MTH714U/MTHM024 Group Theory
Exercises 5: December 2009

Hints and solutions

1. *Let p be a prime, $p \geq 5$, and let $G = \mathrm{SL}_2(p)$. Show that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generates a Sylow p-subgroup S of G.*

   Show that for any $\lambda \in \mathbb{F}_p \setminus \{0\}$ the matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ is in $N_G(S)$.

   What is the order of $N_G(S)$, and how many Sylow p-subgroups does G have?

   We have seen in the lectures that $\mathrm{SL}_2(p)$ has order $p(p-1)(p+1)$ if p is odd, so the Sylow p-subgroups have order p. Now $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$ so by induction we get that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, so that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order p and generates a Sylow p-subgroup.

   Calculate $\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} = \begin{pmatrix} 1 & \lambda^{-2} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\lambda^{-2}}.$

   Since the order of $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ is $p-1$, the order of $N_G(S)$ is divisible by $p(p-1)$. Therefore the index is a divisor of $|G|/p(p-1) = p+1$. But S is not normal in G, so that number of Sylow subgroups is greater than 1. So by Sylow's theorem, the number of Sylow subgroups is $p+1$.

2. *Continuing the notation of the previous question, suppose that $p \equiv 1 \pmod{2^k}$, where $k \geq 2$, but $p \not\equiv 1 \pmod{2^{k+1}}$. Show that a Sylow 2-subgroup of $\mathrm{SL}_2(p)$ has order 2^{k+1} and is generated by $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, where λ is an element of order 2^k in $\mathbb{F}_p$.*

   Deduce that a Sylow 2-subgroup of $\mathrm{PSL}_2(p)$ is isomorphic to D_{2^k}.

   By assumption, $p-1$ is divisible by 2^k but not 2^{k+1}. Therefore $p+1$ is divisible by 2 but not by 4. Therefore the 2-part of the order of G is exactly 2^{k+1}.

   The matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ has order 2^k, so generates a cyclic group of that order. We calculate

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix},$$

so that $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ normalizes this cyclic group. Since its square is $-I_2$, these two matrices together generate a group of order 2^{k+1}, i.e. a Sylow 2-subgroup.

Working modulo $\{\pm I_2\}$, the first generator now becomes an element of order 2^{k-1}, and the second becomes an element of order 2. The calculation above shows that the second element conjugates the first to its inverse. Thus these elements satisfy the defining relations $a^{2^{k-1}} = b^2 = 1$ and $a^b = a^{-1}$ of D_{2^k}.

3. *(a) List the conjugacy classes in S_6 with their cycle types, class sizes, and the centralizer of an arbitrary element in the class.*

   (b) For each class, give its image under the outer automorphism of S_6 (with proof).

   (a) The conjugacy classes are in one-to-one correspondence with the cycle types, which are (1^6), $(2,1^4)$, $(2^2,1^2)$, (2^3), $(3,1^3)$, (3^2), $(3,2,1)$, $(4,1^2)$, $(4,2)$, $(5,1)$, (6). The class sizes are respectively 1, 15, 45, 15, 40, 40, 120, 90, 90, 144, 120. The centralizers are respectively S_6, $S_2 \times S_4$, $S_2 \times D_8$, $S_2 \wr S_3 \cong S_2 \times S_4$, $C_3 \times S_3$, $C_3 \times S_3$, $C_3 \times C_2 \cong C_6$, $C_4 \times C_2$, $C_4 \times C_2$, C_5 and C_6.

   (b) Each class must be mapped to another class with the same size, so the only possible swaps are $(2,1^4)$ with (2^3), and $(3,1^3)$ with (3^2), and $(3,2,1)$ with (6), and $(4,1^2)$ with $(4,2)$. This last one cannot happen, as $(4,1^2)$ is odd but $(4,2)$ is even. We saw in lectures that the first two do happen. Now an element of cycle type $(3,2,1)$ has its cube of type $(2,1^4)$, so must map to (6), whose cube is of type (2^3).

4. *(a) Prove that two elements of* $\mathrm{GL}_2(q)$ *are conjugate if (and only if) they have the same characteristic polynomial, and they have the same minimal polynomial.*

   (b) The same for $\mathrm{GL}_3(q)$.

   (c) Give an example to show that this is false for $\mathrm{GL}_4(q)$.

