UNIVERSITY OF PENNSYLVANIA DEPARTMENT OF MATHEMATICS
Math 370 Algebra Fall Semester 2006
Prof. Gerstenhaber, T.A. Asher Auel

Homework #5 Solutions (due 10/10/06)
Chapter 2 Groups (supplementary exercises)

Subgroups of S_4 It's a general fact about symmetric groups, and in the case of S_4 a fact that I've already told you, that the conjugacy classes are given by the "shapes" of the disjoint cycle decomposition of the elements. In the case of S_4 the conjugacy classes are as follows:

e	$(\cdot\cdot)$	$(\cdot\cdot)(\cdot\cdot)$	$(\cdot\cdot\cdot)$	$(\cdot\cdot\cdot\cdot)$
e	(12)	$(12)(34)$	(123)	(1234)
	(13)	$(13)(24)$	(132)	(1342)
	(14)	$(14)(23)$	(124)	(1423)
	(23)		(142)	(1243)
	(24)		(134)	(1432)
	(34)		(143)	(1324)
			(234)	
			(243)	

The subgroups of S_4 are the following:

n	subgroups of S_4 of order n	$\cong$ type	#
1	$\{e\}$	C_1	1
2	$\{e,(12)\}$, $\{e,(13)\}$, $\{e,(14)\}$, $\{e,(23)\}$, $\{e,(24)\}$, $\{e,(34)\}$	C_2	6
	$\{e,(12)(34)\}$, $\{e,(13)(24)\}$, $\{e,(14)(23)\}$	C_2	3
3	$\{e,(123),(132)\}$, $\{e,(124),(142)\}$, $\{e,(134),(143)\}$, $\{e,(234),(243)\}$	C_3	4
4	$\{e,(12),(34),(12)(34)\}$, $\{e,(13),(24),(13)(24)\}$, $\{e,(14),(23),(14)(23)\}$	$C_2\times C_2$	3
	$\{e,(12)(34),(13)(24),(14)(23)\}$	$C_2\times C_2$	1
	$\{e,(1324),(12)(34),(1423)\}$, $\{e,(1234),(13)(24),(1432)\}$, $\{e,(1243),(14)(23),(1342)\}$	C_4	3
6	$\{e,(123),(132),(12),(13),(23)\}$, $\{e,(124),(142),(12),(14),(24)\}$, $\{e,(134),(143),(13),(14),(34)\}$, $\{e,(234),(243),(23),(24),(34)\}$	S_3	4
8	$\{e,(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\}$, $\{e,(13),(24),(13)(24),(12)(34),(14)(23),(1234),(1432)\}$, $\{e,(14),(23),(14)(23),(12)(34),(13)(24),(1243),(1342)\}$	D_4	3
12	$\{e,(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),$ $(234),(243)\}$	A_4	1
24	S_4	S_4	1

Each row of the table contains a conjugacy class of subgroups. The last column lists the number of subgroups in that conjugacy class. The second to the last column lists the isomorphism type, where C_k denotes the cyclic group of order k.

In all we see that there are 30 different subgroups of S_4 divided into 11 conjugacy classes and 9 isomorphism types.

As discussed, normal subgroups are unions of conjugacy classes of elements, so we could pick them out by staring at the list of conjugacy classes of elements. Also, by definition, a normal subgroup is equal to all its conjugate subgroups, i.e. it only has one element in its conjugacy class. Thus the four normal subgroups of S_4 are the ones in their own conjugacy class, i.e. rows 1, 6, 10, and 11.

Here are some general guidelines for determining which subgroups are conjugate. First a quick

Definition: Let G be a group and $S \subset G$ a subset of G (not necessarily a subgroup).

