Homework 1

Aleck Zhao

February 5, 2017

Section 5.1: Irreducibles and Unique Factorization

2. If $a \sim a'$ and $b \sim b'$ in R, show that $a \mid b$ if and only if $a' \mid b'$.

Proof. We have $a = ua'$ and $b = vb'$ where $u, v \in R^\times$. For the forward direction, if $a \mid b$, then $b = ac$ for some $c \in R$. Then

$$\begin{aligned} b = vb' &= ac = ua'c \\ \implies b' &= v^{-1}uca' \end{aligned}$$

where v^{-1} exists since it is a unit. Thus, $a' \mid b'$ as desired.

For the reverse direction, we have $a' = u^{-1}a$ and $b' = v^{-1}b$ and the result follows similarly. □

8. Find the units in $\mathbb{Z}[\sqrt{-3}]$.

Solution. Suppose the element $a + b\sqrt{-3}$ is a unit, that is, it has a multiplicative inverse

$$\frac{1}{a+b\sqrt{-3}} = \frac{a-b\sqrt{-3}}{a^2+3b^2} = \frac{a}{a^2+3b^2} - \frac{b}{a^2+3b^2}\sqrt{-3}$$

in $\mathbb{Z}[\sqrt{-3}]$. Thus, $a^2 + 3b^2$ must divide a and b. If $|a| > 1$ then $a < a^2 + 3b^2$ so it is impossible for $a^2 + 3b^2$ to divide a. If $a = \pm 1$, then we must have $b = 0$. On the other hand, if $|b| > 0$ then it always holds that $b < a^2 + 3b^2$ so $a^2 + 3b^2 \nmid b$. Thus, the only units are $\boxed{1, -1}$. □

11. Let $p \in \mathbb{Z}$ be a prime and assume that $p \equiv 3 \pmod 4$. Show that p is irreducible in $\mathbb{Z}[i]$.

Proof. Suppose p admits a factorization

$$p = (a + bi)(c + di) = (ac - bd) + (ad + bc)i, \qquad a, b, c, d \in \mathbb{Z}$$

If $ad + bc = 0$, then the two factors are complex conjugates up to multiple, so

$$p = n(a + bi)(a - bi) = n(a^2 + b^2)$$

Since p is prime, we must have either $n = 1$ or $n = p$. If $n = 1$, then

$$a^2 + b^2 = p \equiv 3 \pmod 4$$

but since squares are 0 or 1 modulo 4, this is impossible.

If $n = p$, then $a^2 + b^2 = 1$ so either $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. In either case, one of the two factors must be a unit. Thus, p is irreducible in $\mathbb{Z}[i]$, as desired. □

13. In each case show that p is irreducible in $\mathbb{Z}[\sqrt{-5}]$ but is not a prime.

(a) $p = 2 + \sqrt{-5}$

Proof. We have $\left|2 + \sqrt{-5}\right| = 2^2 + 5 = 9$. Suppose $2 + \sqrt{-5} = ab$ is a factorization. Since the norm is multiplicative, we must have either $|a| = |b| = 3$ or $|a| = 1, |b| = 9$ or $|a| = 9, |b| = 1$. Let $a = r + s\sqrt{-5}, b = t + u\sqrt{-5}$. In the first case, we have

$$\left|r + s\sqrt{-5}\right| = r^2 + 5s^2 = 3$$

which is impossible for $r, s \in \mathbb{Z}$. The second and third cases are identical, so WLOG

$$\left|r + s\sqrt{-5}\right| = r^2 + 5s^2 = 1$$

This is only possible if $r = \pm 1$, in which case $a = \pm 1$, which is a unit, so p does not have any nontrivial factorization, so it is irreducible.
On the other hand, we have $p \mid 9$ since

$$\left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right) = 9$$

Since $9 = 3 \cdot 3$, if p is prime it must divide 3. Suppose

$$\begin{aligned} 3 &= \left(2 + \sqrt{-5}\right)\left(a + b\sqrt{-5}\right) \\ &= (2a - 5b) + (a + 2b)\sqrt{-5} \\ \implies a + 2b = 0 \implies a &= -2b \implies 2(-2b) - 5b = -9b = 3 \end{aligned}$$

This has no solution, so p does not divide 3, so it is not prime, as desired. $\square$

