Math 403, Homework 6 solutions

1. Let R be an integral domain. A nonzero element $p \in R$ is called prime if (p) is a prime ideal.

(a). A prime element is irreducible.

Proof. Let $p \in R$ be prime, and suppose we can write $p = ab$ for some $a, b \in R$. Then $ab \in (p)$, and thus either $a \in (p)$ or $b \in (p)$ (since (p) is a prime ideal). Suppose $b \in (p)$. Then we can write $b = up$ for some $u \in R$. Thus, $p = ab = aup$, and hence $p(1 - au) = 0$. Since R is an integral domain, either $p = 0$ (in which case p is irreducible and we are done) or $1 - au = 0$, in which case a is a unit. Thus, every decomposition $p = ab$ has one of a or b a unit. So p is irreducible. ■

(b). In a PID, a nonzero element is prime if and only if it is irreducible.

Proof. Part (a) shows that all primes are irreducibles, so we must show that every irreducible is prime. Since every PID is a UFD, see problem 8. ■

(c). Consider $\mathbb{Z}[\sqrt{-5}]$ with norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Then $\alpha = 2 + \sqrt{-5}$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but not prime. Thus, $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Proof. To see that α is not prime, consider 9. We have $9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 3^2$, so $\alpha | 9$ but $\alpha \nmid 3$ (because they have the same norm, but are not unit multiples). So α is not prime.

On the other hand, if we can write $\alpha = \beta\gamma$ for some non-units $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$, then $9 = N(\alpha) = N(\beta)N(\gamma)$ with $N(\beta), N(\gamma) \neq 1$. Thus, $N(\beta) = N(\gamma) = 3$. But there are no elements in $\mathbb{Z}[\sqrt{-5}]$ with norm 3. So α is irreducible.

Since we have found an irreducible element that is not prime, $\mathbb{Z}[\sqrt{-5}]$ cannot be a PID, by part (b). ■

2. Consider $\mathbb{Z}[\sqrt{-2}]$ as a subring of $\mathbb{C}$ and with the norm map $N(a + b\sqrt{-2}) = a^2 + 2b^2$.

(a). The ring $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain, hence a PID.

Proof. Take any $a, b \in \mathbb{Z}[\sqrt{-2}]$ with $a \neq 0$. We must produce $q, r \in \mathbb{Z}[\sqrt{-2}]$ with $N(r) < N(a)$ such that $b = qa + r$. Let q be the point in $\mathbb{Z}[\sqrt{-2}]$ closest (in Euclidean distance) to b/a. Let $r = b - qa$. Then it is immediate that $b = qa + r$, so now we must show that this r satisfies $N(r) < N(a)$.

Recall that the norm on $\mathbb{Z}[\sqrt{-2}]$ is just the square of the modulus function $|\cdot|$ on the complex numbers, and recall also that $|\alpha\beta| = |\alpha||\beta|$ for $\alpha, \beta \in \mathbb{C}$. Then we have

$$|r| = |b - qa| = \left|\frac{b}{a} - q\right| |a|.$$

Recall that we picked q so that it is the element of $\mathbb{Z}[\sqrt{-2}]$ closest to b/a. Thus, we must have

$$|(b/a) - q|^2 \leq |\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-2}|^2 = \tfrac{3}{4} < 1.$$

Combining this with the displayed equation above, we get

$$|r|^2 = |(b/a) - q|^2|a|^2 \leq \tfrac{3}{4}|a|^2 < |a|^2.$$

So $N(r) < N(a)$, and we are done.

■

(b). Find a generator for the ideal $(85, -11 + 4\sqrt{-2})$.

We need to find $gcd(85, -11 + 4\sqrt{-2})$, so just run the Euclidean algorithm:

$$85 = (-6 - 2\sqrt{-2})(-11 + 4\sqrt{-2}) + (3 + 2\sqrt{-2})$$
$$-11 + 4\sqrt{-2} = (-1 + 2\sqrt{-2})(3 + 2\sqrt{-2}).$$

Thus, $gcd(85, -11 + 4\sqrt{-2}) = 3 + 2\sqrt{-2}$, and so

$$(85, -11 + 4\sqrt{-2}) = (3 + 2\sqrt{-2}).$$

(c). The only units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1.

