Homework #8 Solutions

p 333, #6 Let $D$ be an integral domain and $a, b, c \in D$

(i) Reflexivity. Since $a = 1a$ and 1 is a unit, $a \sim a$.

(ii) Symmetry. If $a \equiv b$ then $a = ub$ for some unit $u \in D$. But then $b = u^{-1}a$ so that $b \sim a$, since $u^{-1}$ is also a unit in $D$.

(iii) Transitivity. If $a \equiv b$ and $b \equiv c$ then there exist units $u, v \in D$ so that $a = ub$ and $b = vc$. But then $a = ub = u(vc) = (uv)c$. Since the set of units in $D$ is closed under multiplication, $uv$ is also a unit and hence $a \sim c$.

p 333, #8 Let $u$ be a unit in $D$. Then $d(1) \leq d(1u) = d(u)$ and $d(1) = d(uu^{-1}) \geq d(u)$ so that $d(u) = d(1)$. Now suppose that $d(u) = d(1)$. Use the division algorithm to write $1 = qu + r$ for some $q, r \in D$ with $r = 0$ or $d(r) < d(u) = d(1)$. Since $d(1) \leq d(1r) = d(r)$, the latter case cannot occur so we conclude that $r = 0$, i.e. $1 = qu$ for some $q \in D$. That is, $u$ is a unit in $D$.

p 333, #10 It should be pointed out that the problem is incorrectly stated in the text. One must assume at the beginning that $p$ is nonzero. We do so below.

Let $p \in D$ be irreducible and let $I \subset D$ be an ideal with $\langle p \rangle I$. Since $D$ is a PID, $I = \langle a \rangle$ for some $a \in D$. Then $\langle p \rangle \subset \langle a \rangle$ implies that $p = ab$ for some $b \in R$. As $p$ is irreducible, either $a$ is a unit, in which case $I = \langle a \rangle = D$, or $b$ is a unit, in which case $I = \langle a \rangle = \langle p \rangle$. This proves that $\langle p \rangle$ is maximal.

Now suppose that $\langle p \rangle$ is maximal. Since a maximal ideals are always proper, $p$ is not a unit in $D$. Suppose that $p = ab$ for some $a, b \in D$. Then $p \in \langle a \rangle$ so that $\langle p \rangle \subset \langle a \rangle$. The maximality of $\langle p \rangle$ implies that $\langle p \rangle = \langle a \rangle$ or that $\langle a \rangle = D$. In the first case it follows that $a \in \langle p \rangle$ so that $a = kp$ for some $k \in D$. But then $p = ab = (kp)b = p(kb)$ and cancelation in $D$ implies that $kb = 1$, i.e. $b$ is a unit. In the second case, $a$ is a unit since $1 \in \langle a \rangle$ implies that $1 = ka$ for some $k \in D$. So, we have shown that if $p = ab$ in $D$ then either $a$ or $b$ is a unit, and hence $p$ is irreducible.

p 333, #12 Let $I \subset D$ be a proper ideal. If $I$ is maximal, there is nothing to show. So suppose that $I$ is not maximal. Then there is a proper ideal $I_2 \neq I$ so that $I \subset I_2$. If $I_2$ is maximal we are finished. If not, then we may find a proper ideal $I_3 \neq I_2$ so that $I_2 \subset I_3$. Continue to construct ideals in this way: if $I_n$ is not maximal then choose a proper ideal $I_{n+1} \neq I_n$ so that $I_n \subset I_{n+1}$. If none of the ideals $I_n$ is ever maximal then we obtain an infinite ascending chain of ideals $I \subset I_1 \subset I_2 \subset I_3 \subset \cdots$ in which every containment is proper. However, we know that no such a chain can exist in a PID. It follows that at some point one of the $I_n$ will be maximal and since $I \subset I_1 \subset I_2 \subset \cdots \subset I_n$, this finishes the proof.
p 334, #14 In \( \mathbb{Z}[i] \) we have \( N(1 - i) = 1 + 1 = 2 \), which is prime. Therefore \( 1 - i \) is irreducible.

