Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 1

1. Draw a square with vertices $(\pm 1, 0), (0, \pm 1)$, and number the vertices counterclockwise starting at $(1, 0)$ by $4, 1, 2, 3$.

   (a) Write each element of D_4 in cycle notation, thus identifying D_4 as a subgroup of S_4.

   Solution.

   $$\begin{aligned} r &= \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} & r^2 &= \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} \\ r^3 &= \begin{pmatrix} 1 & 4 & 3 & 2 \end{pmatrix} & s &= \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \\ rs &= \begin{pmatrix} 1 & 3 \end{pmatrix} & r^2 s &= \begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix} \\ r^3 s &= \begin{pmatrix} 2 & 4 \end{pmatrix} & e &= \begin{pmatrix} 1 \end{pmatrix} \end{aligned}$$

   . □

   (b) We can think of elements of S_4 as matrices active on $\mathbb{R}^4$, using the rule $\sigma(e_i) := e_{\sigma(i)}$. Write the permutation matrix for each element of D_4.

   Solution.

   $$r = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad r^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

   $$r^3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad e = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

   $$s = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad rs = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

   $$r^2 s = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad r^3 s = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

   □

   (c) Show using cycle notation and then matrix multiplication that $sr = r^{-1}s$.

Homework 1

Solution. $sr = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} = \begin{pmatrix}2 & 4\end{pmatrix}$, $r^3 = r^{-1}$ so that $r^{-1}s = r^3 s = \begin{pmatrix}2 & 4\end{pmatrix}$.
For matrix multiplication:

$$\begin{aligned} sr &= \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix} \\ &= \begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix} \\ &= r^3 s \end{aligned}$$

Then to show $r^{-1} = r^3$ we'll show that $rr^3 = e$ in matrix form:

$$\begin{bmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}.$$

Hence $sr = r^{-1}s$ as required. □

2. Let X be the regular non-oriented tetrahedron, and let X' be the regular oriented tetrahedron.

   (a) Show that S_X is a subgroup of S_4.

   Solution. Give the regular non-oriented tetrahedron the labeling from $\{1, 2, 3, 4\}$ for the vertices, as seen in Figure (4). Then orientation need not be preserved, so that actions on X are any re-labeling of the vertices. Actions on X are then any re-labeling of the vertices of X. That is, allowing $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}$ to act on X yields Figure (2). So clearly, S_X is a non-empty subset of S_4.
   Now to show that S_X is a subgroup of S_4. Appealing to the fact that any permutation is a product of 2−cycles, suppose we have a 2−cycle in S_X, $\sigma = \begin{pmatrix}i & j\end{pmatrix}$ in cycle notation. Then we have that $\sigma^{-1} = \begin{pmatrix}j & i\end{pmatrix}$ is the act of un-doing the relabeling. Hence any 2−cycle in S_X has an inverse, so any permutation in S_X has an inverse.
   Identity is the action of not relabeling.
   Closure is obtained via noting that labeling are only obtained from $\{1, 2, 3, 4\}$. □

Homework 1

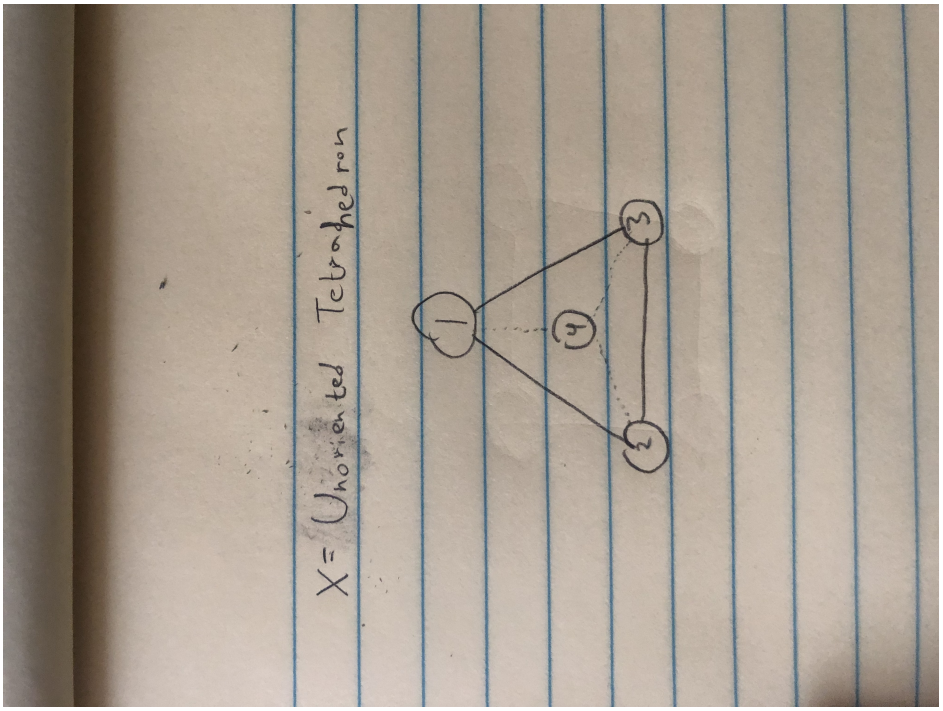


Figure 1: Labeling of a Regular Unoriented Tetrahedron

Homework 1

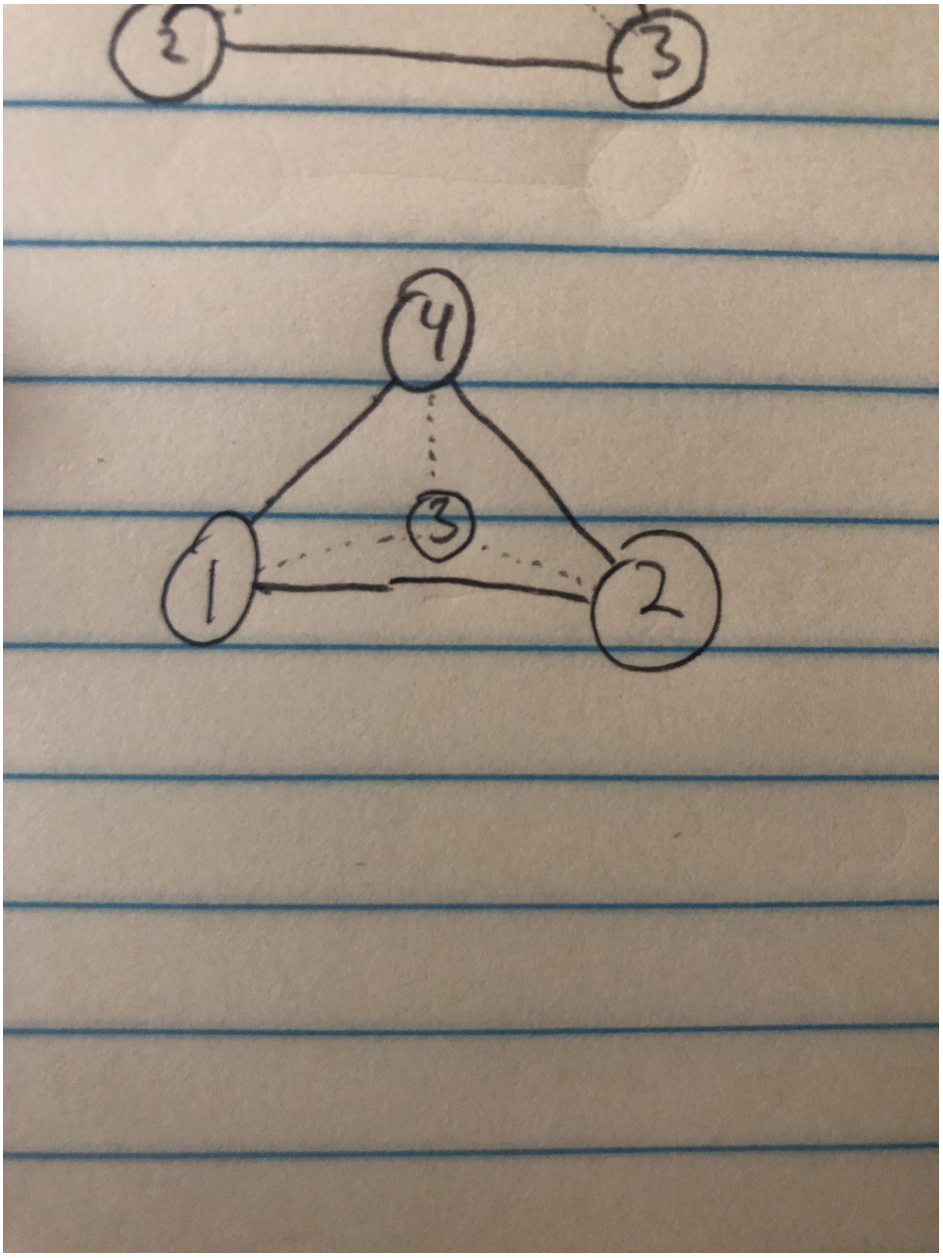


Figure 2: A relabeling of X

Homework 1

(b) Show that S_X equals S_4.

Solution. See Figure 3 □

(c) Determine the subgroup $S_{X'} \leq S_4$ by explicitly writing down all of its elements.

Solution. The first elements of $S_{X'}$ can be obtained by leaving one vertex fixed and rotating the opposite face this gives us the following:

$$\begin{pmatrix}3 & 4 & 2\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}2 & 4 & 3\end{pmatrix}$$
$$\begin{pmatrix}1 & 3 & 4\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1 & 4 & 3\end{pmatrix}$$
$$\begin{pmatrix}1 & 2 & 4\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1 & 4 & 2\end{pmatrix}$$
$$\begin{pmatrix}1 & 2 & 3\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1 & 3 & 2\end{pmatrix}$$

The identity can be obtained by doing nothing, (1). Then reflections and rotations give us:

$$\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$$
$$\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}.$$

This is exactly $A_4 \leq S_4$. □

3. (The Secrete Conjugation Trick in S_n) Let G be a group. The *conjugate* of an element $a \in G$ by an element $b \in G$ is the element $bab^{-1} \in G$. The elements a and bab^{-1} are closely related as symmetries, as will see in the problem.

(a) Suppose $\sigma, \tau \in S_n$. Show that if $\tau(i) = j$, then $(\sigma\tau\sigma^{-1})(\sigma(i)) = \sigma(j)$.

Proof. Let $\sigma, \tau \in S_n$ and suppose $\tau(i) = j$. So that $(\tau\sigma^{-1}\sigma)(i) = j \iff \sigma(\tau\sigma^{-1}(\sigma(i))) = \sigma(j) \iff (\sigma\tau\sigma^{-1})(\sigma(i)) = \sigma(j)$, as desired. □

(b) Use (3a) to show that the disjoint cycle expression of $\sigma\tau\sigma^{-1}$ is obtained from that of τ by substituting $\sigma(i)$ for i in the expression for τ. This is the *conjugation trick*.

Proof. Let $\sigma, \tau \in S_n$. Suppose $\tau(i) = j$ with $i, j \in \{1, 2, 3, \ldots, n\}$. Then by (3$a$) we have that $(\sigma\tau\sigma^{-1})(\sigma(i)) = \sigma(j) \iff (\sigma\tau\sigma^{-1}\sigma\tau^{-1})(j) = \sigma(j)$. Hence the $\tau^{-1}(j)$ entry of $\sigma\tau\sigma^{-1}$ is given by $\tau^{-1}(j)$ replaced by $\sigma(j)$; that is j in τ replaced by $\sigma(j)$. □

(c) Use conjugation trick to quickly compute $\sigma\tau\sigma^{-1}$, where $\tau = \begin{pmatrix}1 & 3 & 4 & 6\end{pmatrix}\begin{pmatrix}2 & 5\end{pmatrix}$ and $\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\end{pmatrix}$.