Proof. Since there are no elements of $\mathbb{Z}[\sqrt{-2}]$ with norm strictly between 0 and 1, we know the only units of $\mathbb{Z}[\sqrt{-2}]$ must have unit norm. (We're again using the fact that $|ab| = |a||b|$ for $a, b \in \mathbb{C}$.) But ± 1 are the only such elements.

■

3. Artin, p. 442, sec. 2, #2a. The ring $\mathbb{Z}[\zeta]$, for $\zeta = e^{2\pi i/3}$, is a Euclidean domain.

Proof. Our norm function N will be the usual complex modulus $|\cdot|$ squared. We need only show that N is integer valued on $\mathbb{Z}[\zeta]$ and that the division algoritm works.

To see that N is integer valued, note that $\zeta^2 = -1 - \zeta$ and $\zeta^3 = 1$. So every element of $\mathbb{Z}[\zeta]$ is of the form $a + b\zeta$ for some $a, b \in \mathbb{Z}$. Also, $\zeta = -1/2 + \sqrt{3}/2$, so

$$|a + b\zeta|^2 = |(a - b/2) + (b/sqrt3i)/2| = a^2 - ab + b^2.$$

Since $a, b \in \mathbb{Z}$, N is integer valued.

Next, suppose $a, b \in \mathbb{Z}[\zeta]$ and $a \neq 0$. Let q be the element of $\mathbb{Z}[\zeta]$ closest to b/a (defined using regular complex division). Note that $|(b/a) - q| \leq 1/\sqrt{3}$. (This is because the points in $\mathbb{Z}[\zeta]$ form a lattice of equilateral triangles with side length 1. The center of the each triangle is the point furthest from all corners, and the center is $1/\sqrt{3}$ units from each corner.) Let $r = b - qa$. Then

$$N(r) = |a|^2 |b/a - q|^2 \leq \tfrac{1}{3} N(a) < N(a).$$

So we can divide (with remainder) with this norm, so $\mathbb{Z}[\zeta]$ is a Euclidean domain.

■

6. Artin, p. 442, sec. 2, #8. Find the greatest common divisor of $11 + 7i$ and $18 - i$ in $\mathbb{Z}[i]$.

Just run the Euclidean algorithm. We have $(18 - i)/(11 + 7i) \approx 1.12 - 0.805i$, so take our first quotient to be $1 - i$, giving

$$18 - i = (1 - i)(11 + 7i) + 3i.$$

Now $(11+7i)/(3i) \approx 2.33 - 3.66i$, so taking $2 - 4i$ for our next quotient,

$$11 + 7i = (1 - 4i)(-1 + 3i) + -1 + i.$$

For the next step,

$$3i = (1 - i)(-1 + i) + i.$$

Since we got a unit as a remainder, the GCD is 1.

8. In a UFD R, a nonzero element is prime if and only if it is irreducible.

Proof. Problem 1(a) shows that any prime is irreducible. We must show that any irreducible is prime. So suppose that $x \in R$ is irreducible, and suppose $ab \in (x)$ for some $a, b \in R$. Then we can write $ab = yx$ for some $y \in R$. Now consider the factorization of each side of $ab = yx$ into irreducibles. Since x is irreducible, it appears in the factorization of yx. But this factorization is the unique factorization of $yx = ab$, so x appears in the factorization of ab. But the factorization of ab is the product of the factorization of a and that of b, so x must appear in one of these factorizations, say in that of a. But then $x|a$, so $a \in (x)$ and (x) is a prime ideal. So x is prime.

■

10.(a). Show that $\sqrt{-2}$, $1+\sqrt{-2}$, $1-\sqrt{-2}$, 5 and 7 are all irreducible in $\mathbb{Z}[\sqrt{-2}]$.

The element $\sqrt{-2}$ is irreducible since the only elements of $\mathbb{Z}[\sqrt{-2}]$ with norm smaller than that of $\sqrt{-2}$ are units. (See problem 12(b).)

The elements $1 \pm \sqrt{-2}$ are irreducible because the only nonunits of $\mathbb{Z}[\sqrt{-2}]$ with norm smaller than them are $\pm\sqrt{-2}$, and these do not divide $1 \pm \sqrt{-2}$.

