since they are Euclidean domains.

2. **PIRs that aren’t Euclidean.**

Suppose that you have an integral domain \( R \), and you want to know if it is a principal ideal domain. One way of checking this is to see if there is an obvious choice of Euclidean norm on it; for \( \mathbb{Z} \) and \( k[x] \) and a handful of other rings (like \( \mathbb{Z}[i] \)) there is a function \( R \setminus \{0\} \to \mathbb{N} \) which you have been calling a “norm” for years, so it’s very natural to check that this norm in fact satisfies the axioms for a Euclidean norm, making the domain \( R \) Euclidean and hence a principal ideal domain.

However, there are other ways of checking whether a domain is a principal ideal domain (for example: the famous identifiable norm group of a Dedekind domain is a group which is trivial if and only if the Dedekind domain is a PID, but we will not get to ideal class groups this semester; these are covered in topics classes in number theory, algebraic geometry, and algebraic K-theory). It is also true that not every principal ideal domain is a Euclidean domain, so a domain may be a PID even in cases where it is totally impossible to produce a Euclidean norm on the domain.

Suppose you have an integral domain that you suspect is not Euclidean. If you can show that the integral domain is not a PID, then it cannot be Euclidean; but not every PID is Euclidean. It is usually cumbersome to show that a given principal ideal domain fails to be Euclidean. The best way to try to do this is to show that Euclidean domains have additional properties which not all principal ideal domains have. For example:

**Definition 2.1.** Let \( R \) be an integral domain. An element \( r \in R \) is called a universal side divisor if \( r \) satisfies the following conditions:

- \( r \neq 0 \).
- \( r \) is not a unit in \( R \).
- For every \( x \in R \), there exists elements \( a, z \in R \) such that \( ra = x - z \) and either \( z = 0 \) or \( z \) is a unit in \( R \).
In other words: if \( r \) is a universal side divisor in \( R \), this means that every element of \( R \) is either a multiple of \( r \), or a multiple of \( r \) plus a unit in \( R \).

**Proposition 2.2.** If \( R \) is a Euclidean domain which is not a field, then there exists a universal side divisor in \( R \).

**Proof.** Choose a Euclidean norm \( \delta \) on \( R \). Let \( R' \) denote the set of nonzero, nonunit elements of \( R \). Then \( R' \) is nonempty since \( R \) is not a field. Let

\[
X = \{ \delta(r) : r \in R' \} \subseteq \mathbb{N}.
\]

Every subset of \( \mathbb{N} \) contains a smallest element, so let \( n \) be the smallest element of \( X \), and let \( r \) be any element of \( R' \) such that \( \delta(r) = n \). Then, given \( x \in R \), by the definition of a Euclidean norm there exist elements \( a, z \in R \) such that \( x = ar + z \) and either \( z = 0 \) or \( \delta(z) < \delta(r) \). Then \( ra = x - z \) and either \( z = 0 \) or \( \delta(z) \) is smaller than the norm of every nonunit element in \( R \), i.e., \( z \in R^x \). \( \square \)

You can use Proposition 2.2 to show that certain PIDs fail to have Euclidean domains, since they fail to have a universal side divisor. For example:

**Proposition 2.3.** Let \( R = \mathbb{Z}[x]/(x^2 - x + 5) \). Then \( R \) is not a Euclidean domain.

**Proof.** I claim that \( R \) does not contain a universal side divisor. (I also claim that \( R \) is a PID, but we won’t prove that until a little bit later.) To prove this, first we ought to know what the units in \( R \) are. I claim that \( R^x \cong \mathbb{Z}/2\mathbb{Z} \), generated by \(-1 \in R \). Here is a proof: first, to find the units in \( R^x \), it is convenient to map \( R^x \) to the group of units of some ring whose units we already know. Let \( N : R^x \to \mathbb{Z}^x \) be the function given by \( N(a+bx) = a^2 + ab + 5b^2 \).

I claim that \( N \) is actually a homomorphism of groups. The proof is easy and explicit:

\[
N((a + bx)(c + dx)) = N(ac + (ad + bc)x + bdx^2)
= N((ac - 5bd) + (ad + bc + bd)x)
= (ac - 5bd)^2 + (ac - 5bd)(ad + bc + bd) + 5(ad + bc + bd)^2
= a^2c^2 - 10abcd + 25b^2d^2 + a^2cd + abc^2 + abcd - 5abd^2 - 5b^2cd - 5b^2d^2 + 5a^2d^2 + 10abcd + 10abc
= a^2c^2 + 25b^2d^2 + a^2cd + abc^2 + abcd + 5abd^2 + 5b^2cd + 5b^2d^2 + 5a^2d^2
= (N(a + bx))(N(c + dx)).
\]
Since \( \mathbb{Z}^\times = \{1, -1\} \), this tells us that every unit \( a + bx \) in \( R \) must satisfy either \( N(a + bx) = 1 \) or \( N(a + bx) = -1 \). Let’s see what this means about \( a \) and \( b \):

\[
1 = N(a + bx) = a^2 + ab + 5b^2 \quad \text{and} \quad 0 = a^2 + ba + (5b^2 - 1), \quad \text{so}
\]

\[
a = \frac{-b \pm \sqrt{b^2 - 4(5b^2 - 1)}}{2}
\]

\[
= \frac{-b \pm \sqrt{-19b^2 + 4}}{2}, \quad \text{while}
\]

\[-1 = N(a + bx) = a^2 + ab + 5b^2 \quad \text{implies that}\n\]

\[
a = \frac{-b \pm \sqrt{b^2 - 4(5b^2 + 1)}}{2}
\]

\[
= \frac{-b \pm \sqrt{-19b^2 - 4}}{2}.
\]

