Math 662 — Spring 2014
Homework 3 — Drew Armstrong

Problem 0. (Drawing Pictures) What does the curve $y^2 = x^2(x+1)$ look like "at infinity"? We define n-dimensional real projective space $\mathbb{R}P^n$ as the set of lines through the origin in $\mathbb{R}^{n+1}$. That is, we define

$$\mathbb{R}P^n := \{[a_0 : a_1 : \cdots : a_n] : a_i \in \mathbb{R}, \text{ not all zero}\},$$

and we declare that $[a_0 : \cdots : a_n] = [b_0 : \cdots : b_n]$ if there exists $0 \neq \lambda \in \mathbb{R}$ such that $a_i = \lambda b_i$ for all i. (These are called homogeneous coordinates.) If we distinguish between the lines with $a_0 \neq 0$ and $a_0 = 0$ we get a decomposition

$$\mathbb{R}P^n = \mathbb{R}^n \cup \mathbb{R}P^{n-1}$$

where $\mathbb{R}^n = \{[1 : a_1 : \cdots : a_n]\}$ is the "affine" part and $\mathbb{R}P^{n-1} = \{[0 : a_1 : \cdots : a_n]\}$ is the part "at infinity". Now, given a polynomial $f(x,y) \in \mathbb{R}[x,y]$ of degree n we can "homogenize" it:

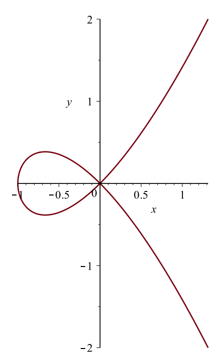
$$F(x,y,z) := z^n \cdot f\left(\frac{x}{z}, \frac{y}{z}\right).$$

Note that the polynomial $F(x,y,z)$ is "homogeneous" of degree n:

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n \cdot F(x,y,z) \text{ for all } 0 \neq \lambda \in \mathbb{R}.$$

Thus the condition $F(x,y,z) = 0$ defines a curve in $\mathbb{R}P^2$ called the homogenization of the curve $f(x,y) = 0$ in $\mathbb{R}^2$. We can recover the original curve by "de-homogenizing", i.e., by setting $z = 1$. **Finally**, consider the curve in $\mathbb{R}P^2$ defined by the homogeneous cubic polynomial $y^2 z = x^2(x+z)$. **Draw** the three de-homogenizations at $z = 1$, $y = 1$, and $x = 1$. Describe the behavior of the curve $y^2 = x^2(x+1)$ at the $z = 0$ "line at infinity" $\mathbb{R}P^1$. We can also think of $\mathbb{R}P^2$ as the unit sphere in $\mathbb{R}^3$ with antipodal points identified. **Draw** the curve $y^2 z = x^2(x+z)$ on the unit sphere. What does it do at the $z = 0$ equator?

Solution. The equation $f(x,y) = y^2 - x^3 - x^2$ defines a zero locus in $\mathbb{R}^2$ that we recognize:



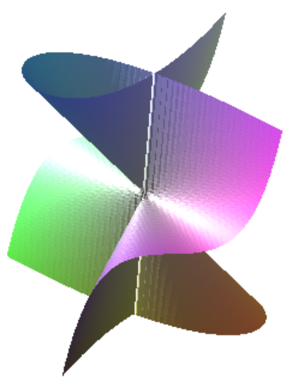
This is called the nodal cubic. Since $f(x, y)$ has degree 3 we homogenize it by defining

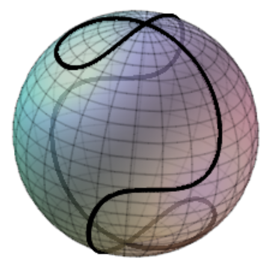
$$F(x, y, z) := z^3 \cdot f\left(\frac{x}{z}, \frac{y}{z}\right) = z^3\left(\frac{y^2}{z^2} - \frac{x^3}{z^3} - \frac{x^2}{z^2}\right) = y^2z - x^3 - x^2z.$$

Because this $F(x, y, z)$ is a **homogeneous** polynomial, it has a well-defined zero locus in the projective plane $\mathbb{R}P^2$. (What does the previous sentence mean? In general we have