(b) $p = 1 + 2\sqrt{-5}$

Proof. We have $\left|1 + 2\sqrt{-5}\right| = 1^2 + 2^2 \cdot 5 = 21$. Suppose $1 + 2\sqrt{-5} = ab$ is a factorization. By a similar argument to part (a), WLOG $|a| \leq |b|$, we must have either $|a| = 1, |b| = 21$ or $|a| = 3, |b| = 7$. In the latter case, we have

$$|a| = \left|r + s\sqrt{-5}\right| = r^2 + 5s^2 = 3$$

which is impossible for $r, s \in \mathbb{Z}$. Then if $|a| = 1$, we must have $a = \pm 1$, so p does not have any nontrivial factorization, so it is irreducible.
To show that p is not prime, use a similar argument to part (a). Since

$$\left(1 + 2\sqrt{-5}\right)\left(2 - \sqrt{-5}\right) = 21 = 3 \cdot 7$$

suppose that p divides 3, so that

$$\begin{aligned} 3 &= \left(1 + 2\sqrt{-5}\right)\left(a + b\sqrt{-5}\right) \\ &= (a - 10b) + (2a + b)\sqrt{-5} \\ \implies 2a + b = 0 \implies b &= -2a \implies a - 10(-2a) = 21a = 3 \end{aligned}$$

This has no solution, so p does not divide 3, so it is not prime, as desired. $\square$

16. Let $p \sim q$ in the integral domain R.

    (a) Show that p is irreducible if and only if q is irreducible.

    Proof. We have $p = uq$ for $u \in R^\times$. Suppose q is not irreducible, that is, it has a nontrivial factorization $q = rs$ with $r, s \in R$ not units. Then $p = uq = (ur)s$ is a nontrivial factorization of p since s and ur are both not units, so p is not irreducible either.

    Suppose p is not irreducible, that is, it has a nontrivial factorization $p = tv$ with $t, v \in R$ not units. Then $p = tv = uq \implies q = (u^{-1}t)v$ which is a nontrivial factorization of q, so q is not irreducible either. □

    (b) Show that p is a prime if and only if q is a prime.

    Proof. Suppose p is a prime, and $p = uq$ for $u \in R^\times$. Now suppose $q = ab$ is a factorization. Substituting, we have $p = uab = (ua)b$. Since p is prime, it either divides ua or b. Suppose $p \mid b$, so that $b = cp$. Then $p = (ua)(cp) \implies 1 = uac$, which means that a is a unit, so since $q = ab$ it follows that $q \mid b$.

    If $p \mid ua$, then it must be that $p \mid a$ since u is a unit. Then let $a = dp$, so $p = (udp)b \implies 1 = udb$, so b is a unit. Since $q = ab$ it follows that $q \mid a$. Thus, q is a prime. By a similar argument, since $q = u^{-1}b = vb$, it follows that if q is a prime, then p is a prime as well. □

19. A commutative ring is said to satisfy the descending chain condition on principal ideals (DCCP) if $\langle a_1 \rangle \supseteq \langle a_2 \rangle \supseteq \cdots$ in R implies that $a_n \sim a_{n+1} \sim \cdots$ for some $n \geq 1$. Show that an integral domain R satisfies the DCCP if and only if R is a field.

    Proof. If R is a field, then every nonzero element divides every other nonzero element, so $a_i \sim a_j$ for all i, j, in fact all ideals are exactly R or $\{0\}$, so it satisfies DCCP trivially.

    If R is not a field, then there exists a nonunit $r \in R \setminus R^\times$. Then consider the descending chain

    $$\langle r \rangle \supset \left\langle r^2 \right\rangle \supset \left\langle r^3 \right\rangle \supset \cdots$$

    This is a strictly descending chain of principal ideals, since $r^{k+1} \neq ur^k$ for any $u \in R^\times$. Thus, R does not satisfy DCCP. □

31. Show that $\operatorname{lcm}(a_1, \cdots, a_n)$ exists in an integral domain R if and only if the intersection $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle$ is a principal ideal.

    Proof. Consider an element p in the intersection

    $$p \in \langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle \implies a_i \mid p, \forall i$$

    Suppose $m \sim \operatorname{lcm}(a_1, \cdots, a_n)$ exists in R. Then it follows that $a_i \mid m$ for all i, and $m \mid p \implies p \in \langle m \rangle$, so any elements in the intersection belong the principal ideal generated by m, so the intersection is a principal ideal.

    On the other hand, if

    $$\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle q \rangle$$

    is a principal ideal, then it follows that $a_i \mid q$ for all i. Now, any element $r \in \langle q \rangle$ satisfies $q \mid r$, so it follows that $q \sim \operatorname{lcm}(a_1, \cdots, a_n)$ exists. □

33. Prove Lemma 5. Let R be a UFD and let $f \neq 0$ be a polynomial in $R[x]$.

(a) f can be written as $f = c(f)f_1$ where $f_1 \in R[x]$ is primitive.

