Lent Term 2007 C.J.B. Brookes

IB Groups, Rings and Modules: Example Sheet 3

1. 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.

2. 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.

3. 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.

4. For each of the following rings, determine whether it is a field, a PID, a UFD, an ID:
(i) $\mathbb{Z}[X]$; (ii) $\mathbb{Z}[X]/(X^2+1)$; (iii) $\mathbb{Z}[X]/(2, X^2+1)$; (iv) $\mathbb{Z}[X]/(2, X^2+X+1)$; (v) $\mathbb{Z}[X]/(3, X^2+1)$.

5. 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) Show that the highest common factor of a and b, if it exists, is unique up to multiplication by a unit.
(ii) 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.]
(iii) 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.

6. (i) Show that $X^4 + 2X + 2$ and $X^4 + 18X^2 + 24$ are irreducible in $\mathbb{Q}[X]$.
(ii) Are $X^3 - 9$ and $X^4 - 8$ irreducible in $\mathbb{Q}[X]$?
(iii) Show that $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbb{Q}[X]$.
(iv) Are $X^3 + X^2 + X + 1$ and $X^4 + X^3 + X + 1$ irreducible in $\mathbb{Q}[X]$?
(v) Show that $X^4 + 1$ is irreducible in $\mathbb{Q}[X]$.
(vi) Show that $X^4 + 4$ factorizes in $\mathbb{Q}[X]$ into irreducible quadratic factors.

7. We see from Eisenstein's criterion that if p is prime then $X^{p-1} + \cdots + X + 1$ is irreducible in $\mathbb{Z}[X]$. Factorize $X^3 + X^2 + X + 1$ and $X^5 + X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$. Suppose $X^{n-1} + \cdots + X + 1$ is irreducible in $\mathbb{Z}[X]$. Does it follow that n is prime?

8. (i) What is the greatest common divisor in $\mathbb{Z}[i]$ of the elements $3 - 4i$ and $4 + 3i$?
(ii) What is the greatest common divisor in $\mathbb{Z}[i]$ of the elements $11 + 7i$ and $18 - i$?

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

10. (i) Show that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.
(ii) Show that $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ is a Euclidean domain (and hence a UFD).
(When $d \equiv 1 \pmod 4$, the 'ring of integers' of the field $\mathbb{Q}[\sqrt{d}]$ is $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$ and not $\mathbb{Z}[\sqrt{d}]$.)

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. Let R be a Noetherian ring. Show that the power series ring $R[[X]]$ is Noetherian.

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 cardinality $q+1$ 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 way $PSL_2(\mathbb{F}_q)$ is isomorphic to the group of Möbius transformations with $ad - bc$ 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 `brookes@dpmms.cam.ac.uk`.