Homework 1

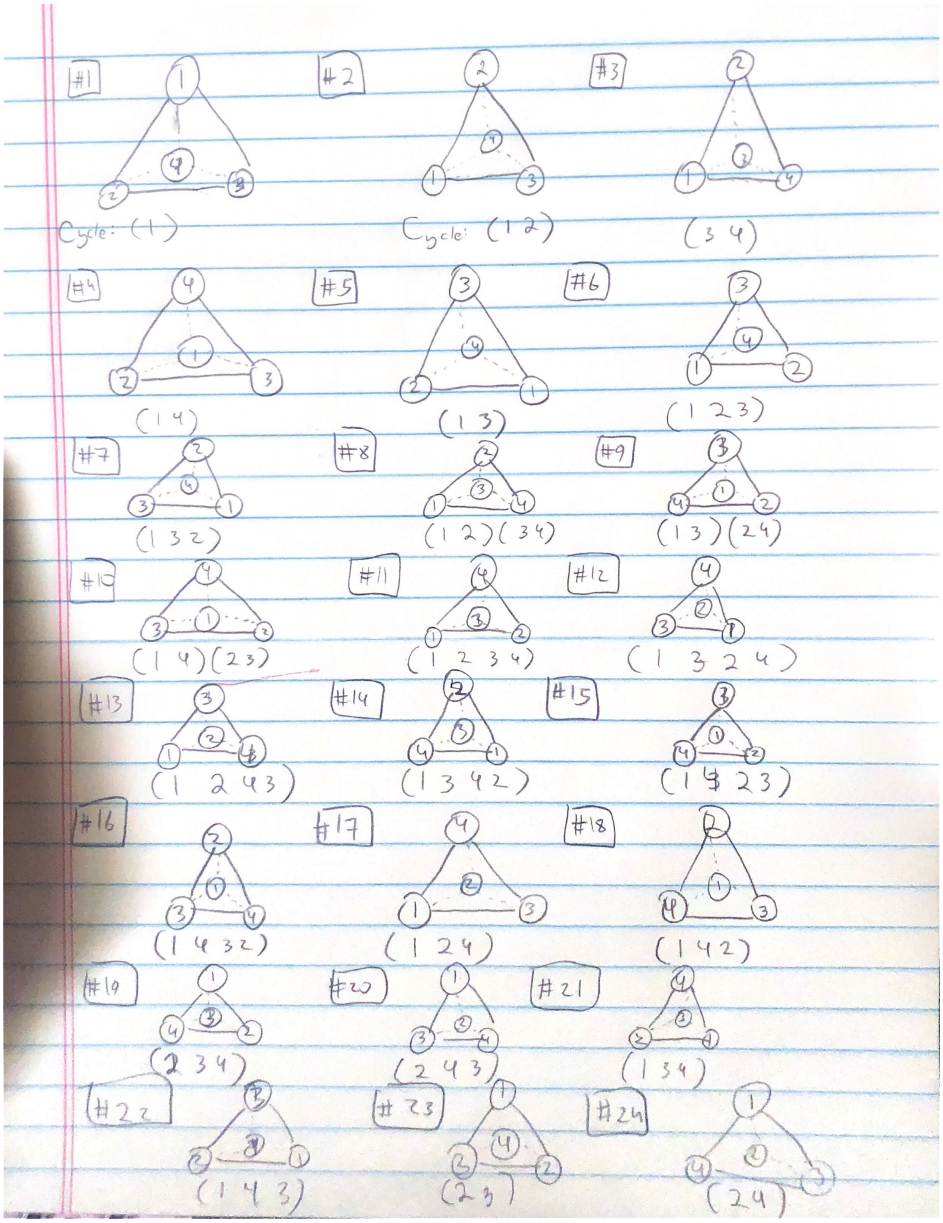


Figure 3: The complete table of elements of X. Note that their cycle notation, gives us the result.

Homework 1

Solution. Using the trick, $\sigma\tau\sigma^{-1} = \begin{pmatrix}\sigma(1) & \sigma(3) & \sigma(4) & \sigma(6)\end{pmatrix}\begin{pmatrix}\sigma(2) & \sigma(5)\end{pmatrix} = \begin{pmatrix}2 & 4 & 5 & 1\end{pmatrix}\begin{pmatrix}3 & 6\end{pmatrix}$ □

(d) If σ and ρ are elements of S_n with the same cycle type, then there exists an element $\tau \in S_n$ such that $\rho = \tau\sigma\tau^{-1}$. Prove this when $n = 4$. [*Same cycle type implies conjugation.*]

Solution. □

4. Let $H \leq G$ be a subgroup, and let $N_G(H) = \{s \in G : sHs^{-1} = H\}$ be the normalizer of H in G. We know that H is normal in $N_G(H)$.

(a) Show that if H is normal in a subgroup $K \leq G$, then $K \leq N_G(H)$.

Proof. Let G be a group, $H \leq G$, and $K \leq G$. Suppose H is normal in K; that is, for all $k \in K$ we have $H = kHk^{-1}$.

Since $K \leq G$ we have that K is non-empty. To show that $K \subseteq N_G(H)$, let $k \in K$. So since H is normal in K, we have that $H = kHk^{-1}$. Hence $k \in N_G(H)$ and so $K \subseteq N_G(H)$.

To show $K \leq N_G(H)$, we'll use the "one-step subgroup test"; that is, for a non-empty subset K of a group G, if $a, b \in K$, then $ab^{-1} \in K$, if and only if, $K \leq G$. So let $a, b \in K$. Then $aH = Ha$ and $bH = Hb$ since H is normal in K. So re-writing that, we have:

$$\begin{aligned} & H = b^{-1}Hb = a^{-1}Ha \\ \iff & H = ab^{-1}Hba^{-1} \\ \iff & H = ab^{-1}H(ab^{-1})^{-1}. \end{aligned}$$

That is $ab^{-1} \in N_G(H)$, as required by the one-step subgroup test. Hence $K \leq N_G(H)$. □

(b) Suppose H is conjugate to H' in G. Determine the relationship between $N_G(H)$ and $N_G(H')$.

Claim: If H is conjugate to H' in G, then $N_G(H)$ is conjugate to $N_G(H')$ in G; that is, there exists a $g \in G$, $N_G(H) = gN_G(H')g^{-1}$.

Proof. Let H be conjugate to H' in G. That is, there exists a $k \in G$ such that $H = kH'k^{-1}$. Now we'll show there exists a $g \in G$ such that $N_G(H) = gN_G(H')g^{-1}$ via set inclusion.

Let $y \in N_G(H)$. Then

$$H = yHy^{-1}. \tag{1}$$

Then by our hypothesis, $H = kH'k^{-1}$. So substituting that into 1 :

$$\begin{aligned} kH'k^{-1} &= y(kH'k^{-1})y^{-1} \\ H' &= (k^{-1}yk)H'(k^{-1}yk)^{-1}. \end{aligned}$$

This gives us $k^{-1}yk \in N_G(H')$, or $y \in kN_G(H')k^{-1}$. So that $N_G(H) \subseteq kN_G(H')k^{-1}$. Conversely, let $y \in kN_G(H')k^{-1}$. Then equivalently $k^{-1}yk \in N_G(H')$ so that $(k^{-1}yk)H'(k^{-1}yk)^{-1} = H'$. Since $H' = k^{-1}Hk$ we have:

$$(k^{-1}ykk^{-1})H(kk^{-1}y^{-1}k) = k^{-1}Hk \iff k^{-1}yH(k^{-1}y)^{-1} = k^{-1}Hk \iff yHy^{-1} = H.$$

Giving us $y \in N_G(H)$.
So that $N_G(H) = kN_G(H')k^{-1}$ as desired. □

5. Prove that the pairing $G \times G \to G$ given by $(s, x) \mapsto xs$ is not an action on G. Show the pairing $(s, x) \mapsto xs^{-1}$ is an action on G.

Counter-Example. Let $a \cdot b$ denote ba. Let $G = S_3$, $x = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, s = \begin{pmatrix} 1 & 2 \end{pmatrix}, h = \begin{pmatrix} 1 & 3 \end{pmatrix}$. Note that

$$xh = \begin{pmatrix} 2 & 3 \end{pmatrix} \qquad sxh = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

and

$$hx = \begin{pmatrix} 1 & 2 \end{pmatrix} \qquad shx = \begin{pmatrix} 1 \end{pmatrix}.$$

That is $x \cdot (h \cdot s) = x \cdot (sh) = shx = \begin{pmatrix} 1 \end{pmatrix}$ and $(xh) \cdot s = sxh = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$. That is, $x \cdot (h \cdot s) \neq (xh) \cdot s$ and hence this is not an action because it is not associative. □

Proof. Let G be a group and define the pairing $G \times G \to G$ by $(s, x) \mapsto xs^{-1}$. Then let $x \cdot s$ denote xs^{-1}. So that to show this is an action we need to show associativity and an identity action exists.

(a) Let $x, s, h \in G$. Then $x \cdot (s \cdot h) = x \cdot (hs^{-1}) = hs^{-1}x^{-1}$ and $(xs) \cdot h = hs^{-1}x^{-1}$, so that $x \cdot (s \cdot h) = (xs) \cdot h$ for all $x, s, h \in G$ as required.

(b) Then let $x \in G$ and e denote the identity in G. So that $e \cdot x = xe^{-1} = xe = x$. Hence $e \in G$ is the identity of the action.

Thus $(s, x) \mapsto (xs^{-1})$ is an action on G. □

Homework 1

6. Suppose $H \leq G$. Consider the pairing $G \times G/H \to G/H$ given by $(s, xH) \mapsto sxH$.

   (a) Show that the pairing is a transitive action.

   Proof. Define the mapping $G \times G/H \to G/H$ to be $(s, xH) \mapsto sxH$ for all $s \in G$ and $xH \in G/H$. Denote $s \cdot (xH) = sxH$. To show this is first is actually an action, we'll show associativity and an identity exist.

   i. Let $x, y \in G$ and $zH \in G/H$. So that $x \cdot (y \cdot zH) = x \cdot (yzH) = xyzH$ and $(xy) \cdot zH = xyzH$. Hence $x \cdot (y \cdot zH) = (xy) \cdot zH$ for all $x, y \in G$ and $zH \in G/H$ as required.

   ii. Let $e \in G$ be the identity of G and $xH \in G/H$. Then $e \cdot (xH) = (ex)H = xH$. Hence $e \in G$ is the identity action.

   That is the pairing $s \cdot (xH) = sxH$ is an action.

   Now to show that this is transitive. Let $xH, yH \in G/H$ and let $a = yx^{-1}$. Then $a \cdot xH = (yx^{-1})xH = yH$. So that, the action is transitive. □

   (b) Determine (with proof) the stabilizer of xH.

   Claim: stab$(xH) = xHx^{-1}$

   Proof. Let $y \in$ **stab**(xH). Then $y \cdot (xH) = xH \iff (yx)H = xH$. So that $(x^{-1}yx)H = H$. Because cosets are disjoint, we have $x^{-1}yx \in H$. So that $y \in xHx^{-1}$.

   Conversely, let $y \in xHx^{-1}$. Then $x^{-1}yx \in H$, so that $(x^{-1}yx)H = H$. Giving us the following:

$$\begin{aligned} & (x^{-1}yx)H = H \\ \iff & y(xH) = xH \\ \iff & y \cdot (xH) = xH. \end{aligned}$$

   Thus $y \in$ **stab**(xH).

