Homework 1

Aleck Zhao

February 11, 2017

1. Let R be a commutative ring. Show that

$$p \in R \text{ is prime} \iff \langle p \rangle \text{ is a nonzero prime ideal.}$$

Proof. $\implies$: Suppose $ab \in \langle p \rangle$ for $a, b \in R$. This means $p \mid ab$, and since p is prime, either $p \mid a$ or $p \mid b$. It then follows that either $a \in \langle p \rangle$ or $b \in \langle p \rangle$, which shows that $\langle p \rangle$ is a prime ideal.

$\impliedby$: Suppose $p \mid ab$, which means that $ab \in \langle p \rangle$. Since $\langle p \rangle$ is a prime ideal, either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. This means that $p \mid a$ or $p \mid b$, so p is a prime element, as desired. □

2. Let R be a UFD. Fill in the gap in the proof of §5.1 Theorem 10 by showing that if $p \in R[x]$ is irreducible of degree 0, then p is prime in $R[x]$.

Proof. If p is irreducible of degree 0, it is just an element in R, and since R is a UFD, we also know that p is prime in R. If $p \mid fg$, where $f, g \in R[x]$, then let $fg = kp$ for $k \in R[x]$. Let

$$\begin{aligned} f &\sim c(f)f_1 \\ g &\sim c(g)g_1 \\ k &\sim c(k)k_1 \end{aligned}$$

where $f_1, g_1, k_1 \in R[x]$ are primitive. Then

$$c(f)f_1c(g)g_1 \sim c(k)k_1p$$

and taking the content of both sides, we have

$$c(f)c(g) \sim c(k)p$$

so $p \mid c(f)c(g)$. Since $c(f), c(g) \in R$ and p is prime in R, it follows that either $p \mid c(f)$ or $p \mid c(g)$, so $p \mid f$ or $p \mid g$, and thus p is prime in $R[x]$, as desired. □

3. Let R be an integral domain, and let $\delta : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ be a function satisfying condition DA. For nonzero $a \in R$, define

$$\tilde{\delta}(a) := \min_{x \in R \setminus \{0\}} \delta(xa).$$

Show that $\tilde{\delta}$ satisfies conditions DA and E in the text.

Proof. E: Since δ takes values in $\mathbb{Z}_{\geq 0}$, we have

$$\tilde{\delta}(ab) = \min_{x \in R \setminus \{0\}} (xab) = \delta(x_0ab)$$

for some $x_0 \in R$. Then we have

$$\tilde{\delta}(a) = \min_{x \in R \setminus \{0\}} \delta(xa) \leq \delta[(x_0b)a]$$

so

$$\tilde{\delta}(ab) = \delta(x_0 ab) \geq \tilde{\delta}(a)$$

as desired.

DA: For any choice of $a, b \in R$ with $b \neq 0$, we must show that we can write $a = qb + r$ such that $\tilde{\delta}(b) > \tilde{\delta}(r)$, or $r = 0$. We know that for the same choice of a, b, we can also write $a = qb + r$ with $r = 0$ or $\delta(b) > \delta(r)$. The case with $r = 0$ is trivial, so it suffices to prove that $\tilde{\delta}(b) > \tilde{\delta}(r)$.

Since $\tilde{\delta}$ satisfies E from above, we have

$$\delta(1 \cdot r) \geq \tilde{\delta}(r) = \min_{x \in R \setminus \{0\}} \delta(xr) = \delta(x_0 r) \geq \delta(r)$$

So $\tilde{\delta}(k) = \delta(k)$ for all $k \in R$. Thus, since $\delta(b) > \delta(r)$, it holds that

$$\tilde{\delta}(b) = \delta(b) > \delta(r) = \tilde{\delta}(r)$$

as desired. □

Section 5.1: Irreducibles and Unique Factorization

35. Let R be a UFD and let $g \mid f$ in $R[x]$, where $f \neq 0$. If f is primitive, show that g is also primitive.

Proof. Let $f = gh$ for $h \in R[x]$. Taking the content of both sides, by Gauss' Lemma, we have

$$c(f) \sim c(gh) \sim c(g)c(h)$$

Since f is primitive, we have

$$1 \sim c(g)c(h) \implies c(g) \in R^\times$$

so $c(g) \sim 1$, which means that g must also be primitive. □

38. Let R be a UFD with field of quotients F. If $p \in R[x]$ is primitive, and p is irreducible in $F[x]$, show that p is irreducible in $R[x]$.

Proof. This is trivial because $R[x] \subset F[x]$, so if p does not have a non-trivial factorization in $F[x]$, it can't possibly have one in $R[x]$ either. □

Section 5.2: Principal Ideal Domains

5. If R is a PID and $A \neq 0$ is an ideal of R, show that R/A has a finite number of ideals, all of which are principal.

Proof. Since R is a PID, $A = \langle d \rangle$ for some $d \in R$. If d is a unit, then $A = R$, so R/A is trivial. Otherwise, let $B \subset R$ be an ideal of R, so $B/A \subset R/A$ is an ideal of R/A. Let $B = \langle b \rangle$, so the quotient ring $B/A = \langle b \rangle / \langle d \rangle$ is only nontrivial if $b \mid d$. Since R is a PID, it is also a UFD, so d has a unique factorization with finitely many irreducible factors, and b is some finite product of them, so the possibilities for b are also finite. It is also clear that all ideals of R/A are principal, where $B/A = \langle b + A \rangle$ for b as above. □

10. Let R be a ring such that $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. Show that R is a PID.

31. Show that every unit of $\mathbb{Z}[\sqrt{2}]$ has the form $\pm u^k$, where $k \in \mathbb{Z}$ and $u = 1 + \sqrt{2}$.

Proof. We have

$$N\left[\pm(1+\sqrt{2})^k\right] = N\left[\pm(1+\sqrt{2})\right]^k = (1^2 - 2\cdot 1^2)^k = \pm 1$$

so $\pm u^k$ is a unit for all $k \in \mathbb{Z}$. On the other hand, if $v \in \mathbb{Z}[\sqrt{2}]$ is a unit not equal to $\pm u^k$ for some $k \in \mathbb{Z}$, WLOG it is positive, and it must lie between two units

$$u^i < v < u^{i+1}$$

for some $i \in \mathbb{Z}$. It follows that $1 < vu^{-i} = w < u$ where w is also a unit, so it suffices to consider w. If w is a unit, then $|w|\,|w^*| = 1$. Since $w > 1$, it follows that $|w^*| < 1$. If $w = a + b\sqrt{2}$, then $w^* = a - b\sqrt{2}$, so we have the two inequalities

$$\begin{aligned} -1 <& a - b\sqrt{2} < 1 \\ 1 <& a + b\sqrt{2} < 1 + \sqrt{2} \end{aligned}$$

and adding them gives

$$0 < 2a < 2 + \sqrt{2}$$

The only possibility is $a = 1$, so then

$$\begin{aligned} 1 < 1 +& b\sqrt{2} < 1 + \sqrt{2} \\ 0 <& b\sqrt{2} < \sqrt{2} \end{aligned}$$

which is impossible for $b \in \mathbb{Z}$. Thus, it is impossible for v to lie between u^i and u^{i+1} for any i, so it must be that $v = \pm u^k$ are the only units. $\square$