- As usual, for $g \in G$, we write

$$\begin{aligned} gSg^{-1} &= \{gsg \in G : s \in S\} \\ &= \{s' \in G : s' = gsg^{-1} \text{ for some } s \in S\} \end{aligned}$$

  for the conjugation of the subset S by $g \in G$. When the set $S = H \subset G$ is a subgroup, we defined a *conjugate subgroup of H in G* to be any subgroup of the form gHg^{-1} for $g \in G$. Note that in particular, for $S =< h >$ the cyclic subgroup generated by $h \in G$ we have

$$g < h > g^{-1} =< ghg^{-1} >,$$

  which is a consequence of Chapter 2 exercise 3.4a.
- Define the *normalizer of S in G* as

$$\begin{aligned} N_G(S) &= \{g \in G : gSg^{-1} = S\} \\ &= \{g \in G : gsg^{-1} \in S \text{ for all } s \in S\}. \end{aligned}$$

- When the set S consists of a single element $S = \{h\}$ then the normalizer of $\{h\}$ in G is also called the *centralizer of h in G*

$$C_G(h) = C(h) = \{g \in G : ghg^{-1} = h\},$$

  i.e. the set of elements of G that commute with h.

The idea is now that normalizers behave nicely under conjugation.

Lemma: Let G be a group and $S \subset G$ be a subset.

i) $N_G(S) \subset G$ is a subgroup,

ii) for every $g \in G$ we have that

$$gN_G(S)g^{-1} = N_G(gSg^{-1}),$$

in particular for centralizers, we get $g\,C(h)g^{-1} = C(ghg^{-1})$.

Proof. To *i)*, for $g, g' \in N_G(S)$ we have

$$(gg')N(gg')^{-1} = g(g'Sg'^{-1})g^{-1} = gSg^{-1} = S \quad \text{and} \quad gSg^{-1} = S \;\Rightarrow\; S = g^{-1}Sg,$$

so that $N_G(S)$ is closed under multiplication and has inverses. Of course $e \in N_G(S)$. So $N_G(S) \subset G$ is a subgroup.

To *ii)*, let $g' \in N_G(S)$ and let $g \in G$, then note that

$$(gg'g^{-1})(gSg^{-1})(gg'g^{-1})^{-1} = g(g'Sg'^{-1})g^{-1} = gSg^{-1},$$

so that $gg'g^{-1} \in N_G(gSg^{-1})$. Thus $gN_G(S)g^{-1} \subset N_G(gSg^{-1})$. For the other containment, let $h \in N_G(gSg^{-1})$. We want to show that $h = gg'g^{-1}$ for some $g' \in N_G(S)$, i.e. that $g' := g^{-1}hg \in N_G(S)$. To that end, note that

$$g'Sg'^{-1} = (g^{-1}hg)S(g^{-1}hg)^{-1} = g^{-1}(h(gSg^{-1})h^{-1})g = g^{-1}(gSg^{-1})g = S,$$

using in the third equality, the fact that $h \in N_G(gSg^{-1})$. So we see that indeed $g' = g^{-1}hg \in N_G(S)$. So we have $N_G(gSg^{-1}) \subset gN_G(S)g^{-1}$. Combining the two inclusions gives our claim. □

An immediate corollary of this is the following mantra of normalizers and conjugacy classes: let $\mathscr{C}$ be a conjugacy class of elements (or subgroups) of a group G, then

the set of normalizers of the members of $\mathscr{C}$, $N_G(\mathscr{C}) = \{N_G(S) : S \in \mathscr{C}\}$, again forms a conjugacy class of subgroups.

Yet another way of expressing this is that N_G may be regarded as a function on the set of conjugacy classes of subgroups.

Now we note that almost all of our subgroups can be identified as either cyclic subgroups or as certain normalizers (or centralizers). Cyclic subgroups are easily divided into conjugacy classes in view of the remark after the first part of the above definition, i.e. the conjugate of a cyclic subgroup is the cyclic subgroup generated by the conjugate element. For non-cyclic subgroups, it's harder to locate an element that will simultaneously conjugate one entire subgroup into another. That's why we appeal to normalizers and centralizers. For example, the subgroups in the fifth row of the table can be identified with centralizers two-cycles:

$$C((12)) = C((34)) = \{e, (12), (34), (12)(34)\},$$

$$C((13)) = C((24)) = \{e, (13), (24), (13)(24)\},$$

$$C((14)) = C((23)) = \{e, (14), (23), (14)(23)\},$$

and so since we know that the two cycles for a conjugacy class, we also know that their centralizers form a conjugacy class of subgroups.