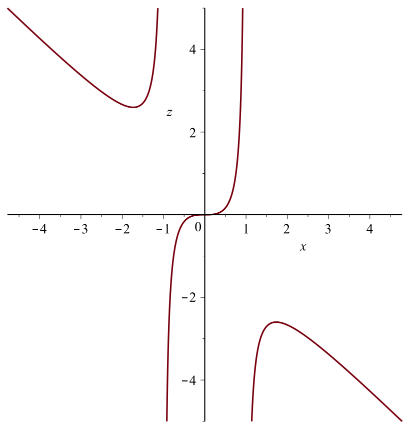
$$F(\lambda x, \lambda y, \lambda z) = \lambda^3 F(x, y, z)$$

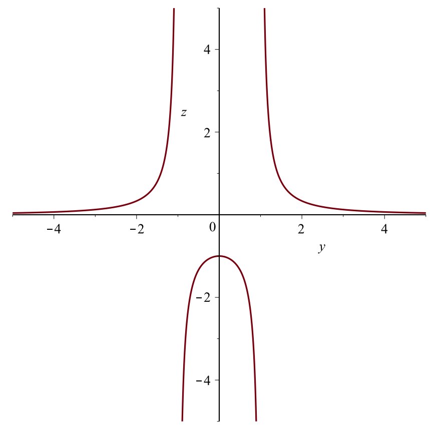
and so F does **not** define a function on points $[x : y : z] \in \mathbb{R}P^2$. However, if $F(x, y, z) = 0$ then we **do** have $F(\lambda x, \lambda y, \lambda z) = \lambda^3 F(x, y, z) = \lambda^3 \cdot 0 = 0$ for all $\lambda \in \mathbb{R}$.) Here we have plotted $F(x, y, z) = 0$ as a surface in $\mathbb{R}^3$ consisting of lines through the origin, and its intersection with the unit sphere, which we think of as a curve in $\mathbb{R}P^2$. (Antipodal points of the sphere are identified.)





Note that the curve on the sphere still "looks like" the nodal cubic in the northern hemisphere, but now we can see what is happening at infinity (i.e., the equator). We can recover the original nodal cubic in the x, y-plane if we substitute $z = 1$. Geometrically we are projecting the curve from the center of the sphere onto the tangent plane at the north pole. However, the north pole is arbitrary in this construction. **Any** point can be the origin, and **any** great circle can be the line at infinity. If we dehomogenize at $y = 1$ and $x = 1$ we obtain the curves $F(x, 1, z) = z - x^3 - x^2z = 0$ in the x, z-plane and $F(1, y, z) = y^2z - 1 - z = 0$ in the y, z-plane, shown here:





If you squint your eyes, you can see that these are the projections of the homogeneous curve from the center of the unit sphere to the tangent planes at the points $[0 : 1 : 0]$ and $[1 : 0 : 0]$ on the equator. Looking at the left picture we see that the nodal cubic nodal cubic is tangent to the line at infinity at the infinite point $[0 : 1 : 0]$, with intersection of multiplicity 3. This is an important property of the curve, but it is not easily visible in the x, y-plane. $\square$

[In the problems that follow we will consider polynomials $R[y]$ where R is a PID. Of course I have in mind the examples $R = \mathbb{Z}$ and $R = K[x]$ (the only two PIDs I know), but there is a certain kind of fun in using language that is general to PIDs. In my experience this kind of fun is exactly what people mean by the words Algebraic Geometry.]

Problem 1. ($\mathbb{Z}[y]$ and $K[x, y]$ are not PIDs) Let R be a ring such that $R[y]$ is a PID. You will show that R must be a field. Since $\mathbb{Z}$ and $K[x]$ are not fields, this implies that $\mathbb{Z}[y]$ and $K[x, y]$ are not PIDs.

(a) Prove that R is a domain.
(b) Prove that $R[y]/(y)$ is isomorphic to R, hence $(y) \leq R[y]$ is a prime ideal.
(c) Prove that $(y) \leq R[y]$ is a maximal ideal, hence R is a field.

Proof. To prove (a), consider any $a, b \in R$ such that $a \neq 0$ and $b \neq 0$. Then a and b are also nonzero as elements of $R[y]$. Since $R[y]$ is a domain this implies that $ab \neq 0$ in $R[y]$ and hence $ab \neq 0$ in R. We conclude that R is a domain.