   Hence **stab**$(xH) = xHx^{-1}$. □

   (c) Show that H is normal in G ($sHs^{-1} = H$ for all $s \in G$), if and only if, the kernel of the action is H.

   Proof. ($\implies$)

   Let H be normal in G; that is, $sHs^{-1} = H$ for all $s \in G$. Now we will show Kernel of the action $= H$ via set inclusion.

   Let a be in the kernel of the action; that is, $a \cdot (xH) = xH$ for all $xH \in G/H$. So that $axH = xH$, since H is normal in G, this is equivalent to $aHx = xH$. Hence

$aH = xHx^{-1} = H$ or just $aH = H$. The property of cosets being disjoint implies that $a \in H$.

Conversely, let $a \in H$. Then let $xH \in G/H$. Consider the following:

$$\begin{aligned} a \cdot (xH) &= (ax)H \\ &= aHx \text{ , by } H \text{ being normal} \\ &= (aH)x \text{ , by aH = H if a is in H} \\ &= Hx \\ &= xH, \text{ by normality of H.} \end{aligned}$$

Hence $a \cdot (xH) = xH$ for all $xH \in G/H$, thus a is in the kernel of the action.

Thus the kernel of the action is $H/$

($\Longleftarrow$) Conversely, let the kernel of the action be H. To show H is normal, we'll show that for $x \in G$, $xHx^{-1} = H$.

Let $y \in xHx^{-1}$. Then $x^{-1}yx \in H$, so that since the kernel of the action is H, we have:

$$x^{-1}yx \cdot x^{-1}H = x^{-1}H.$$

Hence $y(xx^{-1})H = xx^{-1}H \iff yH = H$, because cosets are distinct we have that $y \in H$ as desired.

Conversely, let $y \in H$. Then since H is the kernel of the action, $y \cdot (y^{-1}xH) = (y^{-1}xH)$. Hence $xH = y^{-1}(xH) \iff x^{-1}yxH = H$. Implying $x^{-1}yx \in H$, so that $y \in xHx^{-1}$, as desired.

Thus $xHx^{-1} = H$ for any $x \in G$. Hence H is normal in G. □

Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 2

1. Let $G = A_4$, the rotation group of the tetrahedron, where we number the vertices $1, 2, 3, 4$, and use the permutation action on the subscripts. Consider the subgroups $H = <\begin{pmatrix}1 & 2 & 3\end{pmatrix}>$ and $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. These are the stabilizer groups of the vertex 4, and the pair of edges $\{\overline{12}, \overline{34}\}$, respectively. In this problem we practice computing. Look for shortcuts!

   (a) List the left and right cosets of H in A_4.

   Solution. Left cosets:

$$\begin{aligned} H &= \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \\ (1\ 2\ 4)H &= \{(1\ 2\ 4), (1\ 4)(2\ 3), (1\ 3\ 4)\} \\ (1\ 4\ 2)H &= \{(1\ 4\ 2), (2\ 3\ 4), (1\ 3)(2\ 4)\} \\ (2\ 4\ 3)H &= \{(2\ 4\ 3), (1\ 4\ 3), (1\ 2)(3\ 4)\} \end{aligned}$$

   Right cosets:

$$\begin{aligned} H &= \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \\ H(1\ 2\ 4) &= \{(1\ 2\ 4), (1\ 3)(2\ 4), (2\ 4\ 3)\} \\ H(1\ 4\ 2) &= \{(1\ 4\ 2), (1\ 4\ 3), (1\ 4)(2\ 3)\} \\ H(2\ 3\ 4) &= \{(2\ 3\ 4), (1\ 2)(3\ 4), (1\ 3\ 4)\} \end{aligned}$$

   □

   (b) List the left and right cosets of K in A_4.

   Solution. Left(and Right) cosets:

$$\begin{aligned} K &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\ (1\ 3\ 2)K = K(1\ 3\ 2) &= \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\} \\ (1\ 2\ 3)K = K(1\ 2\ 3) &= \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\} \end{aligned}$$

   □

   (c) G acts on the coset spaces G/H and G/K by left multiplication. Describe explicitly the stabilizers of the different cosets of H and K in A_4.

   Solution. Note that we may calculate the stabilizers $a \in G$ in the following fashion:

$$a \cdot bH = bH, \text{ by stabilizer def.}$$

$$\iff (ab)H = bH, \text{ by definition of left mult. action}$$
$$\iff (b^{-1}ab)H = H, \text{ by left mult. of } b^{-1}$$
$$\iff b^{-1}ab \in H, \text{ by cosets being pairwise disjoint}$$

$\iff a \in bHb^{-1} = \{(1), (b(1)\, b(2)\, b(3)), (b(1)\, b(3)\, b(2))\}$, by secret conjugation trick, where $bH \in G/H$.

So that:

$$b = (1) : bHb^{-1} = H = \mathbf{stab}(H)$$
$$b = (1\ 2\ 4) : bHb^{-1} = \{(1), (2\ 4\ 3), (2\ 3\ 4)\} = \mathbf{stab}((1\ 2\ 4)H).$$
$$b = (1\ 4\ 2) : bHb^{-1} = \{(1), (1\ 3\ 4), (1\ 4\ 3)\} = \mathbf{stab}((1\ 4\ 2)H).$$
$$b = (2\ 4\ 3) : bHb^{-1} = \{(1), (1\ 4\ 2), (1\ 2\ 4)\} = \mathbf{stab}((2\ 4\ 3)H).$$

Those are the stabilizer subgroups of H with left-multiplication.

For $G/K = \{K, (1\ 3\ 2)K, (1\ 2\ 3)K\}$ we can use the same process, that is $a \cdot bK = bK \iff a \in bKb^{-1}$. However by $(1.b)$ we have that K is normal in G, since it's right and left cosets are identical. So that, from the definition of normality $bKb^{-1} = K$. That gives us that $a \cdot bK = bK \iff a \in K$, regardless of what $b \in G$ is. So that the all the stabilizer subgroups are identical:

$$\mathbf{stab}(K) = \mathbf{stab}((1\ 2\ 3)K) = \mathbf{stab}((1\ 3\ 2)K) = K.$$

□

(d) Compute the homomorphisms $A_4 \to S_3$ and $A_4 \to S_4$ determined by the actions of A_4 on A_4/H and A_4/K, respectively.

Solution. First, recall from the leading paragraph in (1) that A_4 is the rotation group of the tetrahedron, with vertices labeled $1, 2, 3, 4$ and permutations act on the subscripts. We'll show the result by examining rotations acting on two substructure sets on the tetrahedron.

Homework 2

For $A_4 \to S_3$, define the substructures $X = \{\overline{12}, \overline{34}\}$, $Y = \{\overline{13}, \overline{24}\}, Z = \{\overline{14}, \overline{23}\}$. Then let A_4 act on these substructures, doing so we'll obtain the following table:

$$\begin{aligned}
(1) &\mapsto (1)\\
(3\ 4\ 2) &\mapsto (X\ Y\ Z)\\
(2\ 4\ 3) &\mapsto (X\ Z\ Y)\\
(1\ 3\ 4) &\mapsto (X\ Z\ Y)\\
(1\ 4\ 3) &\mapsto (X\ Y\ Z)\\
(1\ 2\ 4) &\mapsto (X\ Y\ Z)\\
(1\ 4\ 2) &\mapsto (X\ Z\ Y)\\
(1\ 2\ 3) &\mapsto (X\ Z\ Y)\\
(1\ 3\ 2) &\mapsto (X\ Y\ Z)\\
(1\ 2)(3\ 4) &\mapsto (X\ Z)\\
(1\ 4)(2\ 3) &\mapsto (Y\ Z)\\
(1\ 3)(2\ 4) &\mapsto (X\ Y).
\end{aligned}$$

Label $X = 1, Y = 2, Z = 3$, this gives us a map $\phi : A_4 \to S_3$. By Group Conjugation Theorem 1, this is in one-to-one correspondence with the natural homomorphism from $A_4 \to A_4/H$, where H is the stabilizer of the triangle $\Delta 123$. Similarly, for $A_4 \to S_4$. Consider the substructures:

$$W = \Delta 132, X = \Delta 134, Y = \Delta 234, Z = \Delta 124.$$

Letting A_4 act on the substructures, we obtain the following map:

$$\begin{aligned}
(2\ 3\ 4) &\mapsto (X\ Z\ W)\\
(2\ 4\ 3) &\mapsto (X\ W\ Z)\\
(1\ 3\ 4) &\mapsto (Y\ Z\ W)\\
(1\ 4\ 3) &\mapsto (Y\ W\ Z)\\
(1\ 2\ 4) &\mapsto (X\ W\ Y)\\
(1\ 4\ 2) &\mapsto (X\ Y\ W)\\
(1\ 2\ 3) &\mapsto (X\ Z\ Y)\\
(1\ 3\ 2) &\mapsto (X\ Y\ Z)\\
(1\ 2)(3\ 4) &\mapsto (X\ Y)(W\ Z)\\
(1\ 4)(2\ 3) &\mapsto (X\ Z)(Y\ W)\\
(1\ 3)(2\ 4) &\mapsto (X\ W)(Y\ Z)\\
(1) &\mapsto (1),
\end{aligned}$$

Homework 2

give the labeling $X = 1, Y = 2, Z = 3, W = 4$ and this is clearly a map $\tau : A_4 \to S_4$. By Group Conjugation Theorem 1, this is in one-to-one correspondence with the natural homomorphism from $A_4 \to A_4/K$, where K is the stabilizer of the line pair $\{\overline{12}, \overline{34}\}$. □

2. Prove that if $n \geq 4$, the natural homomorphism $A_n \to \mathrm{Aut}(A_n)$ is injective, but not surjective.

   Proof. Let $n \geq 4$. □

3. Let $H \leq S_n$ be the subgroup $\{a \in S_n : a(n) = n\}$ and let $N_G(H)$ be the normalizer. Then $N_G(H)$ is also a subgroup of S_n.

   (a) Determine $[S_n : H]$.

   Solution.
   $$[S_n : H] = \frac{n!}{|H|},$$
   note that the cardinality of H is exactly $(n-1)!$, we'll show this with a counting argument. Fix $a(n) = n$, then for $a(n-1)$ we have $n-1$ choices, for $a(n-2)$ we have $n-2$ choices since we cannot choose the previous number chosen for $a(n-1)$, and so on for $a(i)$ we have i choices for $i \in \{1, 2, \ldots, n-1\}$. These are dependent choices on each other, meaning we have $(n-1)!$ possibilities for an element being in H. Hence $|H| = (n-1)!$, so that $[S_n : H] = n$. □

   (b) Suppose $b \in S_n$ and $b(n) = m$. Write a set-description of bHb^{-1} in S_n, in terms of b.

   Solution. **Claim:**
   $$bHb^{-1} = \{\sigma \in S_n : \sigma(m) = m\} = X.$$

   Proof. ($\subseteq$)
   Let $\sigma \in bHb^{-1}$ so that $\sigma = bab^{-1}$, where $b(n) = m$, $a(n) = n$, $b^{-1}(m) = n$. Then $bab^{-1}(m) = b(a(n)) = b(n) = m$✓. Hence $\sigma \in X$.
   ($\supseteq$)
   Let $\sigma \in S_n$ and $\sigma(m) = m$. Then define $a = b^{-1}\sigma b$. Note that $(b^{-1}\sigma b)(n) = b^{-1}\sigma(m) = b^{-1}(n) = m$. That is, $b^{-1}ab \in X$. So then, $\sigma = b(b^{-1}\sigma b)b^{-1}$. Since $b^{-1}\sigma b \in H$, we have that $\sigma \in bHb^{-1}$.
   Thus $bHb^{-1} = X$. □

   □

(c) Determine $N_G(H)$.

