18 Divisibility in Integral Domains

2. In an integral domain, show that a and b are associates if and only if $\langle a\rangle = \langle b\rangle$

Assume that a and b are associates, show $\langle a\rangle = \langle b\rangle$. So a and b are irreducible and $u^{-1}a = b$. but $u^{-1}a \in \langle a\rangle$, which implies that $\langle a\rangle = \langle b\rangle$.
Now assume that $\langle a\rangle = \langle b\rangle$, show that $a = ub$.
By definition of ideal $a = tb$ and $b = sa$. This means that $a = (ts)a$, and because this is an integral domain, $1 = ts$. This imples that both t and s are units, and so a and b are associates.

8. Let D be a Euclidean domain with measure d. Prove that u is a unit in D if and only if $d(u) = d(1)$.

Assume that u is a unit in D, show that $d(u) = d(1)$.
By the properties of Euclidean domains, we can say that $d(u) \leq d(uu^{-1}) = d(1) \leq d(1u) = d(u)$. This immediately implies that $d(u) = d(1)$.
Suppose instead that $d(u) = d(1)$, show that u is a unit in D.
So $d(u) = d(1)$, which implies that $d(1) = d(u) \leq d(uq)$. However, $1 = uq + r$, and so $d(1) = d(uq + r)$. When $r = 0$, this implies that $d(1) = d(uq)$, which shows u is a unit. If $r \neq 0$, then $d(r) < d(u) = d(1)$. Which means that $0 < d(u) - d(r)$ or $0 < d(1) - d(r)$, so we can say that $d(r) = 0$. Subsequently, $0 < d(1) - d(r) \leq d(uq) - d(r)$, or $d(r) = 0 < d(1) = d(uq + r) \leq d(uq) = d(1)$. This implies that u is a unit.

10. Let D be a principal ideal domain and let $p \in D$. Prove that $\langle p\rangle$ is a maximal ideal in D if and only if p is irreducible.

Assume that $\langle p\rangle$ is a maximal ideal in D, we must show that p is irreducible.
Let $a, b \in D$, such that $p = ab$. We can say that $p - ab \in \langle p\rangle$ and $p - ab = 0$, which imples that $a^{-1}p - b = 0$, or $a^{-1}p = b$. This means that $\langle p\rangle = \langle b\rangle$. If b is a unit, then $\langle b\rangle = D$, which means that $\langle p\rangle$ is not maximal, which is a contradiction. This means that p is irreducible.
Suppose p is irreducible over D that $\langle q\rangle$ is an ideal of D such that $p \in \langle q\rangle$ and $p = aq$ for some a in D. If q is a unit then q^{-1} exists which means $\langle q\rangle = D$, which is a contradiction. On the other hand, if a is a unit then $q = a^{-1}p$, which implies that $q \in \langle p\rangle$, so $\langle p\rangle = \langle q\rangle$, a contradiction. Therefore a and q are nonunits which implies p is reducible, which is a contradiction.

15. Over $\mathbb{Z}[\sqrt{-6}]$, $10 = 2(5)$ and $10 = (2 + \sqrt{-6})(2 - \sqrt{-6})$, which implies that $\mathbb{Z}[\sqrt{-6}]$ is not a UFD, and is therefore not a PID.

17. Over $\mathbb{Z}[i]$, $3 = 1(3)$ or $(1 + \sqrt{2}i)(1 - \sqrt{2}i) = 3$ but $\sqrt{2} \notin \mathbb{Z}[i]$. However, $2 = 2(1) = (1 + i)(1 - i)$ where $(1 + i)$ and $(1 - i)$ are not units, and $5 = 1(5) = (1 + 2i)(1 - 2i)$ are non units.

22. $\mathbb{Z}[\sqrt{5}]$, show that $2, 1 + \sqrt{5}$ are irreducible but not prime.

We can see that 2 divides 6, but 2 does not divide either $(1 + \sqrt{5})(1 - \sqrt{5})$, which shows that 2 is not prime over $\mathbb{Z}[\sqrt{5}]$. Likewise, $1 + \sqrt{5}$ divides $(1 + \sqrt{5})(1 - \sqrt{5}) = 6$, however, $1 + \sqrt{5}$ does not divide either 2 or 3, so $1 + \sqrt{5}$ is not prime.

35. D is a PID, p is irreducible over D. Prove that $D/\langle p\rangle$ is a field.

We must show that $\langle p\rangle$ is maximal. Because $p = uq$, we know that $uu^{-1}q$ is an element of $\langle p\rangle$, which implies that $\langle p\rangle = \langle q\rangle$. Now we'll assume to the contrary that q is a unit of D, this immediately implies that $\langle q\rangle = D$ which shows $\langle p\rangle$ is not maximal, a contradiction.

Because $\langle p\rangle$ is maximal, we know by Theorem 14.4 that $D/\langle p\rangle$ is a field.

40. Find the inverse of $1+\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$.

Observe that $(1+\sqrt{2})(-1+\sqrt{2}) = -1+\sqrt{2}-\sqrt{2}+2 = 1$, which shows the inverse of $1+\sqrt{2}$ is $-1+\sqrt{2}$. We can also see that $1+\sqrt{2}$ has inifinite multiplicative order.