October 31st, 2015

Remark on Exercise sheet 2

Dr. V. Di Proietto

Remark 1. If A is a ring, then $A[X]$ is not necessarily an Euclidean domain. In particular it is not true that given polynomials $f(X) \in A[X]$ and $b(X) \in A[X]$ such that $b(X) \neq 0$, then there exist polynomials $q(X), r(X) \in A[X]$ such that

$$f(X) = q(X)b(X) + r(X)$$

with $\deg(r(X)) < \deg(b(X))$.

For example for $A = \mathbb{Z}$, $f(X) = X$, $b(X) = 3$, suppose the existence of $q(X), r(X) \in \mathbb{Z}[X]$ such that

$$X = q(X)3 + r(X) \tag{1}$$

and $\deg(r(X)) < 0$. It would follow $\deg(r(X)) = -\infty$, so $r(X) = 0$ and equation (1) becomes

$$X = q(X)3$$

which has not solution in $\mathbb{Z}[X]$, leading to the contradiction.

Let us consider another example. Let A be a ring, denote by B the polynomial ring $A[Y]$, and consider the ring $B[X] = A[Y, X]$. The ring $B[X]$ is not an Euclidean domain: for instance, given $f(X) = X \in B[X]$ and $g(X) = Y \in B[X]$, the equation

$$X = q(X)Y + r(X)$$

cannot be satisfied if we require that $\deg_X(r(X)) < \deg_X Y = 0$. In the solution to exercise 3 we used the Euclidean algorithm in $A[X, Y]$, which is not an Euclidean domain. But we could do this because in $B[X] = A[Y, X]$ the polynomial $X^m - Y^n$ has invertible leading coefficient in $B[X]$, and then given $h(X, Y)$ and $X^m - Y^n$ there exist $q(X, Y)$ and $r(X, Y) \in B[X]$ such that

$$h(X, Y) = q(X, Y)(X^m - Y^n) + r(X, Y)$$

with $\deg_X(r(X, Y)) < m$. This is an application of the following

Theorem 2 ([Lan02], Theorem 1.1)**.** *Let B be a ring and let $h(X)$ and $b(X)$ be polynomials in one variable of degree ≥ 0, and* assume that the leading coefficient of $b(X)$ is a unit in B. *Then there exist unique polymonials $q(X)$, $r(X) \in B[X]$ such that*

$$h(X) = q(X)b(X) + r(X)$$

and $\deg(r(X)) < \deg(b(X))$.

Remark 3. In what follows I want to give the proofs of some result you need to prove exercise 5, which I did in an uncler way at the board last friday.

Proposition 4. *Let A, A_1, A_2 be rings, and we suppose that $A = A_1 \times A_2$. Let I be an ideal of A, then $I = I_1 \times I_2$, with I_i ideal of A_i for $i = 1, 2$. Moreover $A/I = A_1/I_1 \times A_2/I_2$.*

Proof. We consider $I_i := \{a \in A \,|\, (a, 0) \in I\}$ for $i = 1, 2$. Then I_i is an ideal of A for $i = 1, 2$. Indeed $I_i = \pi_i(I)$ where $\pi_i : A_1 \times A_2 \to A_i$ is the natural projecion, and I_i is an ideal of A_i for $i = 1, 2$. We want to prove that $I = I_1 \times I_2$. Clearly $I_1 \times I_2 \subset I_1 \times 0 + 0 \times I_2$. If $a \in I_1 \times I_2$, then $a = (a_1, a_2)$, with $a_1 \in I_1$ and $a_2 \in I_2$, but $(a_1, a_2) = (a_1, 0) + (0, a_2)$ and $(a_1, 0) \in I$ and $(0, a_2) \in I$, hence $I_1 \times I_2 \subset I_1 \times 0 + 0 \times I_2 \subset I$. Viceversa if $a \in I$, then in particular $a \in A$, hence $a = (a_1, a_2)$ with $a_i \in A_i$ for $i = 1, 2$. Then $(1, 0)(a_1, a_2) = (a_1, 0) \in I$, and $(0, 1)(a_1, a_2) = (0, a_2) \in I$ and by definition of I_1 and I_2, $a_1 \in I_1$ and $a_2 \in I_2$. Hence $I \subset I_1 \times I_2$.

We consider the homomorphism of rings $A \to A_1/I_1 \times A_2/I_2$ which sends $(a_1, a_2) \in A$ to $(a_1 + I_1, a_2 + I_2)$. This is surjective and the kernel is the ideal I. Hence by the theorem of homomorphism $A/I = A_1/I_1 \times A_2/I_2$ □

Remark 5. If G, G_1, G_2 are groups such that $G = G_1 \times G_2$, then there exist subgroups of G which are not products of subgroups of G_1 and G_2. Can you find examples?

Proposition 6. *Let A, A_1, A_2 be rings, and suppose that $A = A_1 \times A_2$. Let I be an ideal of A, then $I = I_1 \times I_2$, and I is prime if and only if $I_1 = P_1$ where P_1 is a prime of A_1 and $I_2 = A$ or if $I_1 = A$ and $I_2 = P_2$, where P_2 is a prime ideal of A_2.*

Proof. If $I = P_1 \times A_2$, with P_1 a prime ideal of A_1 then I is a prime ideal of A; indeed let $(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2) \in P_1 \times A_2$, then $a_1b_1 \in P_1$ which is a prime ideal of A_1, hence a_1 or b_1 are in P_2, hence (a_1, a_2) or (b_1, b_2) are in $P_1 \times A_2$.

Viceversa if I is a prime ideal of A, then by Proposition 4, $I = I_1 \times I_2$ and $A/I = A_1/I_1 \times A_2/I_2$. Since A/I is a domain, then $A_1/I_1 = 0$ or $A_2/I_2 = 0$. Indeed $(1, 0)(0, 1) = (0, 0)$ implies that $(1, 0) = (0, 0)$ or $(0, 1) = (0, 0)$, but if $(1, 0) = (0, 0)$ in $A/I = A_1/I_1 \times A_2/I_2$, then every element of the form $(a, 0) = (0, 0)$ in $A_1/I_1 \times A_2/I_2$, hence $A_1/I_1 = 0$. If $A_1/I_1 = 0$ then $A/I = A_2/I_2$ and I_2 is a prime ideal of A_2. An analogous result holds if $(0, 1) = (0, 0)$. □

References

[Lan02] S. Lang, *Algebra*, Springer-Verlag, 2002.