10pt **8.2.4.** *Let R be an integral domain. Prove that the following two conditions (together) imply that R is a PID:*
(i) Any two nonzero elements $a, b \in R$ have a greatest common divisor of the form $ra+sb$ for some $r, s \in R$.
(ii) R satisfies the ascending chain condition for principal ideals: if $a_1, a_2, \dots$ are nonzero elements of R such that $a_{i+1} \,\big|\, a_i$ for all i, then there is n such that the elements $a_n, a_{n+1}, \dots$ are all associate.

Solution. Condition (i) says that any ideal (a, b) generated by two elements is principal.

Let I be a nonzero ideal in R. Choose any nonzero $a_1 \in I$. If $I \neq (a_1)$, choose any $b_2 \in I \setminus (a_1)$. By assumption, the ideal (a_1, b_2) is principal, $= (a_2)$ for some $a_2 \in R$. If $I \neq (a_2)$, choose $b_3 \in I \setminus (a_2)$, etc. The sequence $(a_1) \subset (a_2) \subset \cdots$ is a strictly increasing sequence of principal ideals, by condition (ii) it cannot be infinite, that is, $I = (a_n)$ for some n.

10pt **8.1.7(a).** *Find the generator for the ideal $(85, 1+13i)$ in $\mathbb{Z}[i]$.*

Solution. The problem is to find the gcd of 85 and $1 + 13i$. We could try to guess it, using the field norm N. But since $\mathbb{Z}[i]$ is a ED, we can use the Euclidean algorithm instead. We have $85/(1 + 13i) = 0.5 - 6.5i$; as the nearest element of $\mathbb{Z}[i]$ take $-6i$, and get

$$85 = (-6i)(1 + 13i) + (7 + 6i).$$

Next, $(1 + 13i)/(7 + 6i) = 1 + i$, so $7 + 6i$ divides $1 + 13i$,

$$1 + 13i = (1 + i)(7 + 6i),$$

which means that we are done, and $(85, 1 + 13i) = (7 + 6i)$.

10pt **8.1.9.** *Prove that the ring $\mathbb{Z}[\sqrt{2}]$ is a ED with respect to the norm $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.*

Solution. N is the absolute value of the field norm, and is a multiplicative function. Now, given $\alpha, \beta \in \mathcal{O}$, $\alpha \neq 0$, write $\beta/\alpha = x+y\sqrt{2}$ with $x, y \in \mathbb{Q}$. Find $c, d \in \mathbb{Z}$ such that $|x-c|, |y-d| \leq 1/2$, and put $\gamma = c+d\sqrt{2}$. Then

$$N(\beta/\alpha - \gamma) = N\big((x + y\sqrt{2}) - (c + d\sqrt{2})\big) = \big|(x - c)^2 - 2(y - d)^2\big| \leq 1/2,$$

so, for $\delta = \beta - \gamma\alpha$, we have $N(\delta) = N(\beta/\alpha - \gamma)N(\alpha) \leq \frac{1}{2}N(\alpha) < N(\alpha)$. Hence, we have $\beta = \gamma\alpha + \delta$, with $\gamma, \delta \in \mathcal{O}$, and $N(\delta) < N(\alpha)$, which proves that $\mathcal{O}$ is Euclidean.

8.3.5. *Let $R = \mathbb{Z}[\omega]$ where $\omega = \sqrt{-n}$ and n is a squarefree integer ≥ 5.*

5pt (a) *Prove that 2 is irreducible in R.*

Solution. For $\alpha = a + b\omega \in R$, $a, b \in \mathbb{Z}$, we have $N(\alpha) = a^2 + nb^2$, and if $b \neq 0$, then $N(\alpha) \geq n$. If $\alpha \,\big|\, 2$ then $N(\alpha) \,\big|\, N(2) = 4$, so $b = 0$, so $\alpha = a \,\big|\, 2$, so $a = \pm 1, \pm 2$. Hence, 2 is irreducible.

5pt (b) *Prove that 2 is not prime in R and deduce that R is not a UFD.*

Solution. If n is even, then $2 \,\big|\, n = -\omega^2$, but $2 \nmid \omega$. (For any $\alpha = a + b\omega \in R$ the element $2\alpha = 2a + 2b\omega$ has even coefficients.)