Proof. We can write

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

Since R is a UFD, let

$$\begin{aligned} a_0 &= u_0 p_1^{a_{01}} \cdots p_r^{a_{0r}} \\ a_1 &= u_1 p_1^{a_{11}} \cdots p_r^{a_{1r}} \\ &\vdots \\ a_n &= u_n p_1^{a_{n1}} \cdots p_r^{a_{nr}} \end{aligned}$$

where p_i are all the primes that appear in the factorizations of the coefficients, and $a_{jk} \geq 0, \forall j, k$ and $u_i \in R^{\times}$. Then letting

$$d_i := \min\{a_{0i}, a_{1i}, \cdots, a_{ni}\}, 1 \leq i \leq r$$

we have

$$c(f) \sim p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$$

Now, define

$$\begin{aligned} b_0 &:= p_1^{a_{01}-d_1} p_2^{a_{02}-d_2} \cdots p_r^{a_{0r}-d_r} \\ b_1 &:= p_1^{a_{11}-d_1} p_2^{a_{12}-d_2} \cdots p_r^{a_{1r}-d_n} \\ &\vdots \\ b_n &:= p_1^{a_{n1}-d_1} p_2^{a_{n2}-d_2} \cdots p_r^{a_{nr}-d_r} \end{aligned}$$

and let

$$f_1 := b_0 + b_1 x + \cdots + b_n x^n$$

Clearly, taking $c(f) \cdot b_i$ recovers a_i for all i, so $f = c(f)f_1$. It remains to show that f_1 is primitive. Let

$$e_j := \min\{a_{0j} - d_j, a_{1j} - d_j, \cdots, a_{nj} - d_j\}$$

so that

$$c(f_1) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

Now, since $d_j = a_{kj}$ for some k, it follows that $e_j = 0$ for all j. Thus, $c(f_1) \sim 1$, as desired. □

(b) If $0 \neq a \in R$, then $c(af) \sim ac(f)$.

Proof. Let

$$\begin{aligned} f &= a_0 + a_1 x + \cdots + a_n x^n \\ a &= u p_1^{a_1} \cdots p_r^{a_r} \\ a_0 &= u_0 p_1^{a_{01}} \cdots p_r^{a_{0r}} \\ &\vdots \\ a_n &= u_n p_1^{a_{n1}} \cdots p_r^{a_{nr}} \end{aligned}$$

where p_j are all the primes that appear in the factorizations of a and the coefficients, and the exponents are all nonnegative. Then

$$af = aa_0 + aa_1 x + \cdots + aa_n x^n$$

where

$$aa_i = uu_i p_1^{a_1+a_{i1}} \cdots p_r^{a_r+a_{ir}}$$

Now, let

$$\begin{aligned} d_i &:= \min\{a_{0i}, a_{1i}, \cdots, a_{ni}\} \\ e_i &:= \min\{a_i + a_{0i}, a_i + a_{1i}, \cdots, a_i + a_{ni}\} = a_i + d_i \end{aligned}$$

for all $1 \le i \le r$. Then we have

$$\begin{aligned} c(af) &\sim p_1^{e_1} \cdots p_r^{e_r} \\ &= p_1^{a_1+d_1} \cdots p_r^{a_r+d_r} \\ &= (p_1^{a_1} \cdots p_r^{a_r})(p_1^{d_1} \cdots p_r^{d_r}) \\ &\sim ac(f) \end{aligned}$$

as desired. □

34. Let R be a subring of an integral domain S such that (1) $R^\times = S^\times$, and (2) if $s \in S$ and $s \mid r, r \in R$, then $s \in R$.

(a) Show that $p \in R$ is irreducible in R if and only if it is irreducible in S.

Proof. If p is irreducible in S, then it only has trivial factorizations $p = uq$ for $u \in S^\times$. Since $R^\times = S^\times$, and $q = u^{-1}p$, it follows from (2) that $q \in R$, so p has this same trivial factorization in R, and none others (since elements of R are all elements of S).

For the reverse direction, we prove the contrapositive. Suppose $p = ab$ is a nontrivial factorization in S. By (2), since $p \in R$ and $a \mid p$ and $b \mid p$, it follows that $a, b \in R$, so p has a nontrivial factorization in R. □

(b) If S is a UFD, show that R is a UFD.

Proof. From part (a), we showed that the irreducibles in R are exactly the irreducibles in S. Since S is a UFD, for $a \in S$, we can write

$$a = p_1 p_2 \cdots p_r$$

where $p_1, \cdots, p_r$ are irreducibles in S, and thus irreducibles in R. Now, if

$$p_1 p_2 \cdots p_r = q_1 q_1 \cdots q_s$$

where $p_i, q_j \in S$ are irreducibles, since S is a UFD, it follows that all of these are prime, so we must have $p_i \sim q_i$ after rearranging. Thus, since these are irreducible in S it follows that they are irreducibles in R, so R is a UFD, as desired. □

(c) Prove that if $R[x]$ is a UFD, then R is a UFD.

Proof. $R[x] = S$ satisfies (1) because the units in $R[x]$ are exactly the elements in R that are units as well. Now, if $f \in R[x]$ satisfies $f \mid r$ for $r \in R$, then $r = fg$ for $g \in R[x]$, but $\deg r = 0 = \deg f + \deg g$, so it must be that $\deg f = 0 \implies f \in R$ as well, so $R[x]$, satisfies (2). From part (b), it follows that R is a UFD. □