COMMUTATIVE ALGEBRA HW 16 SOLNS

JC

(1) Let $\beta = i\sqrt{5}$ so that $\mathbb{Q}(\beta) = \{a + b\beta : a, b \in \mathbb{Q}\}$

Let $F = Q(\beta)$ and $R = \mathfrak{o}_F$, the ring of integers

(a) Show that $R = \mathbb{Z}[\beta]$ and $\mathbb{Z}[\beta] = \{m + n\beta : m, n \in \mathbb{Z}\}$.
The second claim is easy as $\beta^2 = -5 \in \mathbb{Z}$. For the first one suppose that $a + b\beta$ is an algebraic integer. Then either $b = 0$ so a is a rational integer, or $b \neq 0$ so $a + b\beta \notin \mathbb{Q}$; in the latter case its minimal polynomial must be $x^2 - 2ax + (a^2 + 5b^2)$, by an old HW the coefficients must be rational integers, so by easy number theory a and b are rational integers.

(b) Show if we define $N(a + b\beta) = a^2 + 5b^2$ for $a, b \in \mathbb{Q}$ then $N(cd) = N(c)N(d)$ for all $c, d \in F$.
Argt 1: brute force calculation. Argt 2: $N(z) = |z|^2$. Argt 3: $N(z)$ is the determinant of the linear map $a \mapsto za$ from F to F. Use the multiplicative property of the determinant.

(c) Use N to identify the units of R and to show that each of 2, 3, $1 + \beta$, $1 - \beta$ is irreducible in R.
If $m + n\beta$ is a unit then $m^2 + 5n^2 = 1$ so $m = 1, -1$ and $n = 0$. There are no elements with $N(z) = 2, 3$ so easily each of the named elements is irreducible.

(d) Use the equation $2 \times 3 = (1 + \beta)(1 - \beta)$ to show that none of $2, 3, 1 + \beta, 1 - \beta$ is prime in R.
Easy! For example 2 divides the product on the RHS but not either factor.

(e) Factorise each of the ideals $(2)_R, (3)_R, (1 + \beta)_R, (1 - \beta)_R$ into prime ideals of R.
$I = (2)$. The quotient ring has 4 elements which (abusively) we write as $0, 1, \beta, 1 + \beta$. $\beta^2 = 1$ so β is not in a prime ideal. $1 + \beta$ generates the ideal $\{0, 1 + \beta\}$ which has quotient the two element field so is prime (in fact maximal, no surprise as R is a DD).

Back in R the only prime ideal containing (2) is thus $(2, 1+\beta)$. So we expect (2) is some power of it. In fact $(2, 1+\beta)^2 = (4, 2+2\beta, -4+2\beta) = (2)$.
$I = (3)$. A little thought shows that in R/I we have $\beta(1+\beta) = 1+\beta$ so that $1+\beta$ generates a prime ideal $\{0, 1+\beta, 2+2\beta\}$. Similarly $\beta(1+2\beta) = 2+\beta$ so $1+2\beta$ generates prime ideal $\{0, 1+2\beta, 2+\beta\}$. Other elements will not work as $\beta^2 = 2^2 = (2\beta)^2 = 1$.
Back in R we get candidate factors $(3, 1+\beta)$ and $(3, 1+2\beta) = (3, 1-\beta)$. In fact we see $(3, 1+\beta)(3, 1-\beta) = (9, 3+3\beta, 3-3\beta, 6) = (3)$.
Similar calculations (or inspired guesswork or computer algebra or using the idea of the next question) gives us that $(2, 1+\beta)(3, 1+\beta) = (1+\beta)$ and $(2, 1+\beta)(3, 1-\beta) = (1-\beta)$. Of course it is helpful that $(2, 1+\beta) = (2, 1-\beta)$.

(f) Check your computation by verifying that the same prime ideals appear in the resulting prime factorisations of $(2)(3)$ and $(1+\beta)(1-\beta)$.
Easy: both sides are $(2, 1+\beta)^2(3, 1+\beta)(3, 1-\beta)$.

(2) Consider the metric d on $\mathbb{Z}$ in which the distance between distinct integers m and n is p^{-a} where a is the largest natural number such p^a divides $m-n$. We say that two Cauchy sequences (a_i) and (b_i) of integers are equivalent iff $d(a_i, b_i) \to 0$ as $i \to \infty$. This is an equivalence relation on Cauchy sequences. Show that every equivalence class contains exactly one sequence (a_i) such that $0 \le a_i < p^i$ and a_i is congruent to a_{i+1} modulo p^i for all i.

It is easy to see that no two such sequences are equivalent, for if they first differ at place i then the distance between subsequent terms is constant at p^{-i}.

So it suffices to show that every Cauchy sequence is equivalent to such a sequence. Let (a_i) be Cauchy. For each n there is i such that for $j \ge i$ $d(a_i, a_j) \le p^{-n}$, that is a_i and a_j are congruent modulo p^n. So choose b_n to be the unique integer such that $0 \le b_n < p^n$ and a_i is congruent to b_n mod p^n for all large i.

Now for all large i we have that a_i and b_n are congruent mod p^n and also that a_i and b_{n+1} are congruent mod p^{n+1}. So b_n and b_{n+1} are congruent mod p^n.

Finally if we fix m then for all large enough $i > m$, a_i is congruent to b_m mod p^m. But also b_m is congruent to b_i mod p^m, so that $d(a_i, b_i) \le p^{-m}$.