21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc Tartar, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

Assignment 6 - Saturday October 15, 2011. Due Monday October 24

Exercise 36: Let R be an integral domain equipped with a function V from $R \setminus \{0\}$ into $\mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = b\,q + r$ and either $r = 0$ or $r \neq 0$ and $V(r) < V(b)$. For a non-zero $x \in R$, one defines $W(x) = \min\{V(x\,y) \mid y \in R, y \neq 0\}$. Show that $W(\xi\,\eta) \geq W(\xi)$ for all non-zero $\xi, \eta \in R$, and that for all $a, b \in R$ with $b \neq 0$ there exist $q_*, r_* \in R$ such that $a = b\,q_* + r_*$ and either $r_* = 0$ or $r_* \neq 0$ and $W(r_*) < W(b)$.

Exercise 37: Let R be a commutative unital ring.
i) Show that if $a_1, \ldots, a_n \in R$ are nilpotent, then $a_1 x + \ldots + a_n x^n$ is nilpotent in $R[x]$, and $1 + a_1 x + \ldots + a_n x^n$ is a unit in $R[x]$ (i.e. it has an inverse in $R[x]$).
ii) Show that $a_0 + a_1 x + \ldots + a_n x^n$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent.

Exercise 38: Let $P(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ with $a_n \neq 0$. Suppose that for some prime p and some k such that $0 < k < n$ one has p divides a_i for $i = 0, \ldots, k-1$, but p divides neither a_k nor a_n, and p^2 does not divide a_0. Show that P has a factor Q of degree at least k which is irreducible in $\mathbb{Z}[x]$ (the excluded case $k = n$ corresponds to Eisenstein's criterion).

Exercise 39: i) Show that all the integer solutions of $x^3 = y^2 + 2$ have x and y odd.
ii) $\mathbb{Z}[\sqrt{-2}] = \{a + i\sqrt{2}\,b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a Unique Factorization Domain, so that every element which is not a unit (here ± 1) has a factorization as a product of irreducible elements, unique up to reordering the factors or replacing them by associates. Deduce that any integer solution of $x^3 = y^2 + 2$ satisfies $y \pm \sqrt{-2} = (a \pm b\sqrt{-2})^3$ for some $a, b \in \mathbb{Z}$.
iii) Find all the integer solutions of $x^3 = y^2 + 2$.

Exercise 40: One says that an ideal P in a ring R is prime if $P \neq R$ and if for any two ideals A, B of R satisfying $A\,B \subset P$ one has $A \subset P$ or $B \subset P$ (recall that $A\,B$ is the set of finite sums of terms like $a\,b$ with $a \in A$ and $b \in B$). Let R be a unital ring (not necessarily commutative).
i) Show that if P is a prime ideal and A is an ideal such that $A^n \subset P$ for some $n \geq 1$, then one has $A \subset P$ (recall that A^n is the set of finite sums of terms like $a_1 \cdots a_n$ with $a_i \in A$ for $i = 1, \ldots, n$).
ii) Show that if P is a prime ideal and $r, s \in R$ are such that $r\,R\,s \subset P$, then $(r)\,(s) \subset P$, so that $r \in P$ or $s \in P$.

Exercise 41: i) Show that if J is a prime ideal in a commutative ring R, then $Rad(J) = J$.
ii) In the case $R = \mathbb{Z}$, show that every ideal J is such that $Rad(J)$ is the intersection of all the prime ideals containing J.

Exercise 42: For a ring R, the ring of formal power series $R[[x]]$ is made of the sequences $(a_0, a_1, \ldots)$ interpreted as $A = a_0 + a_1 x + \ldots$ with the natural operations: if $B = b_0 + b_1 x + \ldots$, then $A + B = C$ and $A\,B = D$ have coefficients $c_k = a_k + b_k$, $d_k = \sum_{j=0}^{k} a_j b_{k-j}$ for $k = 0, \ldots$. If R is an integral domain, then $R[[x]]$ is an integral domain, hence it has a field of fractions. Find necessary conditions for an element $q_0 + q_1 x + \ldots \in \mathbb{Q}[[x]]$ to be equal to $\frac{A}{B}$ for $A, B \in \mathbb{Z}[[x]]$ with $B \neq 0$, and deduce that the field of fractions of $\mathbb{Z}[[x]]$ is strictly smaller than the field of fractions of $\mathbb{Q}[[x]]$.