NOTES FOR SECTION 2.9 OF ASH

SAM EVENS

The purpose of these notes is to help with the discussion of section 2.9 from Ash.

Let R be an unique factorization domain. Let F be the fraction field of R, so $F = \{\frac{a}{b} : a, b \in R, b \neq 0\}$. Let $\{\mathfrak{p}_i : i \in I\}$ be the principal ideals of R that are prime ideals, and for $i \in I$, let $\mathfrak{p}_i = (p_i)$. Let $\mathcal{P} = \{p_i : i \in I\}$. Then $\mathcal{P}$ is a list of irreducible elements of R, except that if $p \in R$ is irreducible, it includes only one element from the set of associates $\{up : u \in R^\times\}$ of p. If $R = \mathbf{Z}$, then it would be standard to take $\mathcal{P}$ to be the set of positive primes, but it is also fine to take $\mathcal{P}$ to be any other set of primes, as long as exactly one of $\pm p$ appears in $\mathcal{P}$.

If F is a field and $R = F[x]$, the nonzero prime ideals are (f), where f is an irreducible polynomial in $F[x]$. Note that for f, g irreducible in $F[x]$, then $(f) = (g)$ if and only if $g = af$, where $a \in F^\times$. Indeed, this follows from Lemma 0.5 of the notes on 2.6, since the units of $F[x]$ are the elements of $F^\times$. It is easy to check that each nonzero principal prime ideal is (f) for a unique monic irreducible polynomial, and the usual convention is to take $\mathcal{P}$ to be the monic irreducible polynomials. However, this is an arbitrary choice, and there is no really good choice for a general unique factorization domain. This choice is a bit unnatural, and it is usually better to avoid making choices like this, but we do so in this case because it allows us to make statements with greater precision. If we did not do this, then many statements would be correct only up to a unit.

Remark 0.1. *Let $a \in R - \{0\}$. Then we can write*

$$a = up_1^{e_1} \cdots p_k^{e_k},$$

with $u \in R^*$, $k \geq 0$, and p_i pairwise distinct elements of $\mathcal{P}$, and $e_i > 0$. Further, this expression is unique up to renumbering of the p_i. Indeed, by property (UF1) of unique factorization domains, since $a \in R - \{0\}$, $a = vq_1^{e_1} \cdots q_k^{e_k}$, with $v \in R^*$, and $q_1, \ldots, q_k$ pairwise nonassociate primes. By definition of $\mathcal{P}$, each $q_i = v_i p_i$ for some $p_i \in \mathcal{P}$ and unit $v_i \in R^*$. Substituting $q_i = v_i p_i$ in $a = vq_1^{e_1} \cdots q_k^{e_k}$ gives $a = v \cdot \prod_{i=1}^k v_i^{e_i} \cdot \prod_{i=1}^k p_i^{e_i}$, which establishes the existence claim above, since R^* is closed under multiplication. Uniqueness follows since if $a = w \cdot \prod_{i=1}^l r_i^{f_i}$ with $w \in R^*$ and $r_i \in \mathcal{P}$, then by property (UF2) of unique factorization domains, then $k = l$, and we can renumber the r_i so p_i is associate to r_i. Since by definition the elements of $\mathcal{P}$ are pairwise nonassociate, then $p_i = r_i$ for $i = 1, \ldots, k$, so since R is an integral domain, $u = w$. This establishes the uniqueness assertion.

Remark 0.2. *Let $\alpha \in F^\times$. Let $p \in \mathcal{P}$. Then we can write*

$$\alpha = p^e \cdot \frac{a}{b}$$

with $e \in \mathbf{Z}$, and $a, b \in R - \{0\}$ such that p does not divide a or b. Indeed, we can certainly write $\alpha = \frac{x}{y}$ for $x, y \in R - \{0\}$, and write

$$x = u \cdot \prod_{i \in I} p_i^{e_i},$$

with $u \in R^\times$, $e_i \geq 0$, and $e_i = 0$ for all but finitely many p_i. Similarly, we can write

$$y = v \cdot \prod_{i \in I} p_i^{f_i},$$

with $v \in R^\times$, $f_i \geq 0$, and $f_i = 0$ for all but finitely many p_i. Thus,

$$\alpha = w \cdot \prod_{i \in I} p_i^{g_i},$$

with $w = u \cdot v^{-1} \in R^\times$, and $g_i = e_i - f_i \in \mathbf{Z}$ and $g_i = 0$ for all but finitely many g_i. We take $a = w \cdot \prod_{i \in I, p_i \neq p, g_i > 0} p_i^{g_i}$ and take $b = \prod_{i \in I, p_i \neq p, g_i < 0} p_i^{-g_i}$. We take $e = g_{i_0}$ where $p = p_{i_0}$.