Solution. **Claim:**

$$N_G(H) = H$$

Proof. Note, if $a \in H$, then $aH = H = Ha$. So that $H \subseteq N_G(H)$.
Conversely, let $a \in N_G(H)$. So that $aH = Ha$, or $aHa^{-1} = H$. Note that $(1\ 2\ \ldots\ n{-}1) \in H$, hence $a(1\ 2\ \ldots\ n{-}1)a^{-1} = (a(1)\ a(2)\ \ldots\ a(n{-}1)) = \sigma \in H$. For $\sigma \in H$, this would imply that $\sigma(n) = n$, implying that $a(i) \neq n$ for all $i \in \{1, 2, \ldots, n-1\}$. So that $a(n) = n$. Hence $a \in H$, giving us $N_G(H) \subseteq H$.
Thus $H = N_G(H)$. □

□

4. Write the (conjugacy) class equations of D_5 and D_6. Find the stabilizer subgroups of a representative element from each class, by first computing the order of the subgroup from the size of the conjugacy class.

Solution. Let $G = D_5$ Draw the pentagon, with the first vertex (v_1) placed at $(0, 1)$ then place $\{v_2, v_3, v_4, v_5\}$ rotations of $\dfrac{2\pi}{5}$ in the plane. Let r be the rotation $\dfrac{2\pi}{5}$ and s be the reflection centered on v_1 and it's opposite face. We can determine the conjugacy classes via conjugacy substructures, define the substructures Y_i to be the vertex i paired with it's opposite face; that is Y_1 is the vertex v_1 and the face opposite from it. Every reflection will then be conjugate to each other, since the $G_{Y_1} = \{e, s\}$, $G_{Y_2} = \{e, rs\}, \ldots, G_{Y_5} = \{e, r^4 s\}$, so that $r(Y_1) = Y_2$ and $r(Y_2) = Y_3$ and so on. Thus by Theorem II in Group Conjugation, we have $G_{Y_1} = rG_{Y_2}r^{-1} = r^2 G_{Y_3} r^{-2} = \ldots = r^4 G_{Y_5} r^{-4}$, implying that the reflections all share the same conjugacy class since this shows up to rotation the stabilizers are equivalent. There are 5 rotations: $\{s, rs, r^2 s, r^3 s, r^4 s\}$. To find the rest of the conjugacy classes, note that $sr^{-1} = rs$ in D_5, so that $(r^m s)r^n(r^m s)^{-1} = sr^{-m+n}sr^{-m} = sr^n s = r^{-n}$. Hence r^n is conjugate to r^{-n} for all $n \in \{1, 2, 3, 4, 5\}$. Implying 2 conjugacy classes for D_5 rotations:

$$\{r, r^4\} \qquad \text{and} \qquad \{r^2, r^3\}.$$

So that the class equation of D_5:

$$|D_5| = 1 + 5 + 2 + 2,$$

in order of proof.

For $G = D_6$, we look at the symmetries of the hexagon on the plane. Construct the hexagon in the same fashion as the pentagon, starting at $(0, 1)$, with rotations $r = \dfrac{\pi}{3}$

and reflection s through the vertices v_1 and v_4. We have the identity is the only element that fixes everything, it is in it's own conjugacy class.

Construct 3 substructures in D_6, line segments pairing opposite vertices. Call these $Y_1 = \overline{1\ 4}, Y_2 = \overline{2\ 5}, Y_3 = \overline{3\ 6}$. Then note that $G_{Y_1} = \{e, r^3, s, r^3s\}, G_{Y_2} = \{e, r^3, r^2s, r^5s\}, G_{Y_3} = \{e, r^3, r^4s, rs\}$.

Note that $r(Y_1) = Y_2$, so that $G_{Y_1} = rG_{Y_2}r^{-1}$ and $r(Y_2) = Y_2$ so that $G_{Y_2} = rG_{Y_3}r^{-1}$ and $r(Y_3) = Y_1$ so that $G_{Y_3} = rG_{Y_1}r^{-1}$. Similar to the pentagon, we obtain $G_{Y_1} = rG_{Y_2}r^{-1} = r^2G_{Y_1}r^{-2}$. Through the conjugate done we obtain 2 classes of reflections in D_6:

$$\{s, r^2s, r^4s\} \qquad \text{and} \qquad \{rs, r^3s, r^5s\}.$$

For the rotations, note again that $(r^ms)r^nsr^{-m} = sr^{-n}s$, that is a rotation and it's inverse form a conjugacy class. So that is: $\{r, r^5\}, \{r^2, r^4\}, \{r^3\}$. Hence

$$|D_6| = 1 + 3 + 3 + 2 + 2 + 1,$$

in order of proof.

Stabilizers:

For $G = D_5$, we found the stabilizer subgroup of the reflections, the lines pairing vertices with midpoints of the opposite face. For the classes $2 + 2$, nothing is fixed, since rotations effect the entire set of vertices and only leave the trivial substructures of the entire set of vertices and the center of the pentagon the same structure. That is $\{e, r, r^2, r^3, r^4\}$ is the stabilizer subgroup of the hexagon.

For $G = D_6$, we found the stabilizer subgroup of line segments through the first point and 4^{th} midpoint to be $< r^3, rs >$. For the line segments through the first vertex and the fourth vertex had a stabilizer subgroup of $< r^3, s >$. For the rotations $< r^2 >$ this is the stabilizer subgroup of an equilateral triangle inscribed into the hexagon. For $\{e, r, r^5\}$ this will only fix the entire hexagon. □

5. Write the class equation of S_5, and then for A_5. Show all work. [*Hint:* Use Action Theorem I to determine the cardinalities of conjugacy classes in A_5.]

Solution. For S_5 we have cycle types of $5^1, 4^1 1^1, 3^1 1^2, 3^1 2^1, 2^2 1^1, 2^1 1^3, 1^5$ which gives us the following class equation:

$$|S_5| = 24 + 30 + 20 + 20 + 20 + 15 + 10 + 1.$$

A_5 is the group of symmetries of tetrahedrons inscribed inside a dodecahedron, and even cycles in S_5, these will have cycle type $5^1, 3^1 1^2, 2^2 1^1, 1^5$. Since $A_5 \leq S_5$, these

conjugacy classes have to be distinct in A_5. The dodecahedron has 12 faces, 30 edges, and 20 vertices.

We can construct these using conjugate substructure, flips about opposite edges, these will amount to the same action and will account for 15 such flips. Similar to D_5, we will have rotations about faces account for 2 separate conjugacy classes, that is a rotation and it's inverse will be the same conjugacy class. Since rotating about a face is equivalent to rotating about the opposite face, we have only 6 face pairs that matter. That is we have a conjugacy classes of $\frac{2\pi}{5}$ rotations and $\frac{-2\pi}{5}$ rotations about a face pair, then a separate conjugacy class of $\frac{4\pi}{5}$ and $\frac{-4\pi}{5}$. These will account for 12 and 12. Finally, we have reflections about vertices, we have 20 of these, all conjugate to each other, since they are similar up to re-labeling. Then of course the identity. That is the class equations of A_5 is:

$$|A_5| = 15 + 12 + 12 + 20 + 1,$$

in order of proof. □

6. Prove that A_5 is a simple group, by examining its conjugacy class sizes and using the fact that a normal subgroup is a union of conjugacy classes.

Proof. From the previous problem, we have the class equation of A_5 is:

$$|A_5| = 1 + 12 + 12 + 15 + 20.$$

For sake of contradiction, suppose $\{e\} \neq N \lhd A_5$. Then N must be the disjoint union of some conjugacy classes of A_5 and $|N|$ must divide 60. However, consider the following combinations of the sizes of the conjugacy classes of A_5:

$$1 + 12 \not| 60 \qquad 1 + 15 \not| 60 \qquad 1 + 20 \not| 60$$

$$1 + 12 + 12 \not| 60 \qquad 1 + 12 + 15 \not| 60 \qquad 1 + 12 + 20 \not| 60$$

$$1 + 12 + 12 + 15 \not| 60 \qquad 1 + 12 + 12 + 20 \not| 60.$$

That no subgroup formed by the union of conjugacy classes can have an order that divides 60. Hence, there can be no non-trivial normal subgroup of A_5. □

7. Use the conjugacy class of $(2, 2)$ cycles in S_4 to prove there exists a nontrivial homomorphism $S_4 \to S_3$. Compute the centralizer of (1 2)(3 4), and compute the kernel of the homomorphism.

Solution. Define $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, and note that K is a normal subgroup of S_4 since conjugation in S_4 preserves cycle and K contains all cycles of cycle type $(2, 2)$ in S_4.

Then define the map $\phi : g \mapsto gK$ on sets $S_4 \to S_4/K$. This is the natural homomorphism from $S_4 \to S_4/K$, now we'll show that $S_4/K \cong S_3$.

We know that $K, (1\ 2\ 3)K, (1\ 3\ 2)K \in S_4/K$ from $1(b)$, then note that:

$$(1\ 2)K = \{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

$$(2\ 3)K = \{(2\ 3), (1\ 3\ 4\ 2), (1\ 2\ 4\ 3), (1\ 4)\}$$

$$(1\ 3)K = \{(1\ 3), (1\ 2\ 3\ 4), (2\ 4), (1\ 4\ 3\ 2)\}$$

Hence $S_4/K \cong S_3$ as we can see with the left cosets. Define the new map $\tau : S_4/K \to S_3$ by sending σK to it's cosets representative element defined above. That gives us that $\tau \circ \phi : S_4 \to S_3$ is a homomorphism as desired.

The centralizer $C((1\ 2)(3\ 4)) = \{\sigma \in S_n : \sigma(1\ 2)(3\ 4)\sigma^{-1} = (1\ 2)(3\ 4)\}$, so by the secrete conjugation trick $C((1\ 2)(3\ 4)) = \{e, (1\ 2)(3\ 4)\}$. Then the kernel of the homomorphism will be everything that gets mapped to K through ϕ; that is $k \in \ker(\phi)$, then $kK = K \iff k \in K$, this then gets sent to (1) through our map τ. Thus the kernel of the homomorphism is K. $\square$

Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 3

1. Prove that the 3−cycles of A_n, $n \geq 5$, are all conjugate. Do this by computing the centralizer $C_{A_n}((1\ 2\ 3))$. Prove that in A_3 and A_4, not all 3−cycles are conjugate.

   Proof. To find the centralizer of $C_{A_n}(1\ 2\ 3)$ we can use the secret conjugation trick.

   Let $\sigma \in C_{A_n}(1\ 2\ 3)$. Then $\sigma = \tau(1\ 2\ 3)\tau^{-1}$, hence by the secret conjugation trick τ must either satisfy:

   (a) $\tau(1) = 1, \tau(2) = 2, \tau(3) = 3$
   (b) $\tau(1) = 2, \tau(2) = 3, \tau(3) = 1$
   (c) $\tau(1) = 3, \tau(2) = 1, \tau(3) = 2$.

   So that the centralizer $C_{A_n}(1\ 2\ 3)$ is anything that either fixes $\{1, 2, 3\}$ or has subcycles $(1\ 2\ 3)$ or $(1\ 3\ 2)$, that leaves $\{4, 5, \ldots, n\}$ to permute, evenly. So that the cardinality of $C_{A_n}(1\ 2\ 3)$ is $\dfrac{3(n-3)!}{2}$.

   By the cycle type of 3-cycles in S_n, $3^1 1^{n-3}$ in multiplicative notation. We know the cardinality of $[(1\ 2\ 3)]_{S_n} = \dfrac{n!}{3^1 1^{n-3} 1!(n-3)!} = \dfrac{n(n-1)(n-2)}{3}$..

