IB Groups, Rings, and Modules // Example Sheet 3

All rings in this course are commutative and have a multiplicative identity.

1. Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$ are Euclidean domains, where $\omega = \frac{1}{2}(1+\sqrt{-3})$. 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 the ideal $(2, 1+\sqrt{-7})$ in $\mathbb{Z}[\sqrt{-7}]$ is not principal.

3. Give 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 $(\mathbb{Z}/8\mathbb{Z})[X]$ that has more than two roots.

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

$$\mathbb{Z}[X], \quad \mathbb{Z}[X]/(X^2+1), \quad \mathbb{Z}[X]/(2, X^2+1), \quad \mathbb{Z}[X]/(2, X^2+X+1), \quad \mathbb{Z}[X]/(3, X^3-X+1).$$

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

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

7. Let R be an integral domain. The *greatest common divisor* (gcd) of non-zero elements a and b in R is an element d in R such that d divides both a and b, and if c divides both a and b then c divides d.
   (i) Show that the gcd of a and b, if it exists, is unique up to multiplication by a unit.
   (ii) In lectures we have seen that, if R is a UFD, the gcd of two elements exists. Give an example to show that this is not always the case in an integral domain.
   (iii) Show that if R is a PID, the gcd of elements a and b exists and can be written as $ra+sb$ for some $r, s \in R$. Give an example to show that this is not always the case in a UFD.
   (iv) Explain briefly how, if R is a Euclidean domain, the Euclidean algorithm can be used to find the gcd of any two non-zero elements. Use the algorithm to find the gcd of $11+7i$ and $18-i$ in $\mathbb{Z}[i]$.

8. Find all ways of writing the following integers as sums of two squares: 221, 209×221, 121×221, 5×221.

9. By working in $\mathbb{Z}[\sqrt{-2}]$, show that the only integer solutions to $x^2+2 = y^3$ are $x = \pm 5$, $y = 3$.

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

11. Let $\mathbb{F}_q$ be a finite field of q elements.
   (i) Show that the prime subfield K (that is, the smallest subfield) of $\mathbb{F}_q$ has p elements for some prime number p. Show that $\mathbb{F}_q$ is a vector space over K and deduce that $q = p^k$, for some k.
   (ii) Show that the multiplicative group of the non-zero elements of $\mathbb{F}_q$ is cyclic.
   (Hint, recall the structure theorem for finite abelian groups, and note Question 4.)

Optional Questions

12. (a) Consider the polynomial $f = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ in $\mathbb{C}[X, Y]$. Write it as an element of $(\mathbb{C}[X])[Y]$, that is collect together terms in powers of Y, and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X, Y]$.

    (b) Let F be any field. Show that the polynomial $f = X^2 + Y^2 - 1$ is irreducible in $F[X, Y]$, unless F has characteristic 2. What happens in that case?

13. Show that the subring $\mathbb{Z}[\sqrt{2}]$ of $\mathbb{R}$ is a Euclidean domain. Show that the units are $\pm(1 \pm \sqrt{2})^n$ for $n \geqslant 0$.

14. Let V be a 2-dimensional vector space over the field $\mathbb{F}_q$ of q elements, let Ω be the set of its 1-dimensional subspaces.

    (a) Show that Ω has size $q+1$ and $GL_2(\mathbb{F}_q)$ acts on it. Show that the kernel Z of this action consists of scalar matrices and the group $PGL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q)/Z$ has order $q(q^2 - 1)$. Show that the group $PSL_2(\mathbb{F}_q)$ obtained similarly from $SL_2(\mathbb{F}_q)$ has order $q(q^2 - 1)/d$ with $d = \gcd(q - 1, 2)$.

    (b) Show that Ω may be identified with the set $\mathbb{F}_q \cup \{\infty\}$ in such a way that $GL_2(\mathbb{F}_q)$ acts on Ω as the group of Möbius transformations $z \mapsto \frac{az+b}{cz+d}$. Show that in this action $PSL_2(\mathbb{F}_q)$ consists of those transformations whose determinant is a square in $\mathbb{F}_q$.

15. Show that the groups $SL_2(\mathbb{F}_4)$ and $PSL_2(\mathbb{F}_5)$ defined above both have order 60. Use this and some questions from sheet 1 to show that they are both isomorphic to the alternating group A_5. Show that $SL_2(\mathbb{F}_5)$ and $PGL_2(\mathbb{F}_5)$ both have order 120, that $SL_2(\mathbb{F}_5)$ is not isomorphic to S_5, but $PGL_2(\mathbb{F}_5)$ is.

Comments or corrections to `or257@cam.ac.uk`