Definition 0.3. *Let $\alpha \in F^\times$ and let $p \in \mathcal{P}$. By Remark 0.2, we can write $\alpha = p^e \cdot \frac{a}{b}$ with $e \in \mathbf{Z}$, and $a, b \in R$, and p does not divide a or b. we define*

$$\mathrm{ord}_p(a) = e.$$

Fix $p \in \mathcal{P}$, and let $\alpha = p^e \cdot \frac{a}{b}$ as above. If $\alpha = p^{e_1} \cdot \frac{c}{d}$ with $e_1 \in \mathbf{Z}$ and $c, d \in R$ with p not dividing c or d. We show that $e = e_1$. We may assume $e \geq e_1$. Then $p^{e - e_1} ac = bd$. Since p is prime (by 2.6.4 in Ash), and p does not divide b or d, then p does not divide bd. Thus, $e - e_1 = 0$,so $e = e_1$.

Lemma 0.4. *Let $p \in \mathcal{P}$. (1) If $\alpha, \beta \in F^\times$, then $\mathrm{ord}_p(\alpha \cdot \beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.*

(2) If $\alpha, \beta \in F^\times$, then $\mathrm{ord}_p(\frac{\alpha}{\beta}) = \mathrm{ord}_p(\alpha) - \mathrm{ord}_p(\beta)$.

(3) If $\alpha \in F^\times$, then $\alpha \in R$ if and only if $\mathrm{ord}_p(\alpha) \geq 0$ for all $p \in \mathcal{P}$.

Proof. For (1), let $\alpha = p^e \cdot \frac{a}{b}$, and let $\beta = p^f \cdot \frac{c}{d}$ with $e, f \in \mathbf{Z}$ and p not dividing any of a, b, c, d. Then $\alpha \cdot \beta = p^{e+f} \cdot \frac{ac}{bd}$. Since p is prime (Ash, 2.6.4), then p does not divide ac or bd. Thus, $\mathrm{ord}_p(\alpha \cdot \beta) = e + f$, which verifies (1). (2) follows from (1) using $\alpha = \frac{\alpha}{\beta} \cdot \beta$. For (3), if $\alpha \in R$, then $\mathrm{ord}_p(\alpha) \geq 0$ is clear. Now suppose that $\mathrm{ord}_p(\alpha) \geq 0$ for every $p \in \mathcal{P}$. By Remark 0.2, we may write $\alpha = w \cdot \prod_{i \in I} p_i^{g_i}$ with $w \in R^\times$, and $\mathrm{ord}_{p_i}(\alpha) = g_i \geq 0$. Thus, $\alpha \in R$.

Q.E.D.

Definition 0.5. *Let* $f = a_0 + a_1x + \cdots + a_nx^n \in F[x] - \{0\}$. *Let* $\mathrm{ord}_p(f) = \min_{i=0,\ldots,n} \mathrm{ord}_p(a_i)$. *We define the content of* f *to be* $c(f) = \prod p_i^{\mathrm{ord}_{p_i}(f)}$, *where the product is over primes* $p_i \in \mathcal{P}$ *such that* $\mathrm{ord}_{p_i}(f) \neq 0$. *This product is a finite product because there are only finitely many primes* $p \in \mathcal{P}$ *such that* $\mathrm{ord}_p(a_k) \neq 0$, *where* $a_k \neq 0$.

Remark 0.6. *If* $\alpha \in F^\times$, *then* α *may be regard as a constant polynomial* $f_\alpha \in F[x]$, *and we set* $c(\alpha) = c(f_\alpha)$.

Exercise 0.7. *Let* $\alpha \in F^\times$ *and let* $f \in F[x] - \{0\}$.

(1) If $\alpha = \frac{a}{b} \in F^\times$, *then* $c(\alpha) = \prod p_i^{\mathrm{ord}_{p_i}(\alpha)}$, *where the product is over primes* $p_i \in \mathcal{P}$ *such that* p_i *divides* a *or* b.

