Section 5.1

1. (Problem 7) Find the units in $\mathbf{Z}[\sqrt{-5}]$.

Solution: Recall we have the "norm" function $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{Z}$ given by $N(a + b\sqrt{-5}) = a^2 + 5b^2$ which is multiplicative, i.e. satisfies $N(xy) = N(x)N(y)$ for $x, y \in \mathbf{Z}[\sqrt{-5}]$ (this is easy to prove, just tedious). Furthermore, notice that $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5})$; from this we conclude if $N(a + b\sqrt{-5}) = 1$ then $a + b\sqrt{-5}$ is a unit with inverse $a - b\sqrt{-5}$. The converse is true as well: if x is a unit in $\mathbf{Z}[i]$, then

$$1 = N(1) = N(xx^{-1}) = N(x)N(x^{-1}),$$

which because $N(x)$ and $N(x^{-1})$ are nonnegative integers (this is easy to see from the way N is defined), we conclude $N(x) = N(x^{-1}) = 1$.

Thus determining the units of $\mathbf{Z}[\sqrt{-5}]$ is the same as determining which elements $a+b\sqrt{-5}$ satisfy $a^2 + 5b^2 = 1$. But if $b \neq 0$ then $a^2 + 5b^2 \geqslant 5$ so this is impossible, and we see any such element satisfies $b = 0$. But then we have $a^2 = 1$ so $a = \pm 1$, and we deduce the units of $\mathbf{Z}[\sqrt{-5}]$ are exactly ± 1.

2. (Problem 10a) Determine whether $p = 11$ is irreducible in $\mathbf{Z}[i]$.

Solution: Just as in the previous solution, it is important to remember that we have the norm function $N : \mathbf{Z}[i] \to \mathbf{Z}$ given by $N(a + bi) = a^2 + b^2$, which is again multiplicative, and by similar remarks for any $x \in \mathbf{Z}[i]$ we have $N(x) = 1 \iff x$ is a unit.

First we notice 11 is not a unit, for instance because $N(11) = 121 \neq 1$. Suppose $11 = xy$ for some $x, y \in \mathbf{Z}[i]$. Then using multiplicativity of the norm, we have

$$11^2 = N(11) = N(xy) = N(x)N(y),$$

so because $N(x), N(y) \geqslant 0$ are integers we see by prime factorization in $\mathbf{Z}$ that the only possibilities are $N(x) = 121$ and $N(y) = 1$, or $N(x) = 1$ and $N(y) = 121$, or $N(x) = 11$ and $N(y) = 11$. If the last possibility occurs and we write $x = a + bi$ for $a, b \in \mathbf{Z}$, then we have $11 = N(x) = a^2 + b^2$, and we claim this is not possible.

To see this, notice that if a is any integer, then a^2 is equivalent to either 0 or 1 modulo 4 (you can check this by cases on the value of a modulo 4), and the same applies to b. But then $a^2 + b^2$ can only be $0, 1$, or 2 modulo 4 (again, check this by cases on the possible combination of values of a^2 and b^2 modulo 4). Thus we can never have $a^2 + b^2 \equiv 3 \bmod 4$ for any $a, b \in \mathbf{Z}$, and in particular we can never have $a^2 + b^2 = 11$.

Thus we conclude we either have $N(x) = 121$ and $N(y) = 1$ or $N(x) = 1$ and $N(y) = 121$. In the former case we deduce x is a unit, and in the latter case we deduce y is a unit, so this proves 11 is irreducible in $\mathbf{Z}[i]$.

Section 5.2

3. (Problem 1) Is every subring of a PID again a PID?

Solution: No; a simple counterexample is given by $\mathbf{Z}[x] \subset \mathbf{Q}[x]$.

Here is a more general method which can sometimes be useful with coming up with counterexamples to questions of the form "is a subring of a *blah* again a *blah*" (if you suspect that the claim is false): first, ask yourself if fields are *blah*. In our case, fields are PID's (fields are integral domains, and they have two ideals, $\langle 0 \rangle$ and $\langle 1 \rangle$, which are both principal), so we can proceed.

Next, find (if possible) an example of an integral domain which is not a *blah*. In our case, we can take $R = \mathbb{Z}[x]$ or $R = F[x, y]$ for a field F. Then recall that we have the field of fractions $Q(R)$ of R, which is a field, hence a PID. But R is a subring of $Q(R)$, so as long as R is chosen to not be a PID then $R \subset Q(R)$ gives us a subring of a PID which is not a PID.

4. (Problem 8b) If $I \neq 0$ is an ideal of $\mathbf{Z}_{(p)}$, show that $I = \langle p^k \rangle$ where $k \geqslant 0$ is the smallest integer such that $p^k \in A$.

Solution: First we need to make sure such an integer k exists; since $I \neq 0$, we can take some nonzero $x \in I$; since $x \in \mathbf{Z}_{(p)}$ we can write $x = a/b$ where $a, b \in \mathbf{Z}$ and $p \nmid b$. By prime factorization of integers we can write $a = p^r c$ where $r \geqslant 0$ and $p \nmid c$. Then $x = p^k(c/b)$. But from part (a), since $p \nmid b$ and $p \nmid c$ we see that c/b is a unit in $\mathbf{Z}_{(p)}$ with inverse b/c. Since $x \in I$ we have that $p^r = x(b/c) \in I$. The result of this is that we know there exists some $p^r \in I$, and then defining k to be the smallest such value of r is justified.

Now we want to prove $I = \langle p^k \rangle$. The inclusion $\langle p^k \rangle$ is immediate since $p^k \in I$ by the way we chose k. On the other hand, clearly $0 \in \langle p^k \rangle$, so take some $x \in I \setminus \{0\}$. By the exact argument we did above, we can write $x = p^r(c/b)$ where $p \nmid b$ and $p \nmid c$, and we can conclude in the same way that $p^r \in I$. But then we know by our choice of k that we must have $k \leqslant r$ (remember k was chosen to be minimal), and then $r - k \geqslant 0$ so $p^{r-k} \in \mathbf{Z}_{(p)}$ and thus we have

$$x = p^r c/b = p^k(p^{r-k} c/b) \in \langle p^k \rangle,$$

which proves the other inclusion.