We can see that 5 and 7 are irreducible as follows: recall that the norm on $\mathbb{Z}[\sqrt{-2}]$ is multiplicative: $N(ab) = N(a)N(b)$. So an irreducible factor x of 5 (or 7) must divide $N(5) = 5^2$ (or $N(7) = 7^2$). If $N(x) = N(5)$ then x is a unit multiple of 5 (similarly for 7), and if $N(x) = 1$, then x is a unit. So we must have $N(x) = 5$ (respectively, $N(x) = 7$). Is this possible? No. There are no elements of $\mathbb{Z}[\sqrt{-2}]$ with norm 5 or 7 (just checking by hand). So 5 and 7 are irreducible.

12. Let R be a Euclidean Domain.

(a). The elements of R of second smallest size are the units of R.

Proof. Suppose $a \in R$ is of second smallest size. Then write

$$1 = qa + r$$

for some $q, r \in R$ with $N(r) < N(a)$. Since a has second smallest size, r must have smallest size, so $r = 0$. Thus, $1 = qa$, and a is a unit.

Now suppose a is a unit, with $ab = 1$. Then

$$N(a) \leq N(ab) = N(1) \leq N(a).$$

Thus, $N(a) = N(1)$. But we know that the size of 1 is second smallest, since

$$N(1) \leq N(1 \cdot x) = N(x)$$

for any $x \in R$. Thus, the size of a is second smallest.

■

(b). The elements of R of third smallest size are irreducible.

Proof. Suppose $x \in R$ has third smallest size, and suppose we can write $x = ab$. Then

$$N(a) \leq N(ab) = N(x) \quad \text{and} \quad N(b) \leq N(ab) = N(x).$$

Suppose $N(b) < N(x)$. Then $N(b)$ has second smallest size (since we can't have $b = 0$), so b is a unit. So suppose $N(b) = N(x)$. By the division algorithm, there are $q, r \in R$ such that

$$b = qx + r = q(ab) + r$$

and $N(r) < N(x) = N(b)$. We can rewrite this as

$$(1 - qa)b = r.$$

We certainly have $b \neq 0$. Also, if $1 - qa \neq 0$, then

$$N(b) \leq N((1 - qa)b) = N(r).$$

But this is a contradiction, because $N(r) < N(b)$. So we must have $1 - qa = 0$, that is, a is a unit.

So we have shown that one of a or b is a unit, thus, x is irreducible. ■

(c). Every nonzero, nonunit element of R is irreducible or a product of irreducible elements.

Proof. Take any nonzero, nonunit element $x \in R$. We proceed by induction on $N(x)$. Certainly, if $N(x)$ is third smallest, then x is irreducible (by part (b)). So suppose x is nth smallest, and suppose that every element of R that is of $(n-1)$st size or less is irreducible or a product of irreducibles. If x is irreducible, we are done, so suppose $x = ab$, with $a, b \in R$ not units. Suppose $N(a) = N(x)$. We proceed as in part (b). Pick $q, r \in R$ with $N(r) < N(x) = N(a)$ such that

$$a = q(ab) + r.$$

Then $r = a(1 - qb)$. If $1 - qb \neq 0$, then

$$N(a) \leq N(a(1 - qb)) = N(r).$$

But this is impossible, since $N(r) < N(a)$. So $1-qb = 0$, and b is a unit. But this contradicts our choice of b. So we cannot have $N(a) = N(x)$.

By symmetry, we cannot have $N(b) = N(x)$ either. Thus, $N(a) < N(x)$ and $N(b) < N(x)$. Now we can apply the inductive hypothesis to write a and b as products of irreducibles. This expresses x as a product of irreducibles.

■

13. Use 12(b) to list the irreducible elements of third smallest size if:

(a). $R = \mathbb{Z}[i]$.

The elements of third smallest size are $\pm 1 \pm i$.

(b). $R = \mathbb{Z}[\sqrt{-2}]$.

Here the elements of third smalest size are $\pm\sqrt{-2}$, having size 2.

(c). $R = \mathbb{Z}[e^{2\pi i/3}]$.

The third smallest size is 3, and the elements having that size are:

$$2 + e^{2\pi i/3}, e^{2\pi i/3} - e^{4\pi i/3}, -1 + e^{2\pi i/3}$$

and their negatives.