Lent Term 2010 R. Camina

IB Groups, Rings and Modules: Example Sheet 3

This sheet is on the second half of the chapter on rings, dealing with factorizations. All rings here are commutative with 1. The last couple of questions, dealing with vector spaces over finite fields and linear groups, lead into the final chapter on modules.

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

3. 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.

4. Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:
$$\mathbb{Z}[X];\ \mathbb{Z}[X]/(X^2+1);\ \mathbb{Z}[X]/(2, X^2+1);\ \mathbb{Z}[X]/(2, X^2+X+1);\ \mathbb{Z}[X]/(3, X^2+1).$$

5. Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:
$$X^4+2X+2,\ X^4+18X^2+24,\ X^3-9,\ X^3+X^2+X+1,\ X^4+1,\ X^4+4.$$

6. Let R be an integral domain. The *highest common factor* 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) Give two elements of $\mathbb{Z}[\sqrt{-5}]$ that do not have a highest common factor.
(ii) Show that the highest common factor of a and b, if it exists, is unique up to multiplication by a unit.
(iii) Explain briefly why, if R is a UFD, the highest common factor of two elements always exists.
(iv) Show that if R is a PID, the highest common factor d of elements a and b exists and can be written as $d = ra + sb$ for some $r, s \in R$. [The ideals (a, b) and (d) in R are equal.]
(v) Explain briefly how, if R is a Euclidean domain, the Euclidean algorithm can be used to find the highest common factor of any two non-zero elements.
(vi) Find the highest common factor of $11 + 7i$ and $18 - i$ in $\mathbb{Z}[i]$.

7. Find all possible ways of writing the following integers as sums of two squares: $221; 209 \times 221; 121 \times 221$.

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

9. Let F be a finite field. Show that the prime subfield K (that is, the smallest subfield) of F has p elements for some prime number p. Show that F is a vector space over K and deduce that F has p^n elements for some n.

10. Let $F = \mathbb{F}_q$ be a finite field of q elements, let V be a vector space of dimension n over F.
(i) Show that V has q^n vectors. How many (ordered) bases does V have? Determine the order of the group $GL_n(\mathbb{F}_q)$ of all non-singular $n \times n$ matrices with entries in $\mathbb{F}_q$.
(ii) Show that the determinant homomorphism from $GL_n(\mathbb{F}_q)$ to $\mathbb{F}_q \setminus 0$ is surjective and hence find the order of the group $SL_n(\mathbb{F}_q)$ of all matrices in $GL_n(\mathbb{F}_q)$ of determinant 1.

Additional Questions

11. (i) Consider the polynomial $f(X,Y) = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ 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 $\mathbb{C}[X,Y]$.
(ii) Let F be any field. Show that the polynomial $f(X,Y) = X^2 + Y^2 - 1$ is irreducible in $F[X,Y]$, unless F has characteristic 2. What happens in that case?

12. 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 $n \geq 0$.

13. Show that the set $SL_2(\mathbb{Z})$ of integer 2×2 matrices of determinant 1 is a group under multiplication. Show that there is a natural homomorphism from $SL_2(\mathbb{Z})$ to $SL_2(\mathbb{F}_p)$, the group of determinant 1 matrices with entries in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Identify the kernel.

14. Let V be a 2-dimensional vector space over the field $F = \mathbb{F}_q$ of q elements, let Ω be the set of its 1-dimensional subspaces.
(i) 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 equal highest common factor of $q-1$ and 2.
(ii) Show that Ω can 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 with determinant 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 and corrections should be sent to `rdc26@dpmms.cam.ac.uk`.