p 334, #18 In \( \mathbb{Z}[\sqrt{6}] \), \( N(7) = 49 \). So 7 is not a unit and if \( 7 = xy \) in \( \mathbb{Z}[\sqrt{6}] \) for some nonunits \( x \) and \( y \), then \( N(x) = \pm 7 \). Writing \( x = a + b\sqrt{6} \) for some \( a, b \in \mathbb{Z} \) this would mean that \( a^2 - 6b^2 = \pm 7 \). Going mod 7 we obtain \( a^2 - 6b^2 = 0 \) in \( \mathbb{Z}_7 \) or \( a^2 = 6b^2 \). If \( b \neq 0 \) in \( \mathbb{Z}_7 \) then this yields \( (a/b)^2 = 6 \), which is impossible since 6 is not a square in \( \mathbb{Z}_7 \). Therefore \( a = b = 0 \) in \( \mathbb{Z}_7 \), i.e. both \( a \) and \( b \) are divisible by 7. But then both \( a^2 \) and \( b^2 \) are divisible by 7^2, which implies that 49 divides \( a^2 - 6b^2 = \pm 7 \), an impossibility. This contradiction means that if \( 7 = xy \) in \( \mathbb{Z}[\sqrt{6}] \) then \( x \) or \( y \) is a unit, i.e. 7 is irreducible.

p 334, #20 According to Example 1, \( \mathbb{Z}[\sqrt{-3}] \) has irreducible elements that are not prime. Since every irreducible in a UFD is also prime, \( \mathbb{Z}[\sqrt{-3}] \) is not a UFD. Since every PID is also a UFD, \( \mathbb{Z}[\sqrt{-3}] \) is not a PID, either.

p 334, #22 In \( \mathbb{Z}[\sqrt{5}] \) we have \( N(2) = 4 \), so 2 is not a unit. If \( 2 = xy \) with neither \( x \) nor \( y \) a unit in \( \mathbb{Z}[\sqrt{5}] \) then it must be the case that \( N(x) = \pm 2 \). Then we would have integers \( a, b \) so that \( \pm 2 = N(a + b\sqrt{5}) = a^2 - 5b^2 \), which implies that \( a^2 \) (mod 5) = 2 or 3, neither of which is possible. Hence, if \( 2 = xy \) in \( \mathbb{Z}[\sqrt{5}] \) then \( x \) or \( y \) is a unit, which means that 2 is irreducible in \( \mathbb{Z}[\sqrt{5}] \). Notice that \( 2 \cdot 2 = 4 = (1 + \sqrt{5})(-1 + \sqrt{5}) \), so that 2 divides \( (1 + \sqrt{5})(-1 + \sqrt{5}) \), but 2 divides neither \( 1 + \sqrt{5} \) nor \(-1 + \sqrt{5} \), proving that 2 is not prime in \( \mathbb{Z}[\sqrt{5}] \).

Similarly, in \( \mathbb{Z}[\sqrt{5}] \) we have \( N(1 + \sqrt{5}) = -4 \), which proves that \(-4 \) is not a unit. Moreover, if \( 1 + \sqrt{5} = xy \) in \( \mathbb{Z}[\sqrt{5}] \) with neither \( x \) nor \( y \) a unit then, as above, \( N(x) = \pm 2 \), which we have already argued is impossible. It follows that \( 1 + \sqrt{5} \) is irreducible. Again noting that \( 2 \cdot 2 = 4 = (1 + \sqrt{5})(-1 + \sqrt{5}) \), we see that \( 1 + \sqrt{5} \) divides \( 2 \cdot 2 \). But for any \( a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}] \) we have \( (a + b\sqrt{5})(1 + \sqrt{5}) = (a + 5b) + (a + b)\sqrt{5} \), which can never equal two since the system \( a + 5b = 2, a + b = 0 \) has no solution in integers. Therefore, \( 1 + \sqrt{5} \) does not divide 2, showing that the former is not prime in \( \mathbb{Z}[\sqrt{5}] \).

p 334, #28 We know that \( x + iy \in \mathbb{Z}[i] \) is a unit if and only if \( 1 = N(x + iy) = x^2 + y^2 \). Since \( x \) and \( y \) are both integers this can only occur if \( (x^2, y^2) = (1, 0) \) or \( (x^2, y^2) = (0, 1) \), which means that \( x + iy \) is one of the four elements \( \pm 1, \pm i \).

p 334, #30 This is not a contradiction because the irreducible factors in question are associates, which is all we are guaranteed in a UFD. In particular we have \( 3(3x + 2) = 9x + 6 = 4x + 1 \) and \( 2(x + 4) = 2x + 8 = 2x + 3 \) over \( \mathbb{Z}_5 \), and both 3 and 2 are units in \( \mathbb{Z}_5 \).

p 335, #34 A subdomain of a Euclidean domain need not be Euclidean. For example, the ring \( \mathbb{Z}[x] \) is not a PID and therefore is not Euclidean, however it is a subdomain of \( \mathbb{Q}[x] \) which we know to be a Euclidean domain.