   Note that under the conjugation action, $C_{A_n}(1\ 2\ 3)$ is the stabilizer of $(1\ 2\ 3)$ or $\mathbf{stab}(1\ 2\ 3)$. So by the orbit-stabilizer theorem we have that $|\text{orb}(1\ 2\ 3)| \cdot |\mathbf{stab}(1\ 2\ 3)| = |A_n| = \dfrac{n!}{2}$ and that $|[(1\ 2\ 3)]_{A_n}| = |\text{orb}(1\ 2\ 3)|$. We have that $|\mathbf{stab}(1\ 2\ 3)| = \dfrac{3(n-3)!}{2}$ by our counting argument. So that $|[(1\ 2\ 3)]_{A_n}| = |\text{orb}(1\ 2\ 3)| = \dfrac{n(n-1)(n-3)}{3}$. That is, the conjugacy classes of $(1\ 2\ 3)$ in A_n and S_n are the same size. Conjugacy classes going from S_n to A_n either split or stay the same. Since this conjugacy class is the same size in A_n and S_n, we must have that $[(1\ 2\ 3)]_{A_n} = [(1\ 2\ 3)]_{S_n}$, which is exactly the set of 3-cycles in S_n, for $n \geq 3$. □

   Counter-Example. Consider $(1\ 2\ 3)$ and $(1\ 3\ 2)$ in A_3. So that for these two to be conjugate we need a $\sigma \in A_3$ such that either one of the three things is true, by the conjugation trick:

   (a) $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$
   (b) $\sigma(1) = 3$, $\sigma(2) = 2, \sigma(3) = 1$
   (c) $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$

   Note that all of these are 2−cycles, hence in A_3, $(1\ 2\ 3)$ is not conjugate to $(1\ 3\ 2)$. Furthermore, neither are they in A_4 since we must have at least 1 fixed point and 1 two-cycle. That is in A_4, $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are not conjugate to each other. □

Homework 3

2. Let G be a group, X a transitive G-set. Prove that X is isomorphic to the G-set of left G_x-cosets where $x \in X$.

Proof. Let G be a group, X be a transitive G-set. We'll show the result by defining an explicit isomorphism.

Then there exists a $x_0 \in X$ such that $X = G \cdot x_0$. Define $\phi : G/G_{x_0} \to X$ given by $\phi(gG_{x_0}) = g \cdot x_0$. To show this is an isomorphism, we'll show structure is preserved and the function is a bijection.

Take $aG_{x_0}, bG_{x_0} \in G/G_{x_0}$. Then $\phi((ab)\cdot G_{x_0}) = (ab)\cdot x_0$ and $\phi(a)\cdot\phi(b) = (a\cdot x_0)\cdot(b\cdot x_0) = a \cdot (b \cdot x_0) = (ab) \cdot x_0$. Hence ϕ is structure preserving as required.

To show it's bijective, we'll show that its inverse is defined. Note that since X is a transitive $G-$set, for all $y \in X$ there exists a $g \in G$ such that $g \cdot y = x_0$, so that g is unique. Hence $y = g^{-1} \cdot x_0$ is unique for every $y \in X$. Define the map $\phi^{-1} : X \to G/G_{x_0}$ by $\phi^{-1}(g^{-1} \cdot x_0) = g^{-1}G_{x_0}$. Hence ϕ^{-1} is well-defined on X, and $\phi(\phi^{-1}(y)) = \phi(\phi^{-1}(g^{-1} \cdot x_0)) = \phi(g^{-1}G_{x_0}) = g^{-1} \cdot x_0 = y$, hence $\phi(\phi^{-1}) = \mathrm{id}_X$ as required.

Thus we have an order-preserving isomorphism between the $G-$sets X and G/G_{x_0}. Furthermore, note since $X = G \cdot x_0$, we'll have that G/G_x us isomorphic to G/G_{x_0} for any $x \in X$. □

Homework 3

3. Suppose N and K are groups, and $\gamma : K \to \text{aut}(N)$ is an action. Let $N \rtimes_\gamma K = (N \times K, *)$, where $(a,b) * (c,d) = (a\gamma(b)(c), bd)$:

   (a) Prove that $N \rtimes_\gamma K$ is a group.

   (b) Let $N' = N \times \{e\}$ and $K' = \{e\} \times K$. These are subgroups of $N \rtimes_\gamma K$. Prove that γ induces a map $\gamma' : K' \to \text{Aut}(N')$ that factors through $\text{Inn}(N \rtimes_\gamma K)$

   (a) *Proof.* Let N and K be groups, and $\gamma : K \to \text{aut}(N)$ be an action.
   Let $(a,b), (c,d), (f,g) \in N \times K$.

      i. (Associativity) Consider the following:

$$\begin{aligned}((a,b) * (c,d)) * (f,g) &= (a\gamma_b(c), bd) * (f,g) \\ &= (a\gamma_b(c)\gamma_{bd}(f), bdg) \\ (a,b) * ((c,d) * (f,g)) &= (a,b) * (c\gamma_d(f), dg \\ &= (a\gamma_b(c\gamma_d(f)), bdg).\end{aligned}$$

      These are equivalent through the fact that γ_i is a homomorphism and splits over the group action, that is $\gamma_b(c\gamma_d(f)) = \gamma_b(c)\gamma_{bd}(f)$.

      ii. (Identity) Let $e_N \in N$ and $e_K \in K$ be the identities in their respective groups. So that:

$$\begin{aligned}(a,b) * (e_N, e_K) &= (a\gamma_b(e_N), be_k) \\ &= (a,b)\end{aligned}$$

      the last step following from the fact that γ_b is a homomorphism and maps identity to identity. To show left identity:

$$\begin{aligned}(e_N, e_K) * (a,b) &= (e_n\gamma_{e_K}(a), e_K b) \\ &= (a,b)\end{aligned}$$

      , where the last step follows because $e_K \cdot a = a$.

      iii. (Inverses) Consider the following:

$$\begin{aligned}(a,b) * (\gamma_{b^{-1}}(a^{-1}), b^{-1}) &= (a\gamma_{bb^{-1}}(a^{-1}a), bb^{-1}) \\ &= (e_N, e_K).\end{aligned}$$

      Hence every (a,b) has a right inverse. Consider the following:

$$\begin{aligned}(\gamma_{b^-}(a^{-1}), b^{-1}) * (a,b) &= (\gamma_{b^{-1}}(a^{-1})\gamma_{b^{-1}}(a), b^{-1}b) \\ &= (\gamma_{b^{-1}}(a^{-1}a), e_K) \\ &= (\gamma_{b^{-1}}(e_N), e_K \\ &= (e_N, e_K),\end{aligned}$$

      so (a,b) has a left inverse as required.

Thus $N \rtimes_\gamma K$ is a group. □

(b) *Proof.* Let $N' = N \times \{e\}$ and $K' = \{e\} \times K$. e denotes e_N in the first coordinate, and e_K in the second.

Then define the map $\gamma' : K' \to \mathrm{Aut}(N')$ given by $\gamma'(e,b) : (c,e) \mapsto \gamma'(e,b)(e,c)$ this being an action. Finally, define $\gamma'(e,b)(c,e) = (e,b) * (c,e) * (e,b)^{-1} = (e\gamma_b(c), b) * (\gamma_{b^{-1}}(e), b^{-1}) = (\gamma_b(c), e)$. This factors through $\mathrm{Inn}(N \rtimes_\gamma K)$ as need. □

Homework 3

4. Prove that the dihedral group D_n, $n \geq 3$, is an internal semidirect product $< r > \rtimes < s >$, where the action $\gamma :< s > \to \text{Aut}(< r >)$ is given by $\gamma_s(r) = srs^{-1}$.

   Proof. Let $n \geq 3$ and $\gamma :< s > \to \text{Aut}(< r >)$ given by $\gamma_s(r) = srs^{-1}$. Note that $< s >= \{(1), s\}$.

   We'll show the result by Theorem 2.2.

   (a) Let $a \in < r > \cap < s >$. Then $a = e$, as required.

   (b) Note that we can define $D_n = \{r^m s^i : r^n = e \text{ and } s^2 = e\}$. So that $sr^m = r^{-m}s$. With these relations it's clear that $< r >< s >= D_n$, for $n \geq 3$.

   (c) Finally we'll show for any $r^m s^i \in D_n$ that $r^m s^i < r > s^{-i} r^{-m} =< r >$.
   Take $r^k \in < r >$. Then $r^m s^i r^k s^{-i} r^{-m} = s^i r^{-m} r^k r^m s^{-i} = s^i r^k s^{-i} = s^{2i} r^k = e^i r^k = r^k$. Hence $< r > \lhd D_n$.

   Thus by Theorem 2.2 we have the result:

$$D_n \cong < r > \rtimes_\gamma < s > .$$

□

Homework 3

5. Prove S_n, $n \geq 3$, is a semidirect product of A_n and $< (1\ 2) >$.

   Proof. Let $n \geq 3$. We'll use Theorem 2.2 on the conjugation theorem to show the result. That is:

   (a) $A_n \cap < (1\ 2) >= \{(1)\}$

   (b) $A_n < (1\ 2) >= S_n$

   (c) $A_n \lhd S_n$

   (a) Let $\sigma \in A_n \cap < (1\ 2) >$. Then since $(1\ 2)$ is an odd cycle and $< (1\ 2) >= \{(1), (1\ 2)\}$. We must have $\sigma = (1)$. So that we have (1) as required.

   (b) Note this is equivalent to $A_n \cup A_n(1\ 2) = S_n$, where the union is a disjoint union (except for (1)). Clearly $A_n \cup A_n(1\ 2) \subseteq S_n$.

   Conversely, let $\sigma \in S_n$. Then σ is either even or odd. If σ is even, then $\sigma \in A_n$. If σ is odd, then $\sigma(1\ 2)$ is even by definition. So that $\sigma(1\ 2)(1\ 2) = \sigma$. Hence $\sigma \in A_n(1\ 2)$.

   Thus $A_n < (1\ 2) >= S_n$.

   (c) Finally, we have by the secret conjugation trick, because conjugation doesn't change cycle type that $\sigma A_n \sigma^{-1} = A_n$ for any $\sigma \in S_n$. So that $A_n \lhd S_n$.

   Hence by Theorem 2.2 in the conjugation handout, $A_n \rtimes_\gamma < (1\ 2) > \cong S_n$. □

Homework 3

6. Prove that if n is odd then $O_n = SO_n \times < -I_n >$.

Proof. Let n be odd. Then we'll show the result by using Theorem 1 from the conjugation handout. Note that $< -I_n >= \{I_n, -I_n\}$ That is, we'll show

(a) $SO_n \cap < -I_n >= \{I_n\}$

(b) $SO_n(< -I_n >) = O_n$

(c) $SO_n \lhd O_n$

(a) Take $A \in SO_n \cap < -I_n >$. Then $\det(A) = 1$ and $A^{-1} = A^T$ and, $A = I_n$ or $A = -I_n$. Since $\det(A) = 1$, we must have $A = I_n$. Hence (a).

(b) Note this is equivalent to $O_n = SO_n \cup (-I_n SO_n)$ is a disjoint union. Clearly $SO_n \cup (-I_n SO_n) \subseteq O_n$. Conversely, take $A \in O_n$.
Then two cases follow:
(1) $\det(A) = 1$ and $AA^T = I_n$, so that $A \in SO_n$.
(2) $\det(A) = -1$ and $AA^T = I_n$. Note that $\det(A) = \det(A^T) = -1$. Furthermore, $\det(A(-I_n)) = 1$ so that $A(-I_n) \in SO_n$, $X(-I_n) = (-I_n)X$ (by scalar multiplication). So that we may write $A = (-I_n)^2 A = (-I_n A)(-I_n)$; that is, $A \in SO_n(-I_n)$. Hence $SO_n \cup < -I_n >= O_n$.

