GRV II, test 1 with answers.

1. Let R be a commutative ring with identity. Write down definitions for: an irreducible element of R, a prime element of R, and give the definition of an Eisenstein polynomial $f \in R[x]$.

   ANS: Let $p \neq 0$ and not a unit. Then p irreducible means: $p = qr$ implies that q or r is a unit.
   p prime means that $p|ab$ implies $p|a$ or $p|b$ (equivalently: the ideal (p) is prime).
   $f = a_0 x^0 + \cdots + a_n x^n$ is Eisenstein if there is a prime ideal P with $a_i \in P$ for $i < n$, $a_n \notin P$ and $a_0 \notin P^2$.

2. Let R be a commutative ring with identity.

   (a) Let K be a field and let $\phi : R \to K$ be a homomorphism with $\phi(1) \neq 0$. Show that the kernel of ϕ is a prime ideal.

   ANS: If $ab \in \ker\phi$ then $\phi(ab) = \phi(a)\phi(b) = 0$, but this is in a field, so $\phi(a) = 0$ or $\phi(b) = 0$, so $a \in \ker\phi$ or $b \in \ker\phi$

   (b) Conversely, if P is a prime ideal, then show that there exists a field K and a homomorphism $\phi : R \to K$ with kernel P.

   ANS: Let K be the field of fractions of R/P and compose the natural homomorphisms $R \to R/P \to K$.

3. Let $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ where p_1, p_2, p_3 are distinct prime numbers and $e_i > 0$. Show there are 8 distinct $m \in \{0, \ldots, n-1\}$ for which $m^2 \equiv m \bmod n$.

   ANS: By the Chinese Remainder Theorem, $\mathbb{Z}/(n) \cong R_1 \times R_2 \times R_3$ where $R_i = \mathbb{Z}/(p_i^{e_1})$. Each R_i has two solutions of $m^2 = m$, taking all combinations gives $2^3 = 8$ solutions in $R_1 \times R_2 \times R_3$.

4. Suppose $f \in \mathbb{Z}[i][x]$ is reducible in the larger ring $\mathbb{Q}[i][x]$.
   Must f then also be reducible in the smaller ring $\mathbb{Z}[i][x]$?

   ANS: The ring $R := \mathbb{Z}[i]$ is a UFD, and $K := \mathbb{Q}[i]$ is its field of fractions. Then we can apply Gauss' lemma to show that reducible in $K[x]$ implies reducible in $R[x]$.

   Note: It is important that R is a UFD. For example, if $R = \mathbb{Z}[\sqrt{-7}]$ then $K = \mathbb{Q}[\sqrt{-7}]$ and $f := x^2 + x + 2$ is reducible in $K[x]$ but irreducible in $R[x]$ (to see this, compute a root of f).

5. List every (up to isomorphism) abelian group of order 128 that has a subgroup isomorphic to $C_2 \times C_2 \times C_2$ but not a subgroup isomorphic to $C_2 \times C_2 \times C_2 \times C_2$.

   C_{2^n} (with $n > 0$) has a subgroup isomorphic to C_2. So our groups look like $C_{2^{n_1}} \times C_{2^{n_2}} \times C_{2^{n_3}}$ with $n_1 \geq n_2 \geq n_3 \geq 1$ and $n_1 + n_2 + n_3 = 7$. We find four solutions $5+1+1$, $4+2+1$, $3+3+1$, $3+2+2$.

6. If p is a prime number and $p \equiv 1 \bmod 3$, then show that there exists a non-abelian group of order $3p$.

   ANS: Let C_p be the cyclic group of order p, and let $H = \mathrm{Aut}(C_p) \cong \mathbb{F}_p^*$ which has order $p-1$. If $3|p-1$, then H has an element h of order 3. Now take the semi-direct product $C_p \rtimes <h>$.

7. (Take home). Let R be a commutative ring with identity.
   Let I, J be ideals and let M be the R-module $R/I \times R/J$. Show that

$$I + J = R \iff M \text{ is a cyclic } R\text{-module.}$$

   ANS: If $I + J = R$ them $M \cong R/IJ$ by the Chinese Remainder Theorem (exercise: an R-module M is cyclic if and only if $M \cong R/I$ for some I).

   Remains to show: If $I + J \neq R$ then show that M is not cyclic.

   ANS: Let $m = (1 + I, 0 + J)$ and $n = (0 + I, 1 + J)$. If $R/I \times R/J$ is cyclic, then it has a generator $(a, b) \in R/I \times R/J$, so then $m = r(a, b)$ and $n = s(a, b)$ for some $r, s \in R$. Then $ra = 1 + I$, $rb = 0 + J$, $sa = 0 + I$, $sb = 1 + J$. Then rsb equals $r1 + J$ but also $0s + J$ and hence $r + J = 0 + J$ and so $r \in J$. Combining $ra = 1 + I$ and $r \in J$ we find $1 \in I + J$ which contradicts $I + J \neq R$.