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?

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.

Problem 2. (Gauss' Lemma) Let R be a PID with field of fractions $K = \text{Frac}(R)$. 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 $g h_0 \in R[y]$ 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

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

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

$$f(y) = u p_1 p_2 \cdots p_k q_1(y) q_2(y) \cdots q_\ell(y),$$

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 $K = \text{Frac}(R)$. First factor $f(y)$ into irreducibles in $K[y]$. Use Problem 2(c) and 2(d) to write $f(y) = c q_1(y) \cdots q_\ell(y)$ 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 $K = \text{Frac}(R)$. 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?]

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 $R[x]$ has a nonmaximal prime ideal.

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

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

is an ideal of $R[x]$ and that we have $(R[x])/(I[x]) \approx (R/I)[x]$. [Hint: Show that the map $R[x] \to (R/I)[x]$ defined by $\sum_k a_k x^k \mapsto \sum_k (a_k + I) x^k$ 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 $(0) < P < R$. (You don't need to prove this.) Show that $P[x]$ is a prime ideal of $R[x]$ that is not maximal. [Hint: Show that $(R/P)[x]$ 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.