(2) $c(\alpha \cdot f) = c(\alpha) \cdot c(f)$.

(3) $c(c(\alpha)) = c(\alpha)$.

(4) $c(f) \in R$ *if and only if* $f \in R[x]$.

(5) $c(\alpha) = u \cdot \alpha$, *for some* $u \in R^*$. *In particular, for* $\alpha \in R$, $c(\alpha) = 1$ *if and only if* $\alpha \in R^*$.

(6) If $\beta \in F^\times$, *then* $c(\alpha \cdot \beta) = c(\alpha) \cdot c(\beta)$.

For example, if $R = \mathbf{Z}$, then $c(-1) = 1$. Further, if we take $\mathcal{P}$ to be the positive primes, then $c(-6) = 6$.

Remark 0.8. *Let* $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x] - \{0\}$, *and let* $\mathcal{P}$ *be the positive primes. Then* $c(f) = \gcd(a_0, \ldots, a_n)$.

Definition 0.9. *Let* $f \in F[x] - \{0\}$. *We say that* f *is primitive if* $c(f) = 1$.

Remark 0.10. *Let* $f \in F[x] - \{0\}$. *Then* f *is primitive if and only if* $f \in R[x]$ *and for every prime* $p \in \mathcal{P}$, p *does not divide* f *in* $R[x]$. *Indeed, assume* f *is primitive. Then* $c(f) = 1 \in R$, *so by Exercise 0.7 (4), it follows that* $f \in R[x]$. *If a prime* p *divides* f *in* $R[x]$, *then* $f = p \cdot g$ *for some* $g \in R[x]$, *so* $c(f) = pc(g)$ *by Exercise 0.7 (2). Since* $c(g) \in R$, *it follows that* $c(f) \neq 1$, *so* f *is not primitive. This proves the assertion in one direction. Conversely, suppose that* $f \in R[x]$ *and* f *is not primitive. Then by the definition of* $c(f)$, *it follows that* p *divides* $c(f)$ *for some prime* p *of* $\mathcal{P}$. *Hence,* $\mathrm{ord}_p(a_i) \geq 1$ *for every coefficient* a_i *of* f, *so* p *divides* f. *This completes the proof.*

Remark 0.11. *Let* p *be a prime of* $\mathcal{P}$, *and let* $\overline{R}_p = R/(p)$. *Let* $q : R \to \overline{R}_p$ *be the projection map given by* $a \mapsto a + (p)$. *By the universal property of polynomial rings, there is a unique ring homomorphism* $\pi : R[x] \to \overline{R}_p[x]$ *such that* $\pi(a) = q(a)$ *for* $a \in R$ *and* $\pi(x) = x$. *Then it is easy to check that if* $f = \sum a_ix^i \in R[x]$, *then* $\pi(f) = \sum q(a_i)x^i \in \overline{R}_p[x]$.

CLAIM: $\ker(\pi) = pR[x]$.
Indeed, an element g *of* $pR[x]$ *is a polynomial* $\sum b_ix^i$ *with* p *dividing all* b_i, *and it follows from the above formula for* π *that* $g \in \ker(\pi)$. *Conversely, by the above formula, if*

$g \in \ker(\pi)$, then all coefficients of g are divisible by p, and it follows that $g \in pR[x]$. If we want to specify the prime p, we will use π_p to denote π.

Remark 0.12. *Let $f \in R[x]$, then f is primitive if and only if $f \notin \ker(\pi_p)$ for every prime $p \in \mathcal{P}$. Indeed, if f is not primitive, then by Remark 0.10, it follows that f is a multiple of p for some $p \in \mathcal{P}$. Hence, by Remark 0.11, $\pi_p(f) = 0$. The argument in the converse argument is similar.*

Remark 0.13. *Let $f \in F[x] - \{0\}$. Then $f = c(f) \cdot f_0$, where f_0 is primitive. Indeed, it follows from definitions that $c(f)$ is a nonzero element of F, so we can set $f_0 = \frac{1}{c(f)} f$ in $F[x]$. Then $f = c(f)f_0$, so by Exercise 0.7, parts (2) and (3), $c(f) = c(f)c(f_0)$. Hence, $c(f_0) = 1$, so f_0 is primitive.*

Department of Mathematics, University of Notre Dame, Notre Dame, IN, 46556

Email address: sevens@nd.edu