

Math 60210, Basic Algebra, Problem Set 11, Fall 2009
due Tues, November 24, or Tues, December 1

Do 7 of these problems

Comment: there will be no homework due the Tuesday after Thanksgiving

Definition: Let D be a unique factorization domain with fraction field F . If p and q are prime elements of D , we say that $p \simeq q$ if p and q are associates, or equivalently if $(p) = (q)$. This defines an equivalence relation on primes of D . Let I index the set of equivalence classes of primes, and for each $i \in I$, choose a representative p_i of the corresponding equivalence class. If $x \in F^*$, then we may write $x = u \cdot \prod_{i \in I} p_i^{f_i}$, for some $u \in D^*$. We define $ord_{p_i}(x) = f_i$. It is elementary to check that if we chose a different representative q_i equivalent to p_i , then $ord_{q_i}(x) = ord_{p_i}(x)$.

Definition: Retain the above notation, and let $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. For one of the primes $p_i, i \in I$ chosen above, let $ord_{p_i}(f) = \min_{j=0}^n ord_{p_i}(a_j)$. Define $c(f) = \prod_{i \in I} p_i^{ord_{p_i}(f)}$.

1. Let D be a unique factorization domain with fraction field F . Then for $p = p_i$, where $i \in I$,

(i) Let $\alpha, \beta \in F^*$. Prove that

$$ord_p(\alpha \cdot \beta) = ord_p(\alpha) + ord_p(\beta)$$

and

$$ord_p\left(\frac{\alpha}{\beta}\right) = ord_p(\alpha) - ord_p(\beta).$$

(ii) If $x \in F^*$, prove that $x \in D$ if and only if $ord_{p_i}(x) \geq 0$ for all $i \in I$. Prove that $x \in D^*$ if and only if $ord_{p_i}(x) = 0$ for all $i \in I$.

2. Let F be the fraction field of D , as above and let $b \in F^*$. For nonzero $f \in F[x]$,

(i) Prove that $c(bf) = u \cdot b \cdot c(f)$ for some unit $u \in D^*$.

(ii) Let $f \in F[x]$. Prove that $f \in D[x]$ if and only if $c(f) \in D$.

(iii) Let $f_1 = \frac{f}{c(f)}$. Prove that $f_1 \in D[x]$, and f_1 is primitive.

3. Let R be a principal ideal domain. Let p in R be prime, and let $R_{(p)} = S^{-1}R$, where $S = R - (p)$. We showed in class that $R_{(p)}$ is a subring of the fraction field of F . Prove that $R = \bigcap R_{(p)}$, where the intersection is over all primes p of R , and takes place in the fraction field F of R (hint: the general case is not very different from the case where $R = \mathbf{Z}$).

4. Definition : Let K be a field. A discrete valuation on K is a function $v : K \rightarrow \mathbf{R}^{\geq 0}$ satisfying

(1) $v(x) \geq 0$ for all $x \in K$ and $v(x) = 0 \iff x = 0$.

(2) For all $x, y \in K$, $v(xy) = v(x)v(y)$.

(3) For all $x, y \in K$, $v(x + y) \leq \max\{v(x), v(y)\}$.

(4) $v(K^*) = \{c^n : n \in \mathbf{Z}\}$ for some nonzero real c with $c < 1$.

Let $R_v := \{a \in K | v(a) \leq 1\}$. Prove that R_v is a ring, and $I := \{a \in K | v(a) < 1\}$ is an ideal. Choose $\pi \in I$ such that $v(\pi)$ is maximal. Prove that every ideal of R_v is (π^k) for some $k > 0$. In particular, prove that R is a Principal Ideal Domain.

5. Let $R = \mathbf{Z}$ and let p be prime. For $x \in \mathbf{Q}^*$, write $x = p^i \cdot \frac{a}{b}$ with $a, b \in \mathbf{Z}$, $a, b \neq 0$ and p relatively prime to a and b . Define $v : \mathbf{Q}^* \rightarrow \mathbf{R}$ by $v(x) = p^{-i}$ and define $v(0) = 0$. Prove that v is a discrete valuation and compute R_v .