(c) We'll show for all $X \in O_n$, $XSO_nX^{-1} = SO_n$. Let $A \in SO_n$ and $X \in O_n$. Additionally,

$$(XAX^{-1})^{-1} = XA^{-1}X^{-1} = XA^TX^T$$

and

$$(XAX^{-1})^T = XA^TX^T.$$

So that $XAX^{-1} \in SO_n$ as required. Conversely, take $A \in SO_n$ and $X \in O_n$. Then using the same argument above $(XAX^{-1}) = (XAX^{-1})^T$. So that

$$SO_n = XSO_nX^{-1} \qquad \text{for all } X \in O_n.$$

Hence $SO_n \lhd O_n$.
Finally, to show that $\{I_n, -I_n\} \lhd O_n$. Let $A \in O_n$, then

$$I_n A I_n = A$$

and

$$-I_n A(-I_n) = (-1)^2 A = A,$$

for all $A \in O_n$. Hence $< (-I_n) > \lhd O_n$.

Hence by theorem 1 on the conjugation handout, we have $O_n \cong SO_n \times < -I_n >$. □

Homework 3

7. Suppose n is even. Let

$$T = \begin{bmatrix} 0 & I_{n/2} \\ I_{n/2} & 0 \end{bmatrix} \in O_n$$

Prove $O_n = SO_n \rtimes_\gamma < T >$, where the action $\gamma :< T > \to \mathrm{Aut}(SO_n)$ is given by

$$\gamma(T)\left(\begin{bmatrix} A & B \\ C & D \end{bmatrix}\right) = \begin{bmatrix} 0 & I_{n/2} \\ I_{n/2} & 0 \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} 0 & I_{n/2} \\ I_{n/2} & 0 \end{bmatrix}^{-1} = \begin{bmatrix} D & C \\ B & A \end{bmatrix}$$

T is the permutation matrix for

$$\tau = \left(1 \ \frac{n+2}{2}\right)\left(2\frac{n+4}{2}\right)\dots\left(\frac{n}{2} \ n\right) \in S_n$$

Intersecting S_n and A_n with O_n and SO_n yields $S_n = A_n \rtimes_\gamma < \tau >$. Prove that the map $-1 \mapsto T$ splits the exact sequence given by the determinant,

$$1 \to SO_n \to O_n \to \{\pm 1\} \to 1$$

So we can write $O_n = SO_n \rtimes_\gamma < -1 >$.

Proof. I worked with Cameron Fredrickson on this one.

Let n be even To show $1 \to SO_n \to O_n \to \{\pm 1\} \to 1$ splits, we just need to show there exists a homomorphism $\phi : \{\pm 1\} \to O_n$. Then via the splitting theorem for short exact sequences (from Wikipedia) we have that $O_n \cong SO_n/\{\pm 1\}$. Define this explicitly, by mapping $\phi(1) = I_n$ and $\phi(-1) = -I_n$. So notice that $\phi(1 \cdot -1) = \phi(-1) = -I_n = I_n(-I_n)$, note that $\{\pm I_n\}$ and $\{\pm 1\}$ are Abelian with their sets. Then $\phi(1 \cdot 1) = \phi(1) = I_n I_n$ and $\phi((-1)(-1)) = \phi(1) = I_n = (-I_n)^2$. Furthermore, note that $\det \circ \phi = \mathrm{id}_{O_n}$ as required for the exact sequence to split.

Hence we have that $O_n \cong \{SO_n, (-1)SO_n\}$ as required. □

Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 4

I worked with Kelsey Lowery, Caroline Semmens, Zach Gelber, Tim Royston, Cameron Fredrickson, Nathan Lafferty, Brandon Le, Lucas Kerbs on this homework set.

1. Conjugacy classes in O_2. We can interpret O_2 as a group of symmetries of the $xy-$ plane.

   (a) Use you intuition to guess the conjugacy classes in O_2. Then prove your guess is correct.

   (b) Do the same for the subgroup of SO_2.

   (c) Prove that the unit circle is a PHS for SO_2, but not for O_2.

   (a) *Solution.* Note that $O_2 = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} : \theta \in [0, 2\pi) \right\} \sqcup \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} : \theta \in [0, 2\pi) \right\}$.
   Let $r(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ and $s(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$, so that $(r(\theta))^{-1} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$.
   Then let $\theta, \phi \in [0, 2\theta)$, so that using Mathematica for the matrix computations we see the following:

   $$r(\phi)s(\theta)(r(\phi))^{-1} = \begin{bmatrix} \cos 2\phi + \theta & \sin 2\phi + \theta \\ \sin 2\phi + \theta & -\cos 2\phi + \theta \end{bmatrix}$$

   That is $r(\phi)s(\theta)r^{-1}(\phi) = s(2\phi - \theta)$ is a reflection in the plane.

   $$r(\phi)r(\theta)(r(\phi))^{-1} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

   That is $r(\phi)r(\theta)r^{-1}(\phi) = r(\theta)$.

   $$s(\phi)s(\theta)(s(\phi))^{-1} = \begin{bmatrix} \cos 2\phi - \theta & \sin 2\phi - \theta \\ \sin 2\phi - \theta & -\cos 2\phi - \theta \end{bmatrix}$$

   $s(\phi)s(\theta)(s(\phi))^{-1} = s(2\phi - \theta)$. Then:

   $$s(\phi)r(\theta)(s(\phi))^{-1} = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} = r^{-1}$$

   That is $s(\phi)r(\theta)(s(\phi))^{-1}$ is an inverse rotation.
   That is, for $\theta \in [0, 2\pi)$, $[r(\theta)] = \{r(\theta), r^{-1}(\theta)\}$ and $[s(\theta)] = \{s(\phi) : \phi \in [0, 2\pi)\}$. That is, every rotation and it's inverse are in there own conjugacy class, while the reflections are all in one conjugacy class. Then the identity is in it's own conjugacy class. □

Homework 4

(b) *Solution.* Note that $SO_2 = \left\{ \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} : \theta \in [0, 2\pi) \right\}$. So by our work in part (a.), we have that the conjugacy classes in SO_2 are just rotations and their inverses, and the identity. That is, with $\theta \in [0, 2\pi)$:

$$[r(\theta)] = \{r(\theta), r^{-1}(\theta)\} \qquad \text{and} \qquad [e] = \{e\}.$$

□

(c) *Solution.* Finally, let $U = \{(\cos(\theta), \sin(\theta))^T : \theta \in [0, 2\pi)\}$ denote the unit circle in the plane.

Then to show U is a principal homogeneous set for SO_2, we must show that SO_2's action on U is free (for all $(x, y) = (\cos(\theta), \sin(\theta))^T \in U$, $(SO_2)_{(x,y)} = \{e\}$ for all $(x, y) \in U$) and homogeneous ($U = \text{orb}(x, y)$ for some $(x, y) \in U$, where the action is matrix multiplication using SO_2 on $(x, y) = (\cos(\theta), \sin(\theta))^T$).

Take $(0, 1)^T$, then let's act on it with an element in SO_2:

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix}$$

Let $\phi \in [0, 2\pi)$, so that $(\cos(\phi), \sin(\phi))^T$ is an arbitrary point on the unit circle. Then I can reach $(\cos(\phi), \sin(\phi))^T$ by letting $\theta = \phi$. Hence $U = \text{orb}(1, 0)^T$.

That is, U is transitive (or homogeneous) in both SO_2 and O_2. We'll show that U is free in SO_2, but not in O_2. Let $(\cos(\phi), \sin(\phi))^T \in U$ and consider an element of SO_2 acting on this element of U:

$$r(\theta)(\cos(\phi), \sin(\phi))^T = \begin{bmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi \\ \sin\theta\cos\phi + \cos\theta\sin\phi \end{bmatrix} = \begin{bmatrix} \cos(\theta + \phi) \\ \sin(\theta + \phi) \end{bmatrix}.$$

Hence $r(\theta)(\cos(\phi), \sin(\phi))^T = (\cos(\phi), \sin(\phi))^T$ if and only if

$$\begin{bmatrix} \cos(\theta + \phi) \\ \sin(\theta + \phi) \end{bmatrix} = \begin{bmatrix} \cos(\phi) \\ \sin(\phi) \end{bmatrix}.$$

This would imply that $\theta \equiv 0 \mod 2\pi$, hence if $\theta \in [0, 2\pi)$, we must have $\theta = 0$. So $(SO_2)_{(x,y)} = \{e\}$ (The stabilizer of (x, y)) for any $(x, y) \in U$, so U is free in SO_2.

Now consider the point $(0, 1)$ and let $s(\pi)$ act on this point:

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Hence $s(\pi) \in (SO_2)_{(0,1)} \neq \{e\}$. So that U is not free in O_2.

That is U is a P.H.S in SO_2, but not O_2. □

Homework 4

2. We have seen that S_4 acts on the cube via its four diagonals.

   (a) Find a Sylow 2−subgroup of S_4 by stabilizing a square within the circle (a "substructure").

   (b) Use orbit-stabilizer theorem to find a collection of conjugate Sylow 2−subgroups, and use 3rd Sylow theorem to show you have them all.

   (c) Repeat for the Sylow 3−subgroups.

Solution. (a) Define a set of substructures on the cube, as bisecting squares of the cube. See the attached image.

By rotations of a dice, we see that the stabilizer of this is:

$$C_{yellow} = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}.$$

This has 8 elements, so is maximal in $S_4 = 2^3 3$ and hence a Sylow 2−subgroup.

(b) We can use the orbit stabilizer theorem to obtain the rest of the 2−Sylow Subgroups of S_4, via acting on the square from (a.). By acting on the square with (1 2 4 3) we obtain the green square in the attached sheet. So we may conclude:

$$C_{green} = (1\,2\,4\,3)C_{yellow}(1\,2\,4\,3)^{-1} = \{(1), (1\,3)(2\,4), (1\,3), (2\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,2\,3\,4), (1$$

We have accounted for 16 elements in S_4, the final one can be accounted for by a reflection of (1 4 3 2) giving us the last square:

$$C_{green2} = (1\ 4\ 3\ 2)C_{yellow}(1\ 4\ 3\ 2)^{-1}.$$

We can use Sylow III and Sylow II to determine if these are all of them. Note that all Sylow 2-subgroups are conjugate and in particular, we know that $n_2 \big| 3$, so that either $n_2 = 1$ or $n_2 = 3$. Since we don't have a trivial action, so that $n_2 \neq 1$. Hence $n_2 = 3$, and we have found all possible conjugate substructures.

(c) Finally, we'll use the diagonals of the labeled in the image attached. We see that $C_{Diagonal1} == \{(1), (2\ 3\ 4), (2\ 4\ 3)\}$ is the stabilizer of the diagonal labeled 1. This has 3 elements hence, this is the maximal 3-group in S_4 hence $C_{Diagonal1}$ must be a 3−Sylow subgroup of S_4.