Similarly, the subgroups in the eighth row of the table can be identified with the normalizers of cyclic subgroups generated by three-cycles:

$$N_{S_4}(< (123) >) = \{e, (123), (132), (12), (13), (23)\},$$

$$N_{S_4}(< (124) >) = \{e, (124), (142), (12), (14), (24)\},$$

$$N_{S_4}(< (134) >) = \{e, (134), (143), (13), (14), (34)\},$$

$$N_{S_4}(< (234) >) = \{e, (234), (243), (23), (24), (34)\},$$

and so since the three-cycles (hence their cyclic subgroups) form a conjugacy class, so do their normalizers. Another way to view these subgroups is as the stabilizers of a given number, e.g.

$$\{e, (123), (132), (12), (13), (23)\} = \{g \in S_4 : g : 4 \to 4\},$$

and it's an easy exercise to show that such stabilizing subgroups are conjugate.

Finally, the subgroups in the ninth row of the table can be identified with centralizers of disjoint products of two cycles:

$$C((12)(34)) = \{e, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\},$$

$$C((13)(24)) = \{e, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\},$$

$$C((14)(23)) = \{e, (14), (23), (14)(23), (12)(34), (13)(24), (1243), (1342)\},$$

and again we see that these form a conjugacy class of elements hence of centralizers.

Another way of encapsulating this is as follows. Let the set of subgroups in the r^{th} row of the table be denoted $\mathscr{C}_r$. Let $\mathscr{C} = \{\mathscr{C}_1, \ldots, \mathscr{C}_{11}\}$ be the set of conjugacy classes of S_4. Then as a function $N_G : \mathscr{C} \to \mathscr{C}$ one can verify that

$$\begin{array}{cccccccccccc}
\mathscr{C}_1 & \mapsto & \mathscr{C}_1 & \mathscr{C}_2 & \mapsto & \mathscr{C}_5 & \mathscr{C}_3 & \mapsto & \mathscr{C}_9 & \mathscr{C}_4 & \mapsto & \mathscr{C}_8 \\
\mathscr{C}_5 & \mapsto & \mathscr{C}_9 & \mathscr{C}_6 & \mapsto & \mathscr{C}_6 & \mathscr{C}_7 & \mapsto & \mathscr{C}_9 & \mathscr{C}_8 & \mapsto & \mathscr{C}_{11} \\
\mathscr{C}_9 & \mapsto & \mathscr{C}_{11} & \mathscr{C}_{10} & \mapsto & \mathscr{C}_{10} & \mathscr{C}_{11} & \mapsto & \mathscr{C}_{11}. & & &
\end{array}$$

The general philosophy is that humans like permutations groups. To understand subgroups of a group, you want to think of them as the permutations of something. For subgroups $H, K \subset G$, making the identification $H = N_G(K)$, really says that under the action of H on G via conjugation (i.e. inner automorphisms), H permutes the elements of K.