6. Note that by Example 2.7.5 of Ash, $R = \mathbf{Z}[z]$ is a Euclidean domain. In this exercise and the next, we will compute the nonzero primes of R and relate them to the problem of determining

whether a prime number in \mathbf{Z} is a sum of two squares. We call a prime of R a Gaussian prime, and a prime of \mathbf{Z} an integral prime.

(a) Let $\pi = a + bi \in R$ be a prime of R . Define $N(\pi) = \pi \cdot \bar{\pi}$, and prove that $N(\pi)$ is either p or p^2 , where p is a prime of \mathbf{Z} . Moreover, if π is not in \mathbf{Z} , then $N(\pi) = p$ is a prime of \mathbf{Z} .

(b) Let $p = 4k + 3$ be a prime of \mathbf{Z} . Then $p \neq a^2 + b^2$ for any $a, b \in \mathbf{Z}$, and p is prime in $\mathbf{Z}[i]$ (hint: compute each side modulo 4).

(c) Factor 2 as a product of Gaussian primes. Write 2 as a sum of two squares.

7. Continuing notation of problem 7:

(a) Let $p = 4k + 1$ be a prime integer. Show that there is $a \in \mathbf{Z}_p^*$ such that the order of a is 4 (hint: let $G = \mathbf{Z}_p^*/N$, where $N = \{\pm 1\}$. Show there is $\alpha \in G$ of order 2, and choose $a \in \mathbf{Z}_p^*$ such that $\alpha = aN$. Prove that a has order 4 in \mathbf{Z}_p^*).

(b) Using notation of (a), Prove that p divides $a^2 + 1$. Prove that p is not a Gaussian prime (hint: use definition of prime, and $a^2 + 1 = (a + i)(a - i)$).

(c) Prove that if $\pi = a + bi$ is a Gaussian prime factor of $p = 4k + 1$, then $p = N(\pi) = a^2 + b^2$.

(d) Prove that up to multiplication by units, the Gaussian primes are :

(1) p , where $p = 4k + 3$ is an integral prime.

(2) $1 + i$

(3) $\pi = a \pm bi$, where $a^2 + b^2 = p$ is congruent to 1, modulo 4, and p is an integral prime.

8. Let R be an integral domain with multiplicative subset S . Let $f : R \rightarrow S^{-1}R$ be the ring homomorphism $f(a) = \frac{a}{1}$.

(i) For an ideal I of R , let $S^{-1}I = \{\frac{a}{s} : a \in I, s \in S\}$. Prove that $S^{-1}I$ is an ideal of $S^{-1}R$.

(ii) For a ring A , let $\text{Spec}(A)$ denote the set of prime ideals of A . Define $f^* : \text{Spec}(S^{-1}R) \rightarrow \text{Spec}(R)$ by $f^*(P) = f^{-1}(P)$. Prove that if P is a prime of $S^{-1}R$, then $S^{-1}f^*(P) = P$, f^* is injective, and the image $\text{Im}(f^*) = \{P \in \text{Spec}(R) : P \cap S = \emptyset\}$.

(iii) If $S = R - P$, where P is a prime ideal of R , prove that $S^{-1}P$ is the unique maximal ideal of $S^{-1}R$.

9. Let $R = F[x, y]/(xy)$ where F is a field. Let $S = \{x^n : n \geq 0\}$. Prove that $S^{-1}R \cong F[x]$.

10. Let $R = \mathbf{Z}$, and let p be prime in \mathbf{Z} . Let $S = \{p^n : n \geq 0\}$. Prove that

$$S^{-1}\mathbf{Z} \cong \left\{ \frac{a}{p^k} \in \mathbf{Q} : k \geq 0 \right\}.$$

11. Let F be a field and let $R = F[x]$. Let $S = R - P$, where $P = (x)$. Construct an injective ring homomorphism $S^{-1}F[x] \rightarrow F[[x]]$. (Extra Credit: is your ring homomorphism surjective).

12. Let F be a field, and consider the integral domain $R = F[[x]]$. Show that the fraction field $\text{Frac}(R)$ of R coincides with the set $\{\frac{a}{x^n} : a \in F[[x]]\}$.

13. Let F be a field and let $R = F[x]$. Let $S = \{x^n : n \geq 0\}$. Prove that $S^{-1}R \cong F[x, y]/(xy - 1)$.