Lent 2014 **GROUPS, RINGS AND MODULES – EXAMPLES 3** IBL

All rings are commutative with 1 unless otherwise stated

1. Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$ are Euclidean domains, where $\omega = (1+\sqrt{-3})/2$. Show also that the usual Euclidean function $\phi(r) = N(r)$ does not make $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain. Could there be some other Euclidean function ϕ making $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain?

2. Show that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

3. Exhibit an element of $\mathbb{Z}[\sqrt{-17}]$ that is a product of two irreducibles and also a product of three irreducibles.

4. Show that if R is an integral domain then a polynomial in $R[X]$ of degree d can have at most d roots. Give a quadratic polynomial in $\mathbb{Z}_8[X]$ that has more than two roots.

5. Write down a prime ideal in $\mathbb{Z}^2$ that is not maximal. Explain why, in a finite ring, all prime ideals are maximal.

6. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:

$$\mathbb{Z}[X],\ \mathbb{Z}[X]/(X^2+1),\ \mathbb{Z}_2[X]/(X^2+1),\ \mathbb{Z}_2[X]/(X^2+X+1), \mathbb{Z}_3[X]/(X^2+X+1)$$

7. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:

$$X^4+2X+2,\ X^4+18X^2+24,\ X^3-9,\ X^3+X^2+X+1,\ X^4+1, X^4+4$$

8. Find all ways (if any) to write the following integers as sums of two squares: 221, $209\cdot 221$, $121\cdot 221$, $101\cdot 221$.

9. A complex number α is an *algebraic integer* if it is a root of a monic polynomial $f \in \mathbb{Z}[X]$. Explain why we may assume that f is irreducible. Prove carefully that $\mathbb{Z}[X]/(f)$ is isomorphic to $\mathbb{Z}[\alpha]$, the subring of $\mathbb{C}$ generated by ($\mathbb{Z}$ and) α – in other words, that quotienting the polynomials over $\mathbb{Z}$ by (f) may be viewed as 'adding a root of f to $\mathbb{Z}$'.

10. Give two elements of $\mathbb{Z}[\sqrt{-5}]$ that do not have an HCF.

11. Explain why, in a PID, the HCF of two elements a and b may always be written as a linear combination of a and b (i.e. as $xa+yb$, some x,y), and give an example in $\mathbb{Z}[X]$ of two elements whose HCF cannot be written in this way. In a Euclidean domain, what would the 'Euclidean algorithm' for calculating HCFs be? Find the HCF of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$.

12. By considering factorisations in $\mathbb{Z}[\sqrt{-2}]$, show that the equation $x^2+2=y^3$ has no solutions in integers except for $x=\pm 5,\ y=3$.

13. Exhibit an integral domain R and a (non-zero, non-unit) element of R that is not a product of irreducibles.

14. If a UFD has at least one irreducible, must it have infinitely many (pairwise non-associate) irreducibles?

$^{+}$15. Let R be a Euclidean domain in which the quotient and remainder are always unique (in other words, for any a and b with $b \neq 0$ there exist unique q and r with $a = bq+r$ and $\phi(r) < \phi(b)$ or $r=0$). Does it follow that the ring R is either a field or a polynomial ring $F[X]$ for some field F?