18.702 April 5, 2008

Solutions to Practice Quiz 2

1. *(20 points) Let ϕ be the homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ defined by $\phi(x) = \frac{1}{2} + \sqrt{2}$. Prove that the kernel of ϕ is a principal ideal, and find a generator for this ideal.*

The homomorphism $\psi : \mathbb{Q}[x] \to \mathbb{R}$ that sends $x \mapsto \alpha = \frac{1}{2} + \sqrt{2}$ is a principal ideal because all ideals in $\mathbb{Q}[x]$ are principal. It is generated by the irreducible polynomial f for α over $\mathbb{Q}$, the monic polynomial of lowest degree that has α as root. If $\alpha' = \frac{1}{2} - \sqrt{2}$, then

$$f(x) = x^2 - (\alpha + \alpha')x + \alpha\alpha' = x^2 - x - textstyle\frac{3}{4}.$$

The associated primitive polynomial is $f_0 = 4x^2 - 4x + 3$. This polynomial also generates the kernel of ψ.

If $g \in \mathbb{Z}[x]$ is in the kernel of ϕ, then f_0 divides g in $\mathbb{Q}[x]$, hence f_0 divides g in $\mathbb{Z}[x]$ (a theorem from class or from the book). So f_0 generates the kernel of ϕ.

2. *(15 points) Prove that a Gauss prime π divides exactly one integer prime in the ring $\mathbb{Z}[i]$.*

The ring $\mathbb{Z}[i]$ is a unique factorization domain, so π is a prime element, and $\overline{\pi}\pi$ is an integer, say n, so π divides one of the integer prime factors of n, say p. Then $\overline{\pi}\pi$ divides $\overline{p}p = p^2$.

If π also divides an integer prime q, then $\overline{\pi}\pi = p^2$ divides $\overline{q}q = q^2$ in $\mathbb{Z}[i]$. An integer a divides another integer b in $\mathbb{Z}[i]$ if and only if a divides b in $\mathbb{Z}$. Therefore p divides q^2 and since q is prime, $p = q$.

3. *(30 points) Let $R = \mathbb{Z}[\delta]$, where $\delta = \sqrt{-10}$. For this ring, $\lfloor \mu \rfloor = 3$.*
(a) Decide whether or not the primes $p = 2$ and/or $p = 3$ remain prime in R.

An integer prime p remains prime in R if and only if $x^2 + 10$ is an irreducible polynomial in $\mathbb{F}_[x]$. So 2 does not remain prime, but 3 remains prime.

(b) If $p = 2$ or 3 does not remain prime, find generators for a prime ideal that divides the principal ideal (p) in R.

Since 2 does not remain prime, $(2) = \overline{P}P$ is a product of two prime ideals of R. Here we an guess that $P = (2, \delta)$, a fact that can be verified by computing the product ideal $\overline{P}P$.

(c) Determine the ideal class group of R.

Since $\lfloor \mu \rfloor = 3$, the class group is generated by the primes ≤ 3. We note that $P = \overline{P}$, so $[P]$ has order 2 in the class group. Since 3 remains prime, it does not contribute to the class group, which is therefore a cyclic group of order 2, generated by $[P]$.

4. *(15 points) Let $L = \mathbb{Z}^2$ be the integer lattice in the plane, and let M be the sublattice spanned by the vectors*

$$\begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}.$$

Determine the index $[L : M]$ of M in L.

Diagonalizing the matrix by integer row and column operations yields the idagonal matrix with diagonal entries $1, 7$. The index is 7.

5. *(20 points)* Describe as a direct sum of cyclic groups the abelian group A that is generated by three elements x, y, z, with the complete set of relations

$$6x + 4y + 4z = 0 \quad \text{and} \quad 2x + 2y + 8z = 0.$$

The presentation matrix is

$$\begin{pmatrix} 6 & 2 \\ 4 & 2 \\ 4 & 8 \end{pmatrix}.$$

Diagonalizing this matrix gives

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}.$$

This presents an abelian group generated by three elements u, v, w with the relations $2u = 0$ and $2v = 0$. It is a sum $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.