Comments about some interesting h.w. problems, and other.

An irreducible in an integral domain R that is not a prime element of R.

Let $R = \mathbb{Z}[2i]$, a proper subring of $\mathbb{Z}[i]$, the Gaussian integers. So $\mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}$. (Let me emphasize that $i \notin R$.) Since R is a subring of an integral domain, a subring that contains 1, R is an integral domain. Notice that $2i \in R$ is irreducible—it's trivial to show this. Is $2i$ prime in R?

No, $2i$ is not prime in R: $(2)(2) = 4$ is in $(2i)$ since $4 = (2i)(-2i)$. But $2 \notin (2i)$, as can be verified quite easily. So $(2i)$ is not a prime ideal of R, and $2i$, despite being irreducible in R, is not prime in R.

Comments on problem 2, HW 3.

Let G be a finite group, and let $exp(G) = \min\{k \in \mathbb{N} : \forall g \in G\ g^k = e\}$. A corollary of Lagrange states that if $h \in G$, then $|h|||G|$ from which it follows that $h^{|G|} = e$. Thus for any finite group, $|G| \geq exp(G)$. In problem 2, you are first asked to show that if G is a finite Abelian group, then $exp(G) = |G|$ if and only if G is cyclic.

(If G is not Abelian, this last statement is not true: With $G = S_3$, $exp(G) = 6$ since for two-cycles x, $x^k = e$ iff k is even and for three-cycles y, $y^j = e$ if and only if $3|j$. Of course S_3 is not cyclic. There's a short discussion at the end of this on which kinds of finite groups might satisfy "$exp(G) = |G|$ iff G cyclic".)

Let A be a finite Abelian group with $|G| = p_1^{r_1} \dots p_k^{r_k}$ its prime-power factorization. In the first parts of the problem, using the Sylow Theorem (namely that for each $p_i^{r_i}$ above, there exists a subgroup of A order $p_i^{r_i}$) and a cardinality property involving set products of subgroups, everyone was able to show that

$$(*) A \cong P_1 \times \dots P_k$$

where for $i = 1, \dots, k$, P_i is a subgroup of A order $p_i^{r_i}$.

Recall that a *p-group* G is a group of order p^j, where p is a prime, $j \in \mathbb{N}$. By Lagrange, if $h \in G$, then $|h||p^j$; thus, $|h|$ is a power of p. Thus if $m = \max\{|h| : h \in G\}$, then for **all** $g \in G$, $g^m = e$. So if G is a p-group, $exp(G)$ is "realized" by some element of G, namely an element of largest order. (If G is not a p-group, this statement does not in general hold—e.g., S_3.)

Since A is isomorphic to $P_1 \times \dots P_k$, we can (and will) identify A with $P_1 \times \dots P_k$. For each $i = 1, \dots, k$, there exists an element $g_i \in P_i$ such that $exp(P_i) = |g_i|$. Consider $(g_1, \dots, g_n) = a$. Since $(|g_i|, |g_j|) = 1$, it follows that $|a| = exp(P_1) \dots exp(P_k)$, from which it follows that $exp(A) = |A|$ if and only if for $i = 1, \dots, j$, $exp(P_i) = |P_i| = p_i^{r_i}$ (if and only if P_i is cyclic, $i = 1, \dots, k$). We have shown the following.

(**) FACT: $exp(A) = |A|$ if and only if A has an element of order $|A|$ if and only if A is cyclic.

The above proves a bit more than was asked for:

(***) **FACT.** If A is a finite Abelian group, then $exp(A) = \max\{|g| : g \in G\}$.

There are non-Abelian finite groups B that satisfy $exp(B) = \max\{|g| : g \in B\}$. As showed above, if B is any p-group, it satisfies that property. For a specific example take D_8, which is a non-Abelian p-group ($p = 2$). This leads us, curious folks that we are, to ask the following:

Problem.: Characterize the set of all finite groups B that satisfy $exp(B) = \max\{|g| : g \in B\}$.

Problem 2 from HW 3 then continues, asking you to use (*) to show that if p is prime, then Z_p^* is cyclic, and show it using another FACT (****) that states that if F is a field, $s(x) \in F[x]$ has degree $n \in \mathbb{N}$, then $s(x)$ has no more than n roots, including multiplicities. (FACT(****) is on your quiz review list, something to be proven using induction.) Most everyone got the argument right: Contradiction. If Z_p^* is not cyclic, by Fact (**), $|Z_p^*| = p - 1 > exp(Z_p^*) := n$. In that case, for all $g \in Z_p{-}^*$, $g^n = 1$. But then the polynomial $x^n - 1 \in Z_p[x]$ has $p - 1$ distinct roots—but $p - 1 > n$, and so $x^n - 1$ is only allowed to have up to n roots, including multiplicities, giving rise to a contradiction. It follows that Z_p^* is cyclic.

In fact, if K is any field and F is a finite subfield of K, then the same arguments can be used to show that F^* is cyclic.

Comments on problem 4, page 306. Everyone did well on proving that the units R are ± 1, part (a). For (b), the irreducibles of degree 0 ("constant polynomials") were not hard to classify: These are $\pm p$, where p is a prime number.

What are the irreducibles of Ri having degree greater than 0? Observe that is $a(x) \in R$ is given by $a(x) = a_n x^n + \dots + a_0$, then by definition of R, $a_0 \in \mathbb{Z}$: Suppose first that $|a_0| \neq 1$. Then $a(x) = a_0(a_n/a_0 x^n + \dots + 1) =$

$a_0 b(x)$. Both a_0 and $b(x)$ are polynomials in R, but ne oa_0 is not a unit, but neither is a unit. Thus $a(x)$ is **reducible.**. Suppose next that $|a_0| = 1$. If $a(x)$ is reducible in $\mathbb{Q}[x]$, arguments used in the proof of Gauss's Lemma can be used to show that $a(x)$ reduces in R. Of course if $a(x) \in R$ is irreducible in $\mathbb{Q}[x]$, it must be irreducible in R.

For (c), you're asked to show $x \in R$ can't be written as a product of irreducible of R: Suppose $x = p_1(x) \dots p_k(x)$, where $p_i(x)$ is irreducible in R, $i = 1, \dots, k$. By a degree argument, it can be assumed without loss generality that $p_1(x)$ has degree 1, and $p_2(x), \dots, p_k(x)$ are degree 0, with $p_i(x) = p_i$, where $|p_i|$ is a prime number, for $i = 2, \dots, k$. It follows that $p_1(x) = (\frac{1}{p_1 \dots p_k})x = (2)(\frac{1}{2p_1 \dots p_k}x)$, a factorization into a product of non-units, contradicting the irreducibility of $p_1(x)$. So x can't be factored into a product of irreducibles, and R is not a UFD.