Math 662 **Spring 2014**
Homework 1 **Drew Armstrong**

Problem 0 (Drawing Pictures). Sketch the curves $y^2 = f(x)$ in $\mathbb{R}^2$ for the following polynomials $f(x) \in \mathbb{R}[x]$: $f(x) = x^3$ and $f(x) = (x+1)(x^2+\varepsilon)$ for $\varepsilon < 0$, $\varepsilon = 0$, $\varepsilon > 0$. [Hint: First sketch $y = f(x)$ then sketch $y = \pm\sqrt{f(x)}$.]

What is a polynomial? Let R be a ring and let x be a formal symbol. A polynomial is a formal expression $a_0 + a_1x^1 + a_2x^2 + \cdots$ in which all but finitely many of the coefficients $a_i \in R$ are zero. If we define addition and multiplication by

$$\sum_k a_k x^k + \sum_k b_k x^k := \sum_k (a_k + b_k) x^k$$

and

$$\left(\sum_k a_k x^k\right)\left(\sum_\ell b_\ell x^\ell\right) := \sum_m \left(\sum_{k+\ell=m} a_k b_\ell\right) x^m,$$

then the set of polynomials becomes a ring which we call $R[x]$. Note that R is naturally embedded in $R[x]$ as a subring via the map $a \mapsto a + 0x + 0x^2 + \cdots$. We define the degree $\deg(f)$ of a nonzero polynomial $f(x) = \sum_k a_k x^k$ as the largest k such that $a_k \neq 0$ (this a_k is called the leading coefficient), and we define the degree of the zero polynomial as $\deg(0) = -\infty$ (but this is rather arbitrary). We consider the symbols $1, x, x^2, \ldots$ to be linearly independent over R, and therefore we have $\sum_k a_k x^k = \sum_k b_k x^k$ if and only if $a_k = b_k$ for all k. This makes $R[x]$ into an infinite-dimensional "free" module over R.

Problem 1 (The Division Algorithm). We say that a polynomial $g(x) \in R[x]$ is monic if its leading coefficient is a unit. Consider polynomials $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ in $R[x]$ with $g(x)$ monic.

(a) Prove that **there exist** polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$ (this includes the case $r(x) = 0$ since $\deg(0) = -\infty < \deg(g)$ for any g). [Hint: Use induction on $\deg(f)$. Assume that $\deg(g) = m \geq 0$ with leading coefficient $b_m \in R^\times$. If $\deg(f) < m$ then we can take $q(x) = 0$ and $r(x) = f(x)$, so the assertion is true. Now suppose that $\deg(f) = n \geq m$ and consider the polynomial $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$. Since $\deg(f_1) < n$ there exist $q_1(x), r(x)$ with $f_1(x) = q_1(x)g(x) + r(x)$ and $\deg(r) < \deg(g)$.]

(b) Prove that the polynomials $q(x), r(x)$ from part (a) are **unique**. [Hint: Assume that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$ with $\deg(r_1), \deg(r_2) < \deg(g)$. Since $g(x)$ is monic, note that $\deg(gh) = \deg(g) + \deg(h)$ for any nonzero $h(x) \in R[x]$. Note that $\deg(r_2 - r_1) \leq \max\{\deg(r_1), \deg(r_2)\}$. Now assume that $r_2(x) - r_1(x) \neq 0$ and show that this leads to a contradiction.]

(c) Give an example where $g(x)$ is not monic and the polynomials $q(x), r(x)$ do not exist.

[By uniqueness we can speak of "the" remainder when $f(x)$ is divided by monic $g(x)$. We will write $g|f$ (and say "g divides f") if and only if the remainder is zero.]

Problem 2 (Descartes' Theorem). Let R be a ring (i.e. commutative).

(a) If $\alpha \in R$ is any element, we define a function $\mathsf{ev}_\alpha : R[x] \to R$ by sending $\sum_k a_k x^k \in R[x]$ to $\sum_k a_k \alpha^k \in R$. Prove that this function (called "evaluation at α") is a morphism of rings. For simplicity we will write $f(\alpha) := \mathsf{ev}_\alpha(f(x))$.

(b) Consider a polynomial $f(x) \in R[x]$ and an element $\alpha \in R$. Prove that we have $(x - \alpha)|f(x)$ if and only if $f(\alpha) = 0$. [Hint: Divide $f(x)$ by $(x - \alpha)$ and evaluate at α.]

Problem 3 (Localization of a Ring). The construction of the field of fractions of a domain can be generalized to arbitrary rings as follows. Let R be a ring and let $S \subseteq R$ be any subset closed under multiplication and containing 1 (we can say that S is a subsemigroup of $(R, \times, 1)$). We define the set of formal symbols

$$R[S^{-1}] := \left\{ \left[\frac{a}{b}\right] : a, b \in R, b \in S \right\}$$

and we declare that

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \iff \exists\, u \in S \text{ such that } u(ad - bc) = 0.$$

(a) Prove that this is an equivalence relation.

(b) Prove that the algebraic operations

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right]$$

and

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad + bc}{bd}\right]$$

are well-defined. It follows (don't prove this) that $R[S^{-1}]$ is a ring.

(c) Prove that $R[S^{-1}] = 0$ if and only if S contains 0.

(d) Prove that the natural map $R \to R[S^{-1}]$ defined by $a \mapsto \left[\frac{a}{1}\right]$ is a ring homomorphism.

(e) We say that $u \in R$ is a $\mathsf{zerodivisor}$ if there exists $v \in R$ such that $uv = 0$. If S contains no zerodivisors, prove that the natural map $R \to R[S^{-1}]$ is injective. (This holds in particular when R is a domain and $0 \notin S$.)

(f) If $P \subseteq R$ is a prime ideal, show that $S := R - P$ is a subsemigroup of R. The localization $R[S^{-1}]$ is denoted as R_P and is called the localization of R at the prime P. We will discuss the geometric meaning of this later.

Problem 4 (Localization of $\mathbb{Z}$).

(a) Let $p \in \mathbb{Z}$ be prime and consider the localization $\mathbb{Z}_{(p)}$ at the prime ideal (p):

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\}.$$

Prove that this ring has a unique nontrivial **maximal** ideal. [Hint: What are the units of $\mathbb{Z}_{(p)}$? Recall that an ideal is the whole ring if and only if it contains a unit.] A ring with a unique nontrivial maximal ideal is called a local ring.

(b) Prove that every ring $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ between $\mathbb{Z}$ and $\mathbb{Q}$ is a localization of $\mathbb{Z}$. [Hint: Since R is a subring of $\mathbb{Q}$ it consists of fractions. Let S be the set of denominators that occur in elements of R. Prove that $R = \mathbb{Z}[S^{-1}]$.]