   (a) If the characteristic polynomial has distinct roots λ, μ, then the matrix is conjugate to a diagonal matrix with entries λ, μ. If the characteristic polynomial is irreducible $x^2 + \lambda x + \mu$, then the matrix is conjugate to $\begin{pmatrix} 0 & 1 \\ -\mu & -\lambda \end{pmatrix}$ (this is called the *companion matrix* of this polynomial, or the *rational canonical form*). If the characteristic polynomial has a repeated root, say it is $(x-\lambda)^2$, then the minimal polynomial can be either $x - \lambda$, in which case the matrix is a scalar matrix, or $(x-\lambda)^2$, in which case the matrix is conjugate to $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$.

(b) Similarly, using the rational canonical form, the conjugacy class is determined whenever there is no repeated root. If there is a repeated root, then the characteristic polynomial is either $(x-\lambda)^2(x-\mu)$ or $(x-\lambda)^3$. In the first case the argument above applies. In the second case the minimal polynomial can be either $x-\lambda$, in which case the matrix is a scalar, or $(x-\lambda)^2$, in which case the matrix is conjugate to $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$, or $(x-\lambda)^3$), in which case the matrix is conjugate to $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$.

(c) The two matrices below both have characteristic polynomial $(x-1)^4$ and minimal polynomial $(x-1)^2$.

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

5. *Calculate the conjugacy classes in* $\mathrm{GL}_2(3)$. *For each class, give a representative of the class, its characteristic polynomial and minimal polynomial, its centralizer, and the size of the class.*

Compare with the conjugacy classes in $\mathrm{PGL}_2(3) \cong S_4$. *What do you notice?*

Representative	Char. poly.	Min. poly.	Centralizer	class size
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$(x-1)^2$	$x-1$	$\mathrm{GL}_2(3)$	1
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$(x+1)^2$	$x+1$	$\mathrm{GL}_2(3)$	1
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$(x-1)^2$	$(x-1)^2$	C_6	8
$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$	$(x+1)^2$	$(x+1)^2$	C_6	8
$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$(x-1)(x+1)$	$(x-1)(x+1)$	$C_2 \times C_2$	12
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	x^2+1	x^2+1	C_8	6
$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$	x^2+x-1	x^2+x-1	C_8	6
$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	x^2-x-1	x^2-x-1	C_8	6

The first two classes correspond to cycle type (1^4) in S_4, and the next two to cycle type $(3,1)$. The next two are $(2,1^2)$ and (2^2) respectively, and the last two are both (4).

6. *(Hard) Compute the conjugacy classes in* $\mathrm{PGL}_2(9)$.

   Compare with the conjugacy classes in $\mathrm{PSL}_2(9) \cong A_6$. *State (and prove, if you can) a criterion for when a conjugacy class in* $\mathrm{PGL}_2(9)$ *(or more generally,* $\mathrm{PGL}_2(q)$*) splits into two classes in* $\mathrm{PSL}_2(9)$ *(or* $\mathrm{PSL}_2(q)$*).*

   Modulo scalars, the diagonal matrices $\mathrm{diag}(\lambda,\mu)$ fall into 5 conjugacy classes, with $\lambda/\mu = 1, -1, \pm i, \pm 1 + i, \pm 1 - i$ respectively (because $\mathrm{diag}(\lambda,\mu)$ is conjugate to $\mathrm{diag}(\mu,\lambda)$).

   The matrices with minimal polynomial $(x-\lambda)^2$ are scalar multiples of conjugates of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

   This leaves the matrices with irreducible characteristic polynomial. Multiplying x by a suitable scalar, we can assume the characteristic polynomial is either $x^2 + 1 + i$, or $x^2 - x + \lambda$, and this is irreducible iff $1 - \lambda$ is not a square, i.e. $1 - \lambda = \pm 1 \pm i$, so $\lambda = \pm i$ or $-1 \pm i$. Thus we have five such classes.

   Altogether this gives $5 + 1 + 5 = 11$ classes. Of these, six lie in $\mathrm{PSL}_2(9)$. These are the classes represented (modulo scalars) by the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 1+i & 0 \\ 0 & -1+i \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1+i \\ 1-i & 1+i \end{pmatrix}, \begin{pmatrix} 0 & 1-i \\ 1+i & 1-i \end{pmatrix}.$$

   In fact the only one of these classes which splits into two in $\mathrm{PSL}_2(9)$ is the fourth one: we looked at this case in lectures, where we saw that the additive group of the field is normalized by only half the multiplicative group in $\mathrm{PSL}_2(q)$. Thus $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1+i \\ 0 & 1 \end{pmatrix}$ are not conjugate in $\mathrm{PSL}_2(9)$.

   You might conjecture that this holds in general: the only class which splits is the class of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. You could look at a few other values of q to see (a) whether you believe this, and/or (b) whether you can prove it.