Claim: For positive integers n and m we have

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z} \quad \Leftrightarrow \quad \gcd(n,m) = 1.$$

Proof. First off, we make the following observation. Let $a \in \mathbb{Z}/n\mathbb{Z}$, and consider the element $(a,0) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Then

$$\#a = \#(a,0),$$

where the order on the left is taken in $\mathbb{Z}/n\mathbb{Z}$ and on the right taken in $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Now, for the "$\Leftarrow$" direction, we first prove that in general

$$\#(1,1) = \operatorname{lcm}(n,m).$$

To that end, first note that by Chapter 2, exercise 2.20a, we have that

$$\#(1,1) = \#(1,0) + (0,1) \,|\, \operatorname{lcm}(\#(1,0), \#(0,1)) = \operatorname{lcm}(n,m).$$

Conversely, for positive integers $r > 0$, we have

$$r(1,1) = (r,r) = (0,0) \quad \Rightarrow \quad n \,|\, r \text{ and } m \,|\, r \quad \Rightarrow \quad \operatorname{lcm}(n,m) \,|\, r,$$

where the last implication follows from the general properties of lcm listed in solution set 4. In particular, taking $r = \#(1,1)$ we see that $\operatorname{lcm}(n,m) \,|\, \#(1,1)$. Together we have finally that $\#(1,1) = \operatorname{lcm}(n,m)$.

Now assuming that $\gcd(n,m) = 1$, we have that $\operatorname{lcm}(n,m) = nm$, and so $\#(1,1) = nm$. But also, we know that the order of a product of finite groups is the product of the orders, i.e.

$$|\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}| \cdot |\mathbb{Z}/m\mathbb{Z}| = nm.$$

So we see that in fact $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is cyclic of order nm with generator $(1,1)$, so is incidentally isomorphic to $\mathbb{Z}/nm\mathbb{Z}$.

Now for the "$\Rightarrow$" direction, we prove the converse statement

$$\gcd(n,m) > 1 \quad \Rightarrow \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \ncong \mathbb{Z}/nm\mathbb{Z}.$$

For $a \in \mathbb{Z}/n\mathbb{Z}$ and $b \in \mathbb{Z}/m\mathbb{Z}$ with $\#a = r$ and $\#b = s$, we consider $(a,b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and as before, we have that

$$\#(a,b) = \#(a,0) + (0,b) | \operatorname{lcm}(\#(a,0), \#(0,b)) = \operatorname{lcm}(r,s) = \frac{rs}{\gcd(r,s)}.$$

We want to show that $\#(a,b) < nm$, which will show that every element has order less than the order of the group, i.e. the group is not cyclic. To that end, note first that for either $r < n$ or $s < m$,

$$\#(a,b) \,|\, \frac{rs}{\gcd(r,s)} \leq rs < nm,$$

so we are left with the case $r = n$ and $s = m$. But now by hypothesis, $\gcd(n,m) > 1$, so we have

$$\#(a,b) \,|\, \frac{nm}{\gcd(n,m)} < nm.$$

So in all cases, $\#(a,b) < nm$ for all $(a,b) \in \mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$, i.e. $\mathbb{Z}/n \times \mathbb{Z}/m\mathbb{Z}$ cannot be cyclic, so in particular, is not isomorphic to $\mathbb{Z}/nm\mathbb{Z}$. $\square$

2.1 Claim: The set $\mathbb{Q}(\sqrt{2})$ of real numbers of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$ forms a subfield of the real numbers.

Proof. First note that for $a, b, a', b' \in \mathbb{Q}$, we have

$$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$$

and

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2},$$

so $\mathbb{Q}(\sqrt{2})$ is closed under addition and multiplication since $\mathbb{Q}$ is.

Second, note that since $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$, which we know is a field, associativity and commutativity for $+$ and $\cdot$ and distributivity hold. Also, note that $0 = 0 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and that $-(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$. So $\mathbb{Q}(\sqrt{2})$ is an abelian subgroup of $\mathbb{R}$ under $+$.

Finally, note that for $a, b\mathbb{Q}$ both nonzero, $a^2 - 2b^2 \in \mathbb{Q}$ is again nonzero since $2 \in \mathbb{Q}$ is not a square, and in this case

$$\frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

is a multiplicative inverse of $a + b\sqrt{2} \neq 0$. Thus $\mathbb{Q}(\sqrt{2})$ is a field. □

2.7 Definition: Let R, R' be rings with 1, then a map $\varphi : R \to R'$ is a *ring homomorphism* if

$$\begin{aligned} \varphi(x + y) &= \varphi(x) + \varphi(y) \\ \varphi(xy) &= \varphi(x)\varphi(y) \\ \varphi(1_R) &= 1_{R'} \end{aligned}$$

for all $x, y \in R$.

