Groups in action

The only noticeable change from the way the old a3 course dealt with this area is that 'the Möbius group acting on the Riemann sphere' is now mentioned specifically as an example. So I have set one question on this example, and then recommended questions from a3 papers. (I assume that you can obtain the papers from the web — let me know if there are problems.)

1. Let G denote the group of Möbius transformations of the Riemann sphere $\mathbb{C} \cup \infty$,

$$G = \left\{ z \to \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{C}, ad - bc \neq 0 \right\}$$

with multiplication in the group given by compositon of functions.

(i) Show that if $\{z_1, z_2, z_3\}$ and $\{w_1, w_2, w_3\}$ are two sets of distinct points in $\mathbb{C}\cup\infty$ then there is a unique Möbius transformation f such that $f(z_i) = w_i$ for $i = 1, 2, 3$.

[*Hint: consider first of all the special case* $w_1 = 0, w_2 = 1, w_3 = \infty$.]

Let $GL_2(\mathbb{C})$ be the group of all 2×2 invertible matrices over $\mathbb{C}$.

(ii) Show that the map $\rho : GL_2(\mathbb{C}) \to G$ defined by

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az+b}{cz+d}$$

is a surjective group homomorphism. What is the kernel of ρ?

Let $f(z) = \frac{az+b}{cz+d}$ and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

(iii) Show that $z \in \mathbb{C}$ is a fixed point of f if and only if $\begin{pmatrix} z \\ 1 \end{pmatrix}$ is an eigenvector of A. Give a similar result if ∞ is a fixed point of f.

(iv) Deduce that the Möbius transformation f has 2 distinct fixed points if and only if A is a diagonalizable matrix. Show that if this is the case then there is a complex number $\alpha \in \mathbb{C}$ and a Möbius transformation g such that $(g^{-1}fg)(z) = \alpha z$ for all $z \in \mathbb{C} \cup \infty$.

The rest of the course is covered in the questions: 2003: Q2; 2002: Q1; 2000: Q2, Q3; 1999: Q3; 1997 Q1. The last one is interesting but probably a bit harder than the others.

Introduction to fields

The lecturer has recommended the following questions: 1997: Q8; 1998: Q7, Q8; 1999: Q7, Q8; 2000: Q7; 2001: Q5; 2002: Q7, Q8; 2003: Q7.

Of these I suggest you do 2002: Q7, Q8 and 1999: Q7. (Many of the other a3 questions e.g. 2003 Q4, Q5, Q6 would provide practice on the ring theory that is now part of the core algebra.)

I've also set 2 questions below:

1. (i) Let F be a field and let $f(X)$ be a non-constant irreducible polynomial over F. Show how to construct a field K such that

(a) K is a field extension of F.

(b) $K = F(\alpha)$ for some $\alpha \in K$ such that $f(\alpha) = 0$.

(ii) Now let $g(X)$ be a non-constant polynomial over F. What is meant by a 'splitting field' for $g(X)$ over F? Show that such a splitting field always exists.

(iii) Determine the degree of the splitting field over $\mathbb{Q}$ of $X^6 - 1$.

(iv) Determine the degree of the splitting field over $\mathbb{Q}$ of $X^4 + 2$.

(iv) Let F be the field with 5 elements. Determine the degree of the splitting field over F of $X^4 + 1$.

2. (i) Let F be a finite field and let $F^\times$ denote the multiplicative group of F. By considering the polynomial $X^m - 1$ prove that there are are at most m elements in $F^\times$ of order dividing m. Show moreover that there are at most $\phi(m)$ elements in $F^\times$ of order exactly m.

(ii) Deduce that $F^\times$ is cyclic. [*You may use the identity* $\sum_{d\,|\,n} \phi(d) = n$.]

(iii) Now let p be an odd prime and let F be the finite field with p elements. Prove that -1 is a square in F if and only if $p \equiv 1 \bmod 4$.