For part (b) we define a map $R \to R[y]/(y)$ by

$$a \mapsto a + 0y + 0y^2 + \cdots + (y).$$

This is clearly a ring homomorphism. To show that it is surjective, consider any $f(y) = \sum_k a_k x^k \in R[y]$. Then $a_0 \mapsto a_0 + (y) = f(y) + (y)$. To show that it is injective, consider any $a, b \in R$ and suppose that $a + (y) = b - (y)$. This implies that $a - b = yf(y)$ for some $f(y) \in R[y]$. If $a - b \neq 0$ then we find that $f(y) \neq 0$ and hence

$$0 = \deg(a - b) = \deg(yf(y)) = \deg(y) + \deg(f) = 1 + \deg(f) \geq 1.$$

Contradiction. Hence $a = b$. We conclude that $R \approx R[y]/(y)$. Since we know from part (a) that R is a domain, this implies that $(y) \leq R[y]$ is a prime ideal.

For part (c), assume for contradiction that $(y) \leq R[y]$ is not a maximal ideal. Since R is a PID this implies that there exists $f(y) \in R[y]$ such that $(y) < (f(y)) < (1)$. Since $y \in (f(y))$ we have $y = f(y)g(y)$ for some nonzero $g(y) \in R[y]$; since $(y) \neq (f(y))$ we know that $g(y)$ is not a constant; and since $(f(y)) \neq (1)$ we know that $f(y)$ is not a constant. Therefore we have

$$1 = \deg(y) = \deg(fg) = \deg(f) + \deg(g) \geq 1 + 1 = 2.$$

Contradiction. We conclude that $(y) \leq R[y]$ is a maximal ideal, and hence $R \approx R[y]/(y)$ is a field. □

[We have just shown that $\mathbb{Z}[y]$ and $K[x, y]$ are not PIDs. It turns out that every prime ideal in these rings can be generated by at most two elements (we say they have Krull dimension 2) but that will wait until later.]

Problem 2. (Gauss' Lemma) Let R be a PID with field of fractions $K = \mathrm{Frac}(R)$. We say that a polynomial $f(y) \in R[y]$ is primitive if its coefficients have no common prime factor.

(a) If $p \in R$ is prime, let $f(y) \mapsto \bar{f}(y)$ denote the map $R[y] \to R/(p)[y]$ defined by reducing coefficients mod p. Prove that this is a ring homomorphism.

(b) If $f, g \in R[y]$ are primitive, prove that the product fg is also primitive. [Hint: Let f, g be primitive and let p be a prime dividing all the coefficients of fg. This implies that $0 = \overline{fg} = \bar{f}\bar{g}$. Conclude that $\bar{f} = 0$ or $\bar{g} = 0$.]

(c) Given any $h(y) \in K[y]$ show that we can write $h(y) = \alpha h_0(y)$ where $\alpha \in K^\times$ and $h_0(y) \in R[y]$ is primitive.

(d) Consider $f, g \in R[y]$ with g primitive. If $f = gh$ with $h \in K[y]$, prove that we actually have $h \in R[y]$. [Hint: By part (c) we can write $h = \alpha h_0$ with $\alpha \in K^\times$ and $h_0 \in R[y]$ primitive. Then by part (b) we have $f = \alpha g h_0$ with $gh_0 \in R[y]$ primitive. Since the coefficients $a_1, \ldots, a_n \in R$ of gh_0 are coprime and since R is a PID, there exist $b_1, \ldots, b_n \in R$ such that $1 = a_1 b_1 + \cdots a_n b_n$. We conclude that

$$\alpha = \alpha \cdot 1 = \alpha \left(\sum a_i b_i\right) = \sum (\alpha a_i) b_i \in R.]$$

Proof. Let R be a PID. For part (a), let $p \in R$ be prime and for all $f(y) = \sum_k a_k y^k \in R[y]$ we define $\bar{f}(y) = \sum_k (a_k + (p)) y^k \in R/(p)[y]$. Note that for $f(x) = \sum_k a_k y^k, g(y) = \sum_k b_k y^k \in R[y]$ we have

$$\begin{aligned}
\overline{\sum_k a_k y^k} + \overline{\sum_k b_k y^k} &= \sum_k (a_k + (p)) y^k + \sum_k (b_k + (p)) y^k \\
&= \sum_k \left((a_k + (p)) + (b_k + (p)\right) y^k \\
&= \sum_k \left((a_k + b_k) + (p)\right) y^k \\
&= \overline{\sum_k (a_k + b_k) y^k} \\
&= \overline{\sum_k a_k y^k + \sum_k b_k y^k}.
\end{aligned}$$