Claim: Let F be a field and R any ring with 1, then any ring homomorphism $\varphi : F \to R$ is injective.

Proof. Since, in particular, $\varphi : F \to R$ is a homomorphism of abelian groups under addition, φ is injective if and only if $\ker \varphi = \{0_F\}$. To that end, we'll argue by contradiction. Suppose $a \in \ker \varphi$ and $a \neq 0_F$. Since F is a field, $a \in F$ has a multiplicative inverse $a^{-1} \in F$ and then

$$1_{R'} = \varphi(1_F) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = 0_{R'} \cdot \varphi(a^{-1}) = 0_{R'},$$

which is a contradiction since $0_{R'} \neq 1_{R'}$ for any ring with 1 by definition. So only $a = 0$ is possible, i.e. $\ker \varphi = \{0_F\}$, and φ is injective. □

2.8 We have the following table:

	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/11\mathbb{Z}$	$\mathbb{Z}/13\mathbb{Z}$
5	1	2	5	5	5
-5	1	1	2	6	8
5^{-1}	1	2	3	9	8

2.10 Consider the system of linear equations $\begin{pmatrix} 8 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$ over $\mathbb{F}_p$ for various primes p. First note that $\det \begin{pmatrix} 8 & 3 \\ 2 & 6 \end{pmatrix} = 42 = 2 \cdot 3 \cdot 7$.

a) For primes $p \neq 2, 3, 7$, this determinant is nonzero (hence invertible), so the matrix is invertible, $\begin{pmatrix} 8 & 3 \\ 2 & 6 \end{pmatrix}^{-1} = \frac{1}{42}\begin{pmatrix} 6 & -3 \\ -2 & 8 \end{pmatrix}$, and our system has the unique solution

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{1}{42}\begin{pmatrix} 6 & -3 \\ -2 & 8 \end{pmatrix}\begin{pmatrix} 3 \\ -1 \end{pmatrix} = \frac{1}{42}\begin{pmatrix} 21 \\ -14 \end{pmatrix} = \frac{1}{6}\begin{pmatrix} 3 \\ -2 \end{pmatrix} = \begin{pmatrix} 2^{-1} \\ -3^{-1} \end{pmatrix}.$$

So we have the table:

p	2^{-1}	3^{-1}	-3^{-1}	solution
5	3	2	3	$\begin{pmatrix} 3 \\ 3 \end{pmatrix}$
11	6	4	7	$\begin{pmatrix} 6 \\ 7 \end{pmatrix}$
17	9	6	11	$\begin{pmatrix} 9 \\ 11 \end{pmatrix}$

b) For $p = 7$ the matrix is no longer invertible, i.e. the two linear equations are now dependent, so one is a scalar multiple of the other. In fact, we see that $4 \cdot (2, 6) = (8, 3)$. So now we have one equation in two variables so we expect more solutions. Lets find them. The second row of the matrix gives the linear equation

$$2x_1 + 6x_2 = -1 = 6,$$

and dividing through by 2 gives

$$x_1 + 3x_2 = 3.$$

Thus for each choice of $x_2 \in \mathbb{F}_7$, we see that $x_1 = 3 - 3x_2$ is determined. So there are seven possible solutions. They are

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 5 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 6 \end{pmatrix}.$$

2.11 Note that the determinant of the matrix

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{pmatrix}$$

is $10 = 2 \cdot 5$. Now $A \in M_{3\times 3}(\mathbb{F}_p)$ is invertible if and only if $\det A \in \mathbb{F}_p$ is nonzero, i.e. $p \not| \det A$. This is only the case for all primes $p \neq 2, 5$.