November 17th, 2015

Number Theory I

Prof. H. Esnault, Dr. V. Di Proietto

Exercise sheet 6[1]

Exercise 1. Recall (from Algebra and Number theory) that a ring A is called a *unique factorization domain* (*UFD*) if every element $a \in A$ which is neither zero nor a unit can be written as a product of prime elements $a = p_1 \cdots p_n$. (An element $p \in A$ is *prime* iff the ideal $(p) \subset A$ is a prime ideal.)

The following is a list of elementary properties of UFD's, which you probably already know. You can prove them again, if you want, but you can also skip them. Then you can use them in the other exercises.

(i) Let A be an integral domain and assume we can write $a \in A$ as a product of prime elements $a = p_1 \cdots p_n$. Show that this presentation is unique up to permutation and multiplication with units, i.e. if $a = p'_1 \cdots p'_m$ with prime elements $p'_i \in A$, then there exists a bijection $\sigma\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ and units $u_i \in A^\times$ such that $p'_i = u_i p_{\sigma(i)}$.

Recall that two prime elements $p, p' \in A$ are *equivalent* if there exists a unit $u \in A^\times$ with $p' = up$. The above result in particular implies, that if A is a UFD, I is the set of equivalence classes of prime elements in A and for each $i \in I$ we pick a representative $p_i \in i$, then any element $a \in A \setminus \{0\}$ can be uniquely written in the form

$$a = u \prod_{i \in I} p_i^{n_i},$$

with $u \in A^\times$ and $n_i \in \mathbb{N}$, $i \in I$, all but finitely many $n_i = 0$.

(ii) Let A be an integral domain. Recall that an element $a \in A \setminus \{0\}$ is *irreducible* if it is not a unit and if whenever we can write $a = bc$, then either $b \in A^\times$ or $c \in A^\times$.

Show that a prime element in A is always irreducible. Show that if A is a UFD, then an irreducible element is also prime.

(iii) Show that a PID is UFD. (*Hint:* First show that in a PID any ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ becomes stationary, i.e., we have $I_n = I_{n+1}$ for all n large enough. Then show that in a PID any non-zero element a which is not a unit can be

[1] If you want your solutions of this exercises to be corrected, please hand them in before the exercise class on November 27th.

written as $a = pa_1$ with p a prime. Continue with a_1 and so on and deduce the statement.)

(iv) Let A be a ring and let $a_1, \ldots, a_n$ be elements of A, we say that d is a greatest common divisor of $a_1, \ldots, a_n$ if
- $d \mid a_i$ for every $i = 1, \ldots n$;
- whenever there exists $a \in A$ such that $a \mid a_i$ for every $i = 1, \ldots, n$, then $a \mid d$.

Prove that if A is UFD, then a greatest common divisor of $a_1, \ldots, a_n$ exists and it is unique up to multiplication by elements of $A^\times$.

(v) (Gauß Lemma) Let A be a UFD. We say a polynomial $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ is *primitive* if a greatest common divisor of a_i for $i = 0, \ldots, n$ is in $A^\times$.

Show that if $f, g \in A[X]$ are primitive then so is fg.

Exercise 2. Let A be an integral domain, and let $K = S^{-1}A$, where $S = A \setminus \{0\}$, be the field of fractions of A.

(i) Let A be a UFD. Show that any $f \in A[X] \setminus \{0\}$ can be written as $f = af_0$ where $f_0 \in A[X]$ is primitive (in the sense of Ex.1, (v)) and $a \in A \setminus \{0\}$.

(ii) Show that if $p \in A$ is a prime element in A then it is also a prime element in $A[X]$.

(iii) Assume that A is a UFD. Show that if $f \in A[X]$ is primitive and its image in $K[X]$ is prime, then $f \in A[X]$ is also prime. (*Hint:* Use (v) of Ex. 1.) Is this still true without the assumption that f be primitive?

(iv) Deduce from (i), (ii) and (iii) above that if A is a UFD then so is $A[X]$. (*Hint:* Notice that we know that $K[X]$ is a PID and hence also a UFD.)

Remark 1. Ex. 1 (iii) and Ex. 2 (iv) together imply that $\mathbb{Z}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$ (K a field) are UFD's.

Exercise 3.

(i) Describe $\operatorname{Spec} \mathbb{Z}[X] := \{P \mid P \text{ is a prime ideal of } \mathbb{Z}[X]\}$

(ii) Show that $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. (*Hint:* To show that 2 is not prime try to factor $6 \in \mathbb{Z}[\sqrt{-5}]$ in two different ways.)

(iii) By Ex. 3 of Exercise sheet 2 the ring $A = K[X, Y]/(Y^2 - X^3)$ is a domain (K a field). Show that $y = \bar{Y} \in A$ is irreducible but not prime. (Thus A is not a UFD.)

Exercise 4. Let A be a ring and let S be a multiplicatively closed subset of A. Prove the following

(i) Show that the prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A which have empty intersection with S.

(ii) Prove that the operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.

(iii) Remember that if $S = A \setminus P$, where P is a prime ideal of A, then $S^{-1}A = A_P$ is a local ring. It is true that for a general multiplicatively closed subset S, the ring $S^{-1}A$ is a local ring?

Exercise 5. Let A be a ring.

(i) Suppose that for each prime ideal P, the local ring A_P has no nilpotent elements $\neq 0$. Show that A has no nilpotent element $\neq 0$.

(ii) If for every prime ideal P, the local ring A_P is an integral domain, is A necessarily an integral domain?