and

$$\begin{aligned}
\overline{\sum_k a_k y^k} \cdot \overline{\sum_k b_k y^k} &= \sum_k (a_k + (p))y^k \sum_k (b_k + (p)y^k \\
&= \sum_k \left(\sum_{i+j=k} (a_i + (p))(b_j + (p)) \right) y^k \\
&= \sum_k \left((\sum_{i+j=k} a_i b_j) + (p) \right) y^k \\
&= \overline{\sum_k (\sum_{i+j=k} a_i b_j) y^k} \\
&= \overline{\sum_k a_k y^k \cdot \sum_k b_k y^k}
\end{aligned}$$

Then since $\overline{1_R} = 1_R + (p) = 1_{R/(p)}$ we conclude that $f \mapsto \bar{f}$ is a ring homomorphism.

For part (b), let $f, g \in R[y]$ be primitive and assume for contradiction that fg is not primitive, i.e., there exists a prime $p \in R$ that divides all the coefficients of fg. Reducing the coefficients mod p then gives

$$0 = \overline{fg} = \bar{f}\bar{g} \in R/(p)[y],$$

where the last equality follows from part (a). Since $p \in R$ is prime we know that $R/(p)$ and hence $R/(p)[y]$ is a domain. Thus $\bar{f}\bar{g} = 0$ implies that $\bar{f} = 0$ or $\bar{g} = 0$. But this means that either f or g is **not** primitive because p divides each of its coefficients. Contradiction.

For part (c), let $0 \neq h(y) = \sum_k \frac{a_k}{b_k} y^k \in K[y]$, where $a_k, b_k \in K$ with $b_k \neq 0$ for all k. First let $b := \prod_k b_k \neq 0$ so that $a'_k := b\frac{a_k}{b_k} \in R$ for all k and hence $bh(y) = \sum_k a'_k y^k \in R[y]$. Then let a be the greatest common denominator of the coefficients a'_k, which exists because R is a PID and the a'_k are not all zero (in fact, the gcd would exist even if R were just a UFD). We conclude that the polynomial

$$h_0(y) := \frac{b}{a} h(y) = \sum_k \frac{a'_k}{a} y^k \in R[y]$$

is primitive, hence we have $h(y) = \frac{a}{b} h_0(y)$ as desired. Right now $\frac{a}{b} \in K$ looks like a fraction, but we will see that it's not.

For part (d), consider $f, g \in R[y]$ with g primitive, and suppose that $f = gh$ for some $h \in R[y]$. By part (c) we can write $h = \alpha h_0$ for some $\alpha \in K^\times$ and **primitive** $h_0(y) \in R[y]$. By part (b) we know that $gh_0 = \sum_k a_k y^k$ is also primitive. Since R is a PID this allows us to write $1 = \sum_k a_k b_k$ for some $b_k \in K$ (use Bézout's identity and induction). Since

$$\sum_k (\alpha a_k) y^k = \alpha \sum_k a_k y^k = \alpha g h_0 = g(\alpha h_0) = gh = f \in R[y],$$

we know that $\alpha a_k \in R$ for all k. Thus we have

$$\alpha = \alpha \cdot 1 = \alpha \sum_k a_k b_k = \sum_k (\alpha a_k) b_k \in R,$$

and we conclude that $h(y) = \alpha h_0(y) \in R[y]$, as desired. $\square$

[Note that parts (a)-(c) above hold even if R is only a UFD. Part (d) is special to PIDs.]

Problem 3. **($\mathbb{Z}[y]$ and $K[x,y]$ are UFDs)** Recall that a domain R is a UFD if every element factors into prime elements, times a unit. In this case the prime factors are unique up to associates. If R is a PID, you will prove that $R[y]$ is a UFD.

(a) Show that every polynomial $f(y) \in R[y]$ can be factored as

$$f(y) = up_1p_2 \cdots p_k q_1(y)q_2(y) \cdots q_\ell(y),$$

where $u \in R^\times$ is a unit, $p_1, \ldots, p_k \in R$ are irreducible constants, and $q_1, \ldots, q_\ell \in R[y]$ are irreducible **primitive** polynomials of degree ≥ 1. [Hint: Let $K = \mathrm{Frac}(R)$. First factor $f(y)$ into irreducibles in $K[y]$. Use Problem 2(c) and 2(d) to write $f(y) = cq_1(y) \cdots q_\ell(y)$ with $c \in R$. Then factor c in R.]

