Noetherian rings and the Hilbert basis theorem

From now on we will assume that all rings, unless otherwise stated, are commutative and have an identity element $1 \neq 0$.

Let R, R' two rings. A map $\phi : R \to R'$ will be called a homomorphism if:

- $\phi(x + y) = \phi(x) + \phi(y)$ for every $x, y \in R$
- $\phi(xy) = \phi(x)\phi(y)$ for every $x, y \in R$
- $\phi(1) = 1$

The kernel of a homomorphism $\phi : R \to R'$ is by definition the set:

$$\ker\phi = \{x \in R : \phi(x) = 0\}$$

This is a subgroup of R and it also has the property that if $x \in \ker(\phi)$ and $y \in R$ then $xy \in \ker(\phi)$. This motivates the following definition:

Definition 0.1 *A subgroup I of a ring R is called an ideal if for every $x \in I$ and $y \in R$, we have that $xy \in I$.*

According to the above definition, nothing prevents the ideal from coinciding with the ring R. From now one we will be making the assumption that, unless otherwise stated, an ideal will not contain the identity, in other words it will be a *strict* ideal. Also, the ideal (0) will be usually referred to as the *trivial* ideal.

For every ideal I of the ring R the group R/I can be naturally given the structure of a ring so that the quotient (group) homomorphism:

$$q : R \to R/I$$

is a ring homomorphism. This is usually referred to as the *natural epimorphism* associated with the ideal I.

We recall that a ring R is called an integral domain if it has no zero-divisors, i.e. whenever $xy = 0$ then either $x = 0$ or $y = 0$. Also an ideal I will be called prime if whenever $xy \in I$ either $x \in I$ or $y \in I$. This definition is clearly motivated by the ideals $p\mathbb{Z}$ of $\mathbb{Z}$ for p prime number. We have a natural connection between prime ideals and integral domains:

Proposition 0.1 *Let I be an ideal of the ring R. Then the quotient R/I is an integral domain if and only if I is prime.*

Proof: Chasing definitions.

□

We also recall that a ring, in which every non-zero element has a multiplicative inverse, is called a field. A simple remark gives us:

Proposition 0.2 *A ring R is a field if and only if it has no non-trivial ideals.*

An ideal I of R is called *maximal* if it is not contained in any strictly larger ideal. Then we have that an ideal I is maximal if and only if the quotient R/I is a field. A standard application of Zorn's lemma also gives us that any ideal is contained in a maximal ideal.

Definition 0.2 *The set of prime ideals of a ring R will be denoted by $specR$ and the set of maximal ideals will be denoted by $m\text{-}specR$.*

If F is a field then the maximal ideals of $F[x]$ are in one-to-one correspondence with monic irreducible polynomials. If F is further algebraically closed then the maximal ideals are in one-to-one correspondence with the elements of F.

Let R be a ring and I an ideal of R. Then a subset $A \subset R$ is said to generate I if:

$$I = \{x_1y_1 + x_2y_2 + ... + x_ny_n | x_i \in A, y_i \in R\}$$

A will be also called a set of generators. If an ideal I has a finite set of generators, then it is called finitely generated. An ideal I is called *principal* if it is generated by just one element $a \in R$. Such an ideal is denoted by (a). We have the very important:

Definition 0.3 *A ring R is called Noetherian if every ideal $I \subset R$ is finitely generated. Also, a ring R is called a principal ideal domain (p.i.d.) if every ideal in R is principal.*

We have the following important characterization of Noetherian rings:

Proposition 0.3 *A ring R is Noetherian if and only if every increasing sequence of ideals:*

$$I_1 \subset I_2 \subset I_3 \subset ...$$

is eventually constant.

Proof: Let R be Noetherian and $\{I_n\}$ an increasing sequence of ideals. Then $\bigcup I_n$ is also an ideal and since R is Noetherian it is finitely generated, say, by $a_1, ..., a_m$ Since the a_i's are elements of the union $\bigcup I_n$, they are each contained in some I_n. But if we take the ideal with the largest index, then it will contain all of them and it will, thus, coincide with the union.

For the converse, notice that if an ideal $I \subset R$ is not finitely generated, then one can inductively define a strictly increasing sequence of ideals as follows: Let $x_1 \neq 0$ be in I. Then set $I_1 = (x)$. We have that $I \neq I_1$, otherwise I would be finitely generated. So there is $x_2 \in I - I_1$. Let now $I_2 = (x_1, x_2)$. Then $I \neq I_2$ and thus we can find $x_3 \in I - I_2$. We set $I_3 = (x_1, x_2, x_3)$ and continue in the same fashion.

□

One of the early and most important theorems of Commutative algebra is:

Theorem 0.1 *(Hilbert basis theorem). Let R be a Noetherian ring. Then $R[x]$ is also Noetherian.*

Proof: Let J be a non-trivial ideal of $R[x]$ and m the least degree of a non-zero polynomial in J. Then for $n \geq m$ define:

$$I_n = \{a \in R | a \text{ is the leading coefficient of an n-th degree polynomial in } J\} \bigcup \{0\}$$

It is a routine to check that the I_n's are ideals of R and that $I_n \subset I_{n+1}$. Since R is a Noetherian ring, each of the I_n is finitely generated and there exists a $k \in \mathbb{N}$ such that $I_n = I_k$ for $n \geq k$. For each n with $m \leq n \leq k$, let A_n be a finite set of polynomials of degree n such that their leading coefficients generate I_n. Let $A = \bigcup A_n$. Then A is a finite set and we will show that it generates J. We will use induction on the degree of a polynomial in J.

If $\deg p(x) = m$ (nothing smaller is possible for a non-zero polynomial!), then there are q_i's in A_m and $a_i \in R$ such that the leading coefficient of $p(x)$ coincides with the leading coefficient of $\sum a_i q_i(x)$. This means that $p(x) - \sum a_i q_i(x)$ has degree strictly less than m, which implies that it is the zero polynomial and our induction is complete for m.

Now, assuming the claim for all naturals between m and n we are going to check it for $n+1$. If $n+1 \leq k$ then there exist $q_i(x)$ in A_{n+1} and $a_i \in R$ such that $p(x) - \sum a_i q_i(x)$ is of degree less than $n+1$. This polynomial can now be written in terms of the elements of A by induction hypothesis. On the other hand, if $n+1 > k$, then there are polynomials of degree n, $q_i(x)$in J and $a_i \in R$ so that the leading coefficient of $p(x)$ coincides with that of $x \sum a_i q_i(x)$. Thus the difference $p(x) - x \sum a_i q_i(x)$ is in J and has degree less than $n+1$. The inductive hypothesis applied both on the $q_i(x)$ and $p(x) - x \sum a_i q_i(x)$ concludes the proof.

□