Now the trick here is that \( a \) and \( b \) have to actually be integers, and \( \sqrt{-19b^2 - 4} \) isn’t even a real number for any choice of integer \( b \), since it’s the square root of a negative number. So \( N(a + bx) = -1 \) has no solutions with \( a + bx \in R \). On the other hand, \( N(a + bx) = 1 \) has solutions: \(-19b^2 + 4 \geq 0 \) if and only if \( |b| \leq \frac{2}{\sqrt{19}} \). There are not a lot of integers whose absolute value is less than or equal to \( \frac{2}{\sqrt{19}} \). So \( b \) must be zero, so that \(-19b^2 + 4 \) can be nonnegative so that \( -b \sqrt{-19b^2 + 4} \) can be an integer. Since \( b = 0 \), we now have that

\[
a = \frac{-b \pm \sqrt{-19b^2 + 4}}{2}
\]

\[
= \pm \frac{\sqrt{4}}{2} = \pm 1.
\]

So the only elements \( a + bx \in R \) such that \( N(a + bx) = 1 \) are 1 and \(-1 \). So the only possible units in \( R \) are 1 and \(-1 \), both of which clearly actually are units in \( R \). So \( R^\times = \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z} \).

(How did I have the idea to try \( N(a + bx) = a^2 + ab + 5b^2 \)? I cheated by knowing a little bit of number theory: this function \( N \) is called a field norm, something which is quite useful in number theory, and which is not the same thing as a Euclidean norm (sometimes field norms turn out to be Euclidean norms, but frequently they don’t). If you are curious about field norms, ask me in class and I will show you more about them. If you don’t have this field norm at your disposal, computing \( R^\times \) by brute force (i.e., by setting \( (a + bx)(c + dx) \) to 1 and trying to solve for \( a, b, c, \) and \( d \)) is really, really hard work, far far harder than what we just did using the field norm; try doing it if you’re curious. On the other hand, there is a way to compute \( R^\times \) which is much faster than using the field norm (in fact, you can do it in your head quite easily), but it requires that you know a little bit more number theory: you need to know the Dirichlet unit theorem, and a little bit about cyclotomic polynomials—we
will get to cyclotomic polynomials this semester, but the Dirichlet unit theorem is really part of a number theory class and I don’t expect to cover it this semester.)

Now that we know \( R \), suppose that \( u + vx \in R \) is a universal side divisor. Now note that, if \( b \neq 0 \), then \( N(a + bx) = a^2 + ab + 5b^2 \geq 5 \), while if \( b = 0 \) then \( N(a) = a^2 \), so since \( u + vx \) is (from the definition of a universal side divisor) not allowed to be a unit, \( N(u + vx) \geq 4 \). By the definition of a universal side divisor, there exist elements \( a, z \in R \) such that \( (u + vx)a = 2 - z \) and such that either \( z = 0 \) or \( z \) is a unit in \( R \). Hence either \( (u + vx)a \) must be either 1, 2, or 3, since the only units in \( R \) are 1 and \(-1\). We cannot have that \( (u + vx)a = 1 \), since then \( u + vx \) is a unit (its inverse is \( a \)), and universal side divisors are not allowed to be units. So \( (u + vx)a \) must be 2 or 3. Taking the field norm, we have

\[
N((u + vx)a) = N(u + vx)N(a) = N(2) \text{ or } N(3), \text{ i.e.},
\]
\[
= 4 \text{ or } 9.
\]

Now here is the trouble: if \( N(2) = 4 \), then since 4’s only divisors are 1, 2, and 4, either \( N(u + vx) \) and \( N(a) \) are both equal to 2 (impossible, since we already showed that no element in \( R \) has norm 2 or 3, the values taken by \( N \) jump from 1 to 4), or one of the two numbers \( N(u + vx) \) is equal to 1 and the other is equal to 4. Since we already that the only solutions to \( N(z) = 1 \) are \( z = 1 \) and \( z = -1 \), this means either \( u + vx = \pm 1 \) (impossible, since then \( u + vx \) would be a unit), or \( a = \pm 1 \), which implies that \( u + vx = \pm 2 \).

Similarly, if \( N(2) = 9 \), then since 9’s only divisors are 1, 3, and 9, either \( N(u + vx) \) and \( N(a) \) are both equal to 3 (impossible, since we already showed that no element in \( R \) has norm 2 or 3, the values taken by \( N \) jump from 1 to 4), or one of the two numbers \( N(u + vx) \) is equal to 1 and the other is equal to 9. Since we already that the only solutions to \( N(z) = 1 \) are \( z = 1 \) and \( z = -1 \), this means either \( u + vx = \pm 1 \) (impossible, since then \( u + vx \) would be a unit), or \( a = \pm 1 \), which implies that \( u + vx = \pm 3 \).

So the only possible elements in \( R \) that might be universal side divisors are 2, \(-2\), \(3\), and \(-3\). Let’s handle them one by one:

**If 2 is a universal side divisor**: Then there exists some \( a, z \in R \) such that \( 2a = x - z \) and \( z \in \{0, -1, 1\} \). But neither \( x \) nor \( x - 1 \) nor \( x + 1 \) is divisible by 2, so this is impossible.

**If \(-2\) is a universal side divisor**: Impossible by the same argument.

**If 3 is a universal side divisor**: Then there exists some \( a, z \in R \) such that \( 3a = x - z \) and \( z \in \{0, -1, 1\} \). But neither \( x \) nor \( x - 1 \) nor \( x + 1 \) is divisible by 3, so this is impossible.

**If \(-3\) is a universal side divisor**: Impossible by the same argument.

So \( R \) does not contain a universal side divisor. So \( R \) is not a Euclidean domain, although it is a principal ideal domain. \( \square \)