(b) If $p \in R$ is an irreducible constant, prove that $p \in R[y]$ is prime. [Hint: If p divides $g(y)h(y)$ in $R[y]$ show that p divides every coefficient of $g(y)h(y)$. If $f \mapsto \bar{f}$ is the reduction homomorphism $R[y] \to R/(p)[y]$ then we have $0 = \overline{gh} = \bar{g}\bar{h}$. Now use the fact that p is irreducible in R.]

(c) If $f(y) \in R[y]$ is irreducible and primitive, show that $f(y) \in R[y]$ is prime. [Hint: Let $K = \mathrm{Frac}(R)$. Problem 2(d) says that if $f(y)$ is irreducible in $R[y]$ then $f(y)$ is irreducible (hence prime) in the PID $K[y]$. Suppose that $f(y)$ divides $g(y)h(y)$ in $R[y]$, and hence also in $K[y]$. It follows that $f(y)$ divides $g(y)$ or $h(y)$ in $K[y]$. Now what?]

Proof. Let R be a PID and consider any $0 \neq f(y) \in R[y]$. If $f(y)$ is a constant then we can use the fact that PIDs are Noetherian to write $f(y) = up_1 \cdots p_k$ where $p_1, \ldots, p_k$ are irreducible elements of R. (See Problem 4(c) below.) Otherwise, assume that $\deg(f) \geq 1$. Then we can use the fact that $K[y]$ is a PID (hence Noetherian) to write

$$f(y) = \alpha f_1(y)f_2(y) \cdots f_\ell(y)$$

where $\alpha \in K^\times$ and $f_1(y), \ldots, f_\ell(y)$ are irreducible (hence nonconstant) polynomials in $K[y]$. We use Problem 2(c) to write $f_i(y) = \alpha_i q_i(y)$ where $\alpha_i \in K^\times$ and $q_i(y) \in R[y]$ is primitive for all i. Then we have

$$f(y) = \alpha\alpha_1\alpha_2 \cdots \alpha_\ell q_1(y)q_2(y) \cdots q_\ell(y),$$

where $q_1(y) \cdots q_\ell(y) \in R[y]$ is primitive by Problem 2(b), and hence Problem 2(d) implies that $a := \alpha\alpha_1 \cdots \alpha_\ell \in R$. Finally, we factor a as an element of R. This completes part (a). Now we will show that the factors $u, p_1, \ldots, p_k, q_1(y), \ldots, q_\ell(y)$ are all **prime** elements of $R[y]$.

For part (b), let $p \in R$ be irreducible in R. We want to show that p is a prime element of $R[y]$. So suppose that we have $f(y)g(y) = ph(y)$ for some $f, g, h \in R[y]$. Reducing the coefficients mod p gives $0 = \overline{ph} = \overline{fg} = \bar{f}\bar{g}$ by Problem 2(a). Then since $R/(p)[y]$ is a domain we have $\bar{f} = 0$ (i.e., p divides $f(y)$) or $\bar{h} = 0$ (i.e., p divides $g(y)$). We have shown that $p|f(y)g(y)$ implies $p|f(y)$ or $p|g(y)$ in $R[y]$.

For part (c), let $f(y) \in R[y]$ be irreducible and primitive. We will show that $f(y)$ is prime. (Note that Euclid's Lemma is not immediately available to us because $R[y]$ is not a PID.) Let $K = \mathrm{Frac}(R)$ and consider $f(y) \in K[y]$. I claim that $f(y)$ is irreducible in $K[y]$. Indeed, if we have $f(y) = g(y)h(y)$ with nonzero, nonconstant $g, h \in K[y]$, then we can use Problem 2(c) to write $h(y) = \alpha h_0(y)$ with $h_0(y) \in R[y]$ primitive. Then since $f(y) = \alpha g(y)h_0(y)$, Problem 2(d) tells us that $\alpha g(y)$ is in $R[y]$, hence $f(y)$ is **reducible** in $R[y]$. We have show that reducible in $K[y]$ implies reducible in $R[y]$; in other words, irreducible in $R[y]$ implies irreducible in $K[y]$. Now since $K[y]$ is a PID we may use Euclid's Lemma to conclude that $f(y)$ is prime in $K[y]$. Finally, suppose that $f(y)$ divides $g(y)h(y)$ for some $g, h \in R[y]$. It follows that f divides g or h in $K[y]$. Using Problem 2(d) again, we conclude that f divides g or h in $R[y]$. $\square$