If n is odd, then $2 \,\big|\, (1 + n) = (1 - \omega)(1 + \omega)$, but $2 \nmid 1 \pm \omega$.

So, in both cases, the irreducible element 2 is not prime, hence, R is not a UFD.

8.3.8. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, the ring of quadratic integers associated with $D = -5$. Let $\alpha = 1 + \sqrt{-5}$, then $\overline{\alpha} = 1 - \sqrt{-5}$.*

5pt (b) *Let $I_2 = (2, \alpha)$ and $I_3 = (3, \alpha)$, then $\overline{I}_3 = (3, \overline{\alpha})$. Prove that $\overline{I}_2 = I_2$, and that I_2, I_3, and $\overline{I}_3$ are maximal ideals in $\mathcal{O}$.*

Solution. Since $\overline{\alpha} = 2 - \alpha$, I_2 is "self-conjugate": $I_2 = (2, \alpha) = (2, \overline{\alpha}) = \overline{I}_2$.

In R/I_2, $2 = 0$ and $\sqrt{-5} = -1 = 1$, so $R/I_2 \cong \mathbb{Z}_2$, which is a field, so I_2 is maximal.

In R/I_3, $3 = 0$ and $\sqrt{-5} = -2 = 1$, so $R/I_3 \cong \mathbb{Z}_3$, which is a field, so R/I_3 is maximal.

$\overline{I}_3$ is conjugate to I_3, so is also maximal.

10pt (c) *Prove that $(2) = I_2^2$, $(3) = I_3\overline{I}_3$, $(\alpha) = I_2 I_3$, and $(\overline{\alpha}) = I_2\overline{I}_3$.*

Solution.
$$I_2^2 = (2^2, 2\alpha, \alpha^2) = \big(4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\big).$$
All the generators of I_2^2 are divisible by 2, so $I_2^2 \subseteq (2)$. Also, $2 = -4 + (2+2\sqrt{-5}) - (-4+2\sqrt{-5})$, so $2 \in I_2^2$, so $(2) \subseteq I_2^2$.
$$I_3\overline{I}_3 = \big(3^2, 3\overline{\alpha}, 3\alpha, \alpha\overline{\alpha}\big) = \big(3^2, 3\overline{\alpha}, 3\alpha, 6\big),$$
so $I_3\overline{I}_3 \subseteq (3)$. Also, $3 = 9 - 6$, so $(3) \subseteq I_3\overline{I}_3$.
$$I_2I_3 = \big(2\cdot 3, 2\alpha, 3\alpha, \alpha^2\big).$$
Since $2\cdot 3 = 6 = \alpha\overline{\alpha}$, all the generators of I_2I_3 are divisible by α, so $I_2I_3 \subseteq (\alpha)$. Also, $3\alpha - 2\alpha = \alpha$, so $(\alpha) \subseteq I_2I_3$.

Since $I_2 = \overline{I}_2$, $I_2\overline{I}_3 = \overline{I_2I_3}$, so $I_2\overline{I}_3 = (\overline{\alpha})$.

Now, $(6) = (2)(3) = I_2^2I_3\overline{I}_3$, and $(6) = (\alpha)(\overline{\alpha}) = I_2\overline{I}_3I_2I_3 = I_2^2I_3\overline{I}_3$.

10pt **8.3.9.** *If a quadratic integer ring $\mathcal{O}$ is a PID, prove that the absolute value $|N|$ of the field norm N on $\mathcal{O}$ is a Dedekind-Hasse norm.*

Solution. Let $\alpha, \beta \in \mathcal{O}$. Since $\mathcal{O}$ is a PID, the ideal $(\alpha, \beta) = (\gamma)$ for some $\gamma \in \mathcal{O}$. Then $\gamma \,\big|\, \beta$, so $N(\gamma) \,\big|\, N(\beta)$, so $|N(\gamma)| \le |N(\beta)|$. If $|N(\gamma)| = |N(\beta)|$, then $N(\beta/\gamma) = \pm 1$, so β/γ is a unit, so $(\beta, \alpha) = (\gamma) = (\beta)$, so $\alpha \in (\beta)$. Otherwise $|N(\gamma)| < |N(\beta)|$, which just proves that $|N|$ is a Dedekind-Hasse norm.