Comments on Ch. 8 Homework

8.2.5 Think of $R = \mathbb{Z}[\sqrt{-5}]$ as $\mathbb{Z}[X]/(X^2+5)$. Let x denote the natural image of X in R. Argue that $2, 3$ are irreducible by the usual norm argument. First, note that $u \in R$ is a unit iff $N(u) = 1$ iff $u = \pm 1$.

If $p \in \mathbb{Z}$ is a prime and p is reducible in R, then $p = ab$ where a, b are non units. Then $p^2 = N(p) = N(a)N(b)$ implies $N(a) = N(b) = p$.

Since $N(f + gx) = f^2 + 5g^2$ this is not possible for $p = 2, 3$.

Note that if an ideal $I = (a, b) \neq R$ where a is irreducible and $I = (f)$ for some f (i.e. I is principal), then $f|a$ and since f is a non unit, f is an associate of a. Thus, a must divide b.

Now, it is easy to see that the ideals $I_2, I_3, {I_3}'$ are non principal.

To argue that the ideals are not unit ideals, calculate their residue class rings. Thus, $R/I_3 = \mathbb{Z}[X]/(J)$ where $J = (X^2+5, 3, 2+X)$. Note that $J = ((X+2)(X-2)+9, 3, X+2) = (3, X+2)$ and so the ring is $\mathbb{Z}_3[X]/(X+3) = \mathbb{Z}_3$.

This proof is better than the book's!

Here is an explicit proof for principalness of $I_2 I_3$. Consider its lift, say K in $\mathbb{Z}[X]$ generated by $a = (X^2+5), b = (2)(3), c = (2)(2+X), d = (3)(1+X), (1+X)(2-X)$. Combining a, d get $7 + X$ in K and then using b, deduce that $1 + X \in K$.

Claim that K is generated by $a, 1+X$. Note that $b = 6 = (1+X)(1-X)+a$, $c = 4+2X = 6+2(X+1)$.

So, in R, the image of K is generated by $(1+x)$.

8.2.6 Some common omissions.

- A totally ordered set of ideals is best described as $\{I_r\}_{r \in S}$ where S is a totally ordered set. Writing a sequence is not sufficiently general!
- It is important to argue that the union I of such a totally ordered set is again non principal, for otherwise, its generator would be in some I_r and then $I_r = I$ will also be principal.
- The existence of a, b as stipulated in (b) should be proved by noticing that I being non principal, must not be prime!

8.2.6 Common omission was a detailed proof of (a) and not using induction for (b).

8.3.1 I would organize the argument differently.

- Argue that the given multiplicative group is isomorphic to a direct sum G of additive groups G_i where each G_i is isomorphic to $\mathbb{Z}$ for $i = 1, 2, \cdots$. The isomorphism is defined by $\psi(r) = (\mathrm{ord}_{p_1}(r), \mathrm{ord}_{p_2}(r), \cdots)$, where $p_1 = 2, p_2 = 3$ and generally p_i is the i-th prime.
- The fundamental theorem of Arithmetic guarantees (is equivalent to) that this ψ is an isomorphism.

- The group G has infinitely many automorphisms given by fixed permutations of its components. We then get different automorphisms of $\mathbb{Q}^\times$ by conjugation $\psi^{-1}\sigma\psi$.
  The one given in the book swaps the first and the second component.

8.3.5
- Start by writing the ring as $R = \mathbb{Z}[X]/(X^2+n)$ and denote the image of X by x. The arguments will be similar to 8.2.5.
- As before, units are still only ± 1 and irreducibility is deduced using norms. Thus, if $1+x = ab$, with a, b non units, note that $1+n = N(a)N(b)$. Note that norm of a non unit $u+vx$ is u^2+nv^2 is bigger than n if v is non zero. It follows that at least one of a, b must be in $\mathbb{Z}$. But then it must divide $1+n$ in R and hence divides 1 in $\mathbb{Z}$.. So, it would be a unit, contrary to assumption.
- To check if $(1+x)$ is prime, note that the residue class ring by it would be $\mathbb{Z}[X]/J$ where $J = (X^2+n, 1+X)$ But $X^2+n = (X+1)(X-1)+1+n$. So $J = (1+n, X+1)$.
  Now, $\mathbb{Z}[X]/(1+n, 1+X) \approx \mathbb{Z}_{1+n}[X]/(1+X) = \mathbb{Z}_{1+n}$.
  Thus, if $1+n$ is not prime, then $1+x$ is not prime!
  The case of x is similar.
  Also, out of n and $1+n$, at least one is even and bigger than 2, so non prime.
- To find an explicit non principal ideal, consider $(2, x)$. Since x is irreducible, this will be principal only if it is generated by x. But 2 is not in (x) since $R/(x) = \mathbb{Z}[X]/(X^2+n, x) = \mathbb{Z}_n$ and the image of 2 in this ring is non zero, since $n > 2$.

8.3.6
- The ring $\mathbb{Z}[i]/(1+i) = \mathbb{Z}[X]/J$ where $J = (X^2+1, 1+X) = (2, 1+X)$, so the ring is just $\mathbb{Z}_2$ as before.
- If q is $2, 3$ modulo 4, then the ring is $\mathbb{Z}[X]/K$ where $K = (X^2+1, q)$. The ring is then $\mathbb{Z}_q[Y]/(Y^2+1)$ where Y is the image of X modulo q (still transcendental). By assumption on q the ideal (Y^2+1) is prime and generated by a quadratic polynomial and hence the residue class ring is a 2 dimensional space over $\mathbb{Z}_q$.
- The case when p is 1 mod 4.
  Let $\pi = a+bx$ be an element with norm p. Then $\mathbb{Z}[X]/(X^2+1, a+bX) = \mathbb{Z}[X]/(p, a+bX) \approx \mathbb{Z}_p[Y]/(a+bY)$ where Y is the image of X modulo p (still transcendental). The last ring is clearly $\mathbb{Z}_p$ since b cannot be zero modulo p.
  The ring $\mathbb{Z}[X]/(X^2+1, p)$ is easily seen to be $\mathbb{Z}_p[Y]/(Y^2+1)$ and in the current case Y^2+1 is reducible. However, the residue class ring is still a vector space of dimension 2 and has p^2 elements.