[We just proved an absolutely fundamental result, which nevertheless is not easy. In fact I would call it tricky. If you want something even trickier, look back over the proof and show that it still works if R is only a UFD. The result that

$$R \text{ UFD} \Longrightarrow R[y] \text{ UFD}$$

is sometimes humorously referred to as "Gauss' Lemma". By induction we conclude that if R is a UFD then $R[x_1, x_2, \ldots, x_n]$ is a UFD for any number of variables. Most books on Algebraic Geometry will begin by assuming that you know this.]

Problem 4. (Nonmaximal primes in $\mathbb{Z}[y]$ and $K[x, y]$) Let R be a ring that is not a field. You will show that $R[y]$ has a nonmaximal prime ideal.

(a) Given an ideal $I \leq R$, prove that the set

$$I[y] := \left\{ \sum_k a_k y^k \in R[y] : a_k \in I \text{ for all } k \right\}.$$

is an ideal of $R[y]$ and that we have $(R[y])/(I[y]) \approx (R/I)[y]$. [Hint: Show that the map $R[y] \to (R/I)[y]$ defined by $\sum_k a_k y^k \mapsto \sum_k (a_k + I) y^k$ is a ring homomorphism.]

(b) Since R is not a field, Zorn's Lemma (i.e., the Axiom of Choice) implies that R contains a maximal (hence prime) ideal $(0) < P < (1)$. (You don't need to prove this.) Show that $P[y]$ is a prime ideal of $R[y]$ that is not maximal. [Hint: Show that $(R/P)[y]$ is a domain but not a field.]

(c) If R is a PID but not a field, show that there exists a prime ideal $(0) < (p) < (1)$ without using the Axiom of Choice.

Proof. We saw in Problem 1 that $\mathbb{Z}[y]$ and $K[x, y]$ are not PIDs. Now we will show more explicitly that they contain nonmaximal primes. We will not yet be fully explicit (stay tuned).

Given an ideal $I \leq R$, the map $R[y] \to (R/I)[y]$ that reduces coefficients mod I is a ring homomorphism for the same reason as in Problem 2(a). Note that this map is surjective and its kernel is $I[y]$. Hence $I[y]$ is an ideal and we have $R[y]/I[y] \approx (R/I)[y]$, proving part (a).

For part (b), let $P \leq R$ be a nontrivial prime ideal. Since R/P is a domain we know that $(R/P)[y]$ is also a domain, and it follows that $P[y] \leq R[y]$ is a prime ideal. However, $(R/P)[y]$ is not a field. Indeed, the element $y + P \in (R/P)[y]$ has no inverse because if $(y + P)f(y) = 1 + P$ then $0 = \deg(1 + P) = \deg(y + P) + \deg(f) = 1 + \deg(f) \geq 1$. We conclude that $R[y]/P[y]$ is not a field, hence $P[y] \leq R[y]$ is not a maximal ideal.

For part (c), let R be a PID that is not a field, so there exists a nontrivial ideal $(0) < (a) < (1)$. If a is irreducible then (a) is maximal (hence prime) and we are done, so suppose that we have $a = a_1 b_1$ for some $(a) < (a_1), (b_1) < (1)$. If either a_1 or b_1 is irreducible then we are done, so suppose without loss of generality that $a_1 = a_2 b_2$ for some $(a_1) < (a_2), (b_2) < (1)$. Now assume for contradiction that this process never stops. We obtain an infinite increasing chain of ideals:

$$(a) < (a_1) < (a_2) < (a_3) < \cdots.$$

Let $J = (a) \cup_{i \geq 1} (a_i)$ be the infinite union of these ideals. It is straightforward to check that J is an ideal, and since R is a PID this implies that $J = (b)$. Finally, since $b \in J$ there exists N such that $b \in J_N$ and we have a contradiction:

$$J = (b) \leq J_N < J_{N+1} \leq J.$$

$\square$

[We just (re)proved that PIDs are Noetherian. Recall that this is one of the two steps in the proof that PIDs are UFDs. The other step is Euclid's Lemma.]