October 26, 2017

Number Theory I (Commutative Algebra)

Hélène Esnault, Exercises: Shane Kelly

Exercise sheet 2

As in the textbook, all rings are commutative with a unit. Recall that an element $a \in R$ of a ring is *irreducible* if $a = bc$ implies that b or c is a unit. Recall that an element $a \in R$ is called *prime* if whenever $ad = bc$ for some $d \in R$, we have $ad' = b$ or $ad' = c$ for some $d' \in R$. (Equivalently, $a \in R$ is a prime element if and only if $\langle a \rangle$ is a prime ideal.)

Exercise 1 ([AK 2017, Paragraph 2.17)**.** Let R be a ring. We will show that if R is a principal ideal domain (PID), then it is a unique factorisation domain (UFD).

(1) Suppose R is a domain. Show that $\langle a \rangle = \langle b \rangle$ if and only if $a = bc$ for some unit c.
(2) Suppose every ascending chain of principal ideals $\langle x_1 \rangle \subset \langle x_2 \rangle \subset \dots$ of R stabilises, that is, there exists $N \in \mathbb{N}$ such that $\langle x_i \rangle = \langle x_{i+1} \rangle$ for all $i \geq N$.
   (a) Show that every nonzero nonunit a factors into a product $a = bc$ such that b is irreducible.
   (b) Deduce that every nonzero nonunit a factors into a product $a = b_1 b_2 \dots b_n$ such that each b_i is irreducible.
(3) Suppose that R is a PID. Show that every ascending chain of ideals stabilises.
(4) Suppose R is a PID. Show a nonzero element $0 \neq a \in R$ is irreducible if and only if $\langle a \rangle$ is maximal.
(5) Suppose R is a PID. Show that every irreducible element is prime. (Recall that every maximal ideal is a prime ideal).
(6) Suppose R is a PID, and suppose that we have irreducible elements $p_1, \dots, p_r, q_1, \dots, q_s \in R$ (with $r < s$) such that $p_1 \dots p_r = q_1 \dots q_s$. Use part (5) to find units $u_1, \dots, u_r$ such that $q_i = u_i p_i$ for each $1 \leq i \leq r$ (possibly relabelling the q_j).
(7) Deduce from the previous parts that every PID is a UFD.

Remark 1. Note that above we have shown that in a PID R, a nonzero element a is prime iff $\langle a \rangle$ is prime iff $\langle a \rangle$ is maximal iff a is irreducible. So we have classified the poset of prime ideals $Spec(R)$: There is (0), contained in every other prime ideal, and the set of nonzero prime ideals is in bijection with the set of irreducible (=prime) elements modulo the action of the unit group R^*, with no inclusion relations between the nonzero prime ideals.

Exercise 2. Let R be a PID. Note the converse to (5) above, that is, note that every prime element is irreducible. Use (4) above to show that if $\mathfrak{p}$ is a nonzero prime ideal, then $R/\mathfrak{p}$ is a field.

Recall that two elements $x, y \in R$ of a ring are said to be *coprime* if there exist $a, b \in R$ such that $ax+by = 1$ (equivalently, $\langle x, y\rangle = R$). Two elements $x, y \in R$ are said to be *relatively prime* if there is does not exist any prime z with $z|x$ and $z|y$ (equivalently, for any prime $\langle z\rangle$, either $x \notin \langle z\rangle$ or $y \notin \langle z\rangle$).

Exercise 3 ([AK2017, Theorem.2.20])**.** Let R be a PID. Let $P = R[X]$ be the polynomial ring in one variable X, and $\mathfrak{p}$ a nonzero prime ideal of P. Assuming that P is a UFD (because it is [AK2017, 2.5]), we will show that there are three classes of prime ideals of $R[X]$:

- The zero ideal (0).
- Principal ideals $\langle F\rangle$ with F a prime element of $R[X]$.
- Ideals of the form $\langle p, G\rangle$ where $p \in R$ is prime, $pR = \mathfrak{p} \cap R$, and $G \in R[X]$ is prime with image $G' \in (R/pR)[X]$ also prime.

and that all nonprincipal prime ideals are maximal.

(1) [AK2017, Exercise 2.18] Show that in a PID, nonzero elements x and y are *relatively prime* if and only if they're coprime.

(2) Let $K = Frac(R)$ be the fraction field of R. Recall that Gauss's Lemma says that "if $F \in R[X]$ is prime in $R[X]$, then it is also prime in $K[X]$". Show that given prime elements $F_1, F_2 \in R[X]$ with $F_2 \notin \langle F_1\rangle$, the elements F_1, F_2 are coprime in $K[X]$.

(3) Given a nonprincipal prime ideal $\mathfrak{p} \subset R[X]$, use the previous two parts to find a nonzero element $c \in \mathfrak{p} \cap R$. Conclude that under the canonical map $\pi : Spec(R[X]) \to Spec(R), \mathfrak{q} \mapsto \mathfrak{q} \cap R$ from the poset of prime ideals of $R[X]$ to the poset of prime ideals of R, our nonprincipal prime $\mathfrak{p}$ is sent to a maximal ideal, say pR of R.

(4) Define $k = R/pR$. Note that the primes of $R[X]$ sent to pR by $\pi : Spec(R[X]) \to Spec(R)$, are precisely those in the image of $\iota : Spec(k[X]) \to Spec(R[X]); \mathfrak{q} \mapsto \phi^{-1}\mathfrak{q}$ where $\phi : R[X] \to k[X]$ is the canonical map. Define $\mathfrak{q} = \mathfrak{p}/pR \subset k[X]$. Show that $\mathfrak{q}$ is a maximal ideal of $k[X]$, that $\mathfrak{p} = \phi^{-1}\mathfrak{q}$, and deduce that $\mathfrak{p}$ is therefore a maximal ideal of $R[X]$.

(5) Using the fact that $k[X]$ is a PID, $\mathfrak{q}$ is prime, and $R[X]$ is a UFD, find a prime $G \in R[X]$, whose image $G' \in k[X]$ is also prime, and such that $\mathfrak{p} = \langle p, G\rangle$.