Next we act on $C_{Diagonal1}$ via rotations we will end up with the 3 other substructures:

$$C_{Diagonal2} = (1\ 2)C_{Diagonal1}(1\ 2)^{-1}$$
$$C_{Diagonal3} = (1\ 3)C_{Diagonal1}(1\ 3)^{-1}$$
$$C_{Diagonal4} = (1\ 4)C_{Diagonal1}(1\ 4)^{-1}.$$

Homework 4

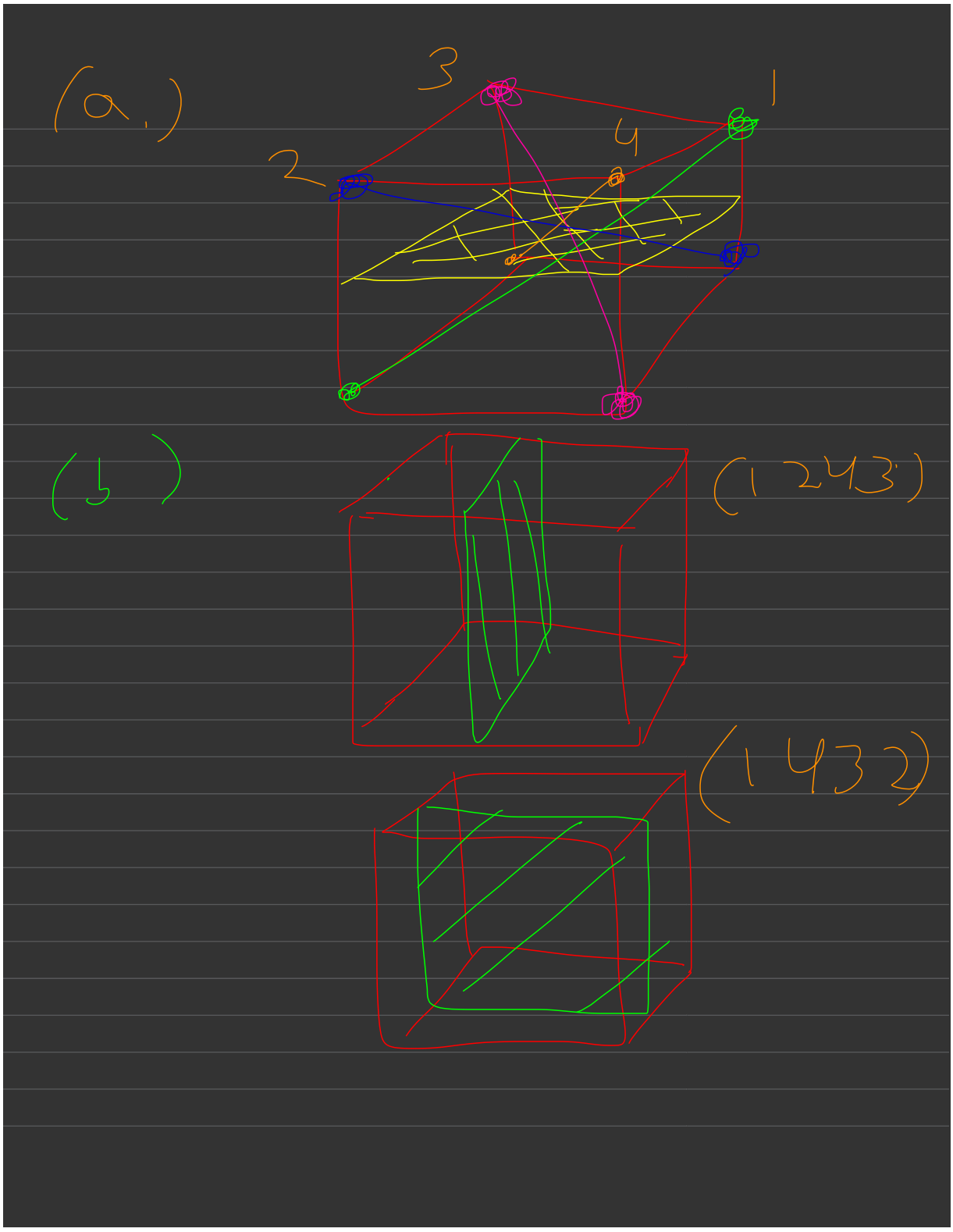


Figure 4: For Problem 2

Homework 4

To show these are all possible, note that Sylow III gives us that $n_3 \mid 8$, so that either $n_3 = 1, 2, 4$, or 8. We've seen that this is not a trivial action, so that $n_3 \neq 3$ Then we can rule out $n_3 = 8$ and $n_3 = 2$ since we must simultaneously have $n_3 \equiv 1 \mod 3$, so $n_3 = 1, 4, 7$, by Sylow III. This gives us $n_3 = 4$. So we have found all possible substructures and all $3-$Sylow subgroups.

□

Homework 4

3. Let G be a finite group, p be a prime dividing $|G|$, and $P \in Syl_P(G)$. Prove that if $N \lhd G$ is a normal subgroup, then $P \cap N$ is a $p-$Sylow subgroup of N.

   Proof. Let G be a finite group, and p be a prime divisor of $|G|$, so that $|G| = mp^n$, with $\gcd(p, m) = 1$, with $P \in Syl_p(G)$.

   Since $P \cap N \leq P$, we have that $|P \cap N| \Big| p^n$. Hence $|P \cap N| = p^k$, for some $0 \leq k \leq n$. Then since $N \lhd G$ we have that $PN \leq G$, with:

$$|PN| = \frac{|P||N|}{|P \cap N|} = p^{n-k}|N|.$$

   Furthermore, since $P \cap N \leq N$, we have that $p^k \Big| |N|$. That is, $|N| = p^k a$ but that would imply:

$$|PN| = p^n a,$$

   so that $a \Big| m$ and $\gcd(a, p) = 1$. But note that we must have $p \not| m$. So combining our work we have:

$$\frac{|PN|}{|P|} = \frac{|N|}{|P \cap N|} = a,$$

   where $\gcd(a, p) = 1$. So that $[N : P \cap N] = a$. This implies that $P \cap N$ is a $p-$Sylow subgroup of N, since $P \cap N$ is of prime-power order and $\gcd(a, p) = 1$. □

Homework 4

4. Let G be a group of order p^2q, where p and q are distinct primes. Prove that either a $p-$Sylow subgroup or a $q-$Sylow subgroup are normal in G.

Proof. Let G be a finite group, and p and q be distinct primes. Suppose $|G| = p^2q$. Note that by Sylow 3 we have $n_p = |Syl_P(G)| = [G : N_G(P)]$, where $P \in Syl_Q(G)$, and similarly $n_q = |Syl_Q(G)| = [G : N_G(Q)]$, where $Q \in Syl_Q(G)$. So that if $n_q = 1$ or $n_p = 1$, we must have $G = N_G(Q)$ or $G = N_G(P)$, respectively. That is, our result is equivalent to showing either $n_q = 1$ or $n_p = 1$.

By Sylow 3, we also have that n_p divides $[G : P] = q$, where $P \in Syl_P(G)$, so either $n_p = 1$ or q.

If $n_p = 1$, we're done. If $n_p = q$, then let's examine n_q: By Sylow 3 n_q must divide $[G : Q] = p^2$, where $Q \in Syl_Q(G)$, that is, $n_q = 1$ or p or p^2.

If $n_q = 1$, we're done. If $n_q = p$, then by Sylow 3, we have $p \equiv 1 \mod q$ and $q \equiv 1 \mod p$. So that for some $m, k \in \mathbb{Z}^+$, $p = 1 + qk$ and $q = 1 + pm$. So that implies $m = \dfrac{q-1}{p}$ and $k = \dfrac{p-1}{q}$. So with $m, k \in \mathbb{Z}$, this requires that $q-1 \geq p$ and $p-1 \geq q$, hence $q \geq p+1$, but that implies $p - 1 \geq q \geq p + 1$ or $p - 1 \geq p + 1 \implies -1 \geq 1$, a contradiction. Hence $n_q \neq p$. Similarly, suppose $n_q = p^2$, then we'll arrive at $p^2 \equiv 1 \mod q$ and $q \equiv 1 \mod p$. So note that

$$p^2 - 1 \equiv 0 \mod q \iff (p-1)(p+1) \equiv 0 \mod q,$$

so since $\mathbb{Z}_q$ is an integral domain, we have that either $p \equiv 1 \mod q$, in which case we've shown that leads to a contradiction. So suppose $p \equiv -1 \mod q$ and $q \equiv 1 \mod p$. So that $p + 1 = qk$ and $q - 1 = pm$, for some $k, m \in \mathbb{Z}$. Then this requires that $p + 1 \geq q$ and $q - 1 \geq p$, so that $p + 1 \geq q$ and $q \geq p + 1$. So that $q = p + 1$, a contradiction unless $(p, q) = (2, 3)$.

Suppose $(p, q) = (2, 3)$ (hence $|G| = 12$). Then we $n_2|3$ and $n_3|4$, so $n_2 = 1$ or $n_2 = 3$ and $n_3 = 1, 2, 4$. Suppose $n_2 = 3$, then $n_3 = 4$ (as we have shown what occurs if $n_3 = 2$). So we have 8 elements of order 3, and up to 9 elements of order dividing 4, possibly less however. However, if $n_2 = 3$ then $Syl_2(G) = \{P_1, P_2, P_3\}$. So note that in the worst case scenario, we have $|P_1 \cap P_2| = |P_1 \cap P_3| = |P_2 \cap P_3| = 2$, so that we have only 6 elements of order dividing 4. A contradiction, that $|G| = 12$.

Hence either, $n_q = 1$ or $n_p = 1$, implying that either $P \in Syl_p(G)$ or $Q \in Syl_q(G)$ are normal. □

Homework 4

5. Let G be a group, p a prime dividing $|G|$.

   (a) Prove that there is a one-to-one correspondence between Sylow $p-$subgroups and normalizers of Sylow $p-$subgroups.

   (b) Prove $N(N(P)) = N(P)$ for any $P \in Syl_P(G)$. [Hint: Use orbit-stabilizer correspondence.]

   (a) *Proof.* Let G be a group, and p be a prime divisor of $|G|$ such that $|G| = p^n m$ and $\gcd(p, m) = 1$.

   Define a map $\phi : Syl_p(G) \to \{N_G(P) : P \text{ is a Sylow } p - \text{subgroup}\}$ by $\phi(P) = N_G(P)$. To show this is a well-defined map, clearly if $P = P'$, then $N_G(P) = N_G(P')$, so $\phi(P)$ is a well-defined map.

   By the definition of our codomain, we have that ϕ is surjective.

   To show that ϕ is injective, let $P, P' \in Syl_p(G)$ and suppose $N_G(P) = N_G(P')$. Then $P \lhd N_G(P)$ and $P' \lhd N_G(P')$, so that $P'P \lhd N_G(P) \leq G$. Note that $|P| = |P'| = p^n$, and that $P \cap P' \leq P$ (and P'), so that $|P \cap P'| = p^k$, where $0 \leq k \leq n$. Hence

   $$|PP'| = \frac{|P||P'|}{|P \cap P'|} = p^{2n-k}.$$

   Moreover, we need $p^{2n-k} | p^n$, since $PP' \leq G$. This implies that $2n - k \leq n$, so that $n \leq k$. However, we need $0 \leq k \leq n$. So that $n = k$, and hence $|P \cap P'| = p^n$. Since both $|P| = |P'| = p^n$, we must have that $P \cap P' = P = P'$.

   Thus ϕ is injective and ϕ is $1 - 1$ correspondence. □

   (b) *Proof.* Let G be a group, and p a prime divisor of $|G|$ with $|G| = p^n m$ such that $\gcd(p, m) = 1$. Let $P \in Syl_p(G)$.

   For any group we have $G \subseteq N(G)$, so that with $G = N(P)$ we have:

   $$N(P) \subseteq N(N(P)).$$

   Conversely, let $A \in N(N(P))$. Then, by definition, $A(N(P))A^{-1} = N(P)$. So since $P \subseteq N(P)$, we have $APA^{-1} \subseteq AN(P)A^{-1} = N(P)$. Furthermore, note that APA^{-1} is the same order as P, since conjugation doesn't change order. Hence $APA^{-1} \leq N(P)$ and $P \lhd N(P)$, So using the method from the proof of (a.), note that $P(APA^{-1}) \leq N_G(P) \leq G$. That is, $|P| = |APA^{-1}| = p^n$ and that $P \cap APA^{-1} \leq P$ (and of APA^{-1}) so that $|P \cap APA^{-1}| = p^k$, where $0 \leq k \leq n$. Then

   $$|P(APA^{-1})| = \frac{|P||APA^{-1}|}{|P \cap APA^{-1}|} = p^{2n-k}.$$

So that $p^{2n-k}|p^n$, since $P(APA^{-1}) \leq G$. So that $2n - k \leq n$, hence $n \leq k$. Implying that $k = n$. Whence $P = APA^{-1}$. Giving us the desired result that $A \in N(P)$.

So we have $N(N(P)) = N(P)$ for any $P \in Syl_G(P)$. □

Homework 4

6. Classify groups of order 30, by showing there's a normal subgroup of order 15, and using product construction.

Proof. Let G be a finite group with $|G| = 30$. Then by Sylow III, we know that:

$$|Syl_2(G)| = n_2 \equiv 1 \mod 2 \qquad \text{and} \qquad n_2|15.$$

Implying that $n_2 = 1, 3, 5, 15$. Similarly, we'll have that

$$|Syl_3(G)| = n_3 \equiv 1 \mod 3 \qquad \text{and} \qquad n_3|10,$$

so that $n_3 = 1, 10$. And finally,

$$|Syl_5(G)| = n_5 \equiv 1 \mod 5 \qquad \text{and} \qquad n_5|6,$$

so that $n_5 = 1, 6$. This gives us exactly 16 ordered pairs of (n_2, n_3, n_5). However, we may rule out:

$$\begin{gathered}(1, 10, 6)\\(3, 10, 6)\\(5, 1, 6)\\(5, 10, 6)\\(15, 10, 1)\\(15, 1, 6)\\(15, 10, 6),\end{gathered}$$

since this gives us too many elements of differing order; for example with $(n_2, n_3, n_5) = (15, 10, 1)$ would have 15 elements of order 2, 20 of order 3, so that this is a contradiction of $|G| = 30$. So this leads us to the following possibilities:

$$\begin{gathered}(1, 1, 1)\\(1, 10, 1)\\(1, 1, 6)\\(3, 1, 1)\\(3, 10, 1)\\(3, 1, 6)\\(5, 1, 1)\\(5, 10, 1)\\(15, 1, 1).\end{gathered}$$

Notice that leads to either $n_3 = 1$ or $n_5 = 1$, implying that $[G : N(P_3)] = 1$ or $[G : N(P_5)] = 1$, where $P_3 \in Syl_3(G)$ and $P_5 \in Syl_5(G)$. Hence either P_3 or P_5 are normal in G.

So then we have $P_3P_5 \leq G$. Moreover, $P_3 \cap P_5 = \{e\}$, since $g \in P_3 \cap P_5$ must have order dividing 3 and 5. Hence $|P_3P_5| = \dfrac{|P_3||P_5|}{|P_3 \cap P_5|} = 15$, so that $[G : P_3P_5] = 2$ hence P_3P_5 is normal in G. Moreover, note that $|P_3P_5| = 3 \cdot 5$, by 2.16 in $IV.2$ of Aloffi (p.201) we have that P_3P_5 is cyclic in G, so let: $\langle x \rangle = P_3P_5$. So that $\langle x \rangle \lhd G$.

Note that $\langle x \rangle \cap P_2 = \{e\}$, since $\gcd(2, 15) = 1$. Finally then $\langle x \rangle P_2 = G$, since $\langle x \rangle P_2 = \dfrac{|\langle x \rangle||P_2|}{|\{e\}|} = 15 \cdot 2 = 30$. Hence by Handout 4, we have that $G \simeq \langle x \rangle \rtimes_\gamma P_2$, where $\gamma : P_2 \to \text{Aut}\langle x \rangle$ and γ is the adjoint action on G.

Note γ is a homomorphism, $|\gamma(a)|$ divides $|a| = 2$, where $P_2 = \langle a \rangle$. Moreover, for $\gamma(a)$ to be an automorphism on P_3P_5 we need $\gamma(a) \in U(15)$, i.e $\gamma(a) = j$ where $\gcd(j, 15) = 1$. So that $j \in \{1, 2, 4, 7, 8, 11, 14\}$. But since $|\gamma(a)|$ divides 2, this implies that $j = 1, 4, 11, 14$. Hence $\phi(a)(x) = axa^{-1} = x^j$. So we have 4 groups of order 30 with conjugation defined by:

$$axa^{-1} = x^j,$$

where $j = 1, 4, 11, 14$.

Finally, call these respective groups

(a) $G_1 \simeq P_2 \rtimes_\gamma N$ with $\gamma(a)(x) = axa^{-1} = x$

(b) $G_2 \simeq P_2 \rtimes_\gamma N$ with $\gamma(a)(x) = axa^{-1} = x^4$

(c) $G_3 \simeq P_2 \rtimes_\gamma N$ with $\gamma(a)(x) = axa^{-1} = x^{-4}$

(d) $G_4 \simeq P_2 \rtimes_\gamma N$ with $\gamma(a)(x) = axa^{-1} = x^{-1}$

So notice that for G_1, the relation $axa^{-1} = x$ implies $ax = xa$. So that $(ax)^j = (xa)^j \iff a^jx^j = x^ja^j$, implying that G_1 is Abelian. With G_2, G_3, G_4 are all non-Abelian since conjugation should be the trivial map under an Abelian group.

Note that with G_4, we have that $|x| = 15, |a| = 2$ and $axa^{-1} = x^{-1}$ is exactly the defining relations of D_{15}, so that $G_4 \simeq D_{15}$. Moreover we have that $\phi \in \text{aut}(D_n) \iff \phi(x) = x^\alpha$ and $\phi(a) = ax^\beta$, where $\gcd(\alpha, n) = 1$. Implying that G_2 and G_3 are not isomorphic to D_{15}.

Finally, the conjugation rules of G_2 and G_3 make them incompatible since we have for G_2: $x = ax^4a^{-1}$ and $x = ax^{11}a^{-1}$ in G_3. That imply that $x^4 = x^{11}$ so that $x^7 = e$ and so $|x| = 7$, a contradiction of Lagrange's Theorem. $\square$

Homework 4

7. Determine all groups of order 12.

Proof. Let G be a group and $|G| = 12 = 2^2 \cdot 3$. Then by Problem 4 on this homework, we have that there's either a $P_2 \in Syl_2(G)$ or $P_3 \in Syl_3(G)$ that is normal in G. Note that $P_2 \cap P_3 = \{e\}$ since $\gcd(2,3) = 1$ and $\gcd(4,3) = 1$. And that $P_2P_3 \leq G$, since either P_2 or P_3 is normal. Finally, $|P_2P_3| = \dfrac{|P_2||P_3|}{|P_2 \cap P_3|} = 4 \times 3 = 12$, so that $P_2P_3 = G$.

So consider the following cases:

(a) Suppose $P_2 \lhd G$. Then $G \simeq P_2 \rtimes_\gamma P_3$ where $\gamma : P_3 \to \text{aut}(P_2)$. So note since $|P_3| = 3$ we have $P_3 \simeq \mathbb{Z}_3$ so that for some $x \in P_3$, $\langle x \rangle = P_3$. Hence $|\gamma(x)| \Big| |x| = 3$, so that $|\gamma(x)| = 1$ or 3.

Note that there are only 2 groups of order 4, $\mathbb{Z}_4$ and K_4 (the Klein 4−group). So that either P_2 is either cyclic or not.

i. Suppose P_2 is cyclic, so that $P_2 \simeq \mathbb{Z}_4$. Then there's a $a \in P_2$ such that $\langle a \rangle = P_2$ with $|a| = 4$. So that $\gamma(x)(a) = xax^{-1} = x^j$ with $j \in U(4) = \{1, -1\}$.
If $j = 1$, then $\gamma(x) = 1$ and $\gamma(x)(a) = a$ is the trivial map. So that $\gamma(x)(\mathbb{Z}_4) = x\mathbb{Z}_4x^{-1} = \mathbb{Z}_4$, hence $\mathbb{Z}_4$ is normal in G. So by Prop.1.1 on Handout 1, that gives us $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3$.
If $j = 3$, then $|\gamma(x)| = 2$ but since $\langle x \rangle = \mathbb{Z}_3$ it must be that $|x| = 3$, so that $|\gamma(x)| = 2 \Big| 3$, a contradiction. Hence $j \neq 3$.

ii. Suppose P_2 is not cyclic, so that since we know there are only 2 groups of order 4, and we've accounted for $\mathbb{Z}_4$, it follows that $P_2 \simeq K_4$. We know K_4 is not cyclic, but it is Abelian. Moreover, note that $K_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and we'll show that $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) = S_3$.
So we have that $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\} = \langle (0,1),(1,0) \rangle$. So that any $\phi \in \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is determined by $(0,1)$ and $(1,0)$. We must have $\phi(0,0) = (0,0)$, so that label $1 : (0,1)$, $2 : (1,0)$ and $3 : (1,1)$. Hence $\phi(1,0) = (1,0)$ or $(0,1)$ or $(1,1)$ and $\phi(0,1) = (0,1)$ or $(1,0)$ or $(1,1)$. If $\phi(1,0) = (1,0)$ and $\phi(0,1) = (0,1)$, then that corresponds to the identity map (1). Fixing $\phi(1,0) = (1,0)$ and letting $\phi(0,1) = (1,1)$ will give us (1 3). Similarly we obtain (2 3) and (1 2). To obtain the three-cycles, we let $\phi(1,0) = (1,1)$ and $\phi(0,1) = (1,0)$ so that this corresponds to (1 2 3), similarly we obtain (1 3 2). Hence $\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$.
That means the inner automorphism on G is: $\gamma : \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$. So that we have 6 choices for the generator of $\mathbb{Z}_3$ to get sent to, however, we can rule out some elements of S_3 as we need $|\gamma(x)| = 1$ or 3. Note that $|(1\ 2)| = |(2\ 3)| = |(1\ 3)| = 2$ are all impossibilities, that leaves us with 3 choices $(1), (1\ 2\ 3)$, and $(1\ 3\ 2)$.

If $\gamma(x) = (1)$, then $\gamma(x)$ is the trivial map so that:

$$\gamma(x)(K_4) = xK_4x^{-1} = K_4,$$

giving us that $K_4 \lhd G$. Hence we have $K_4 \times \mathbb{Z}_3 \simeq G$ or equivalently $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq G$. That is G is a finite Abelian, non-cyclic group.
If $\gamma(x) = (1\,2\,3)$ so that $|\gamma(x)| = 3$. However, note that since $(2\,3)(1\,2\,3)(2\,3) = (1\,3\,2)$ so that sending $\gamma(x) = (1\,3\,2)$ is an isomorphic map, since conjugation is an automorphism on S_3. That is, that $\gamma(x) = (1\ 2\ 3)$ and $\gamma(x) = (1\ 3\ 2)$ define the same group up to isomorphism.
So note that by assumption we have $K_4 \lhd G$ and by our preliminary argument that $K_4P_3 = G$ and $K_4 \cap P_3 = \{e\}$. So that by the semi-direct product handout we have $K_4 \rtimes_\gamma P_3 \simeq G$ where $\gamma : P_3 \to \mathrm{Aut}(K_4)$. Moreover, by using the definition of $\gamma(a)$ in K_4 we have that P_3 is not a normal subgroup in G; that is using our labeling of $1 : (0,1), 2 : (1,0), 3 : (1,1)$ we see that conjugation on P_3 is not the trivial action under $\gamma(a)$.
Moreover, note that $\langle(1\,2\,3)\rangle \simeq P_3$ and $K_4 \simeq \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,4)\} \lhd A_4$ (as shown in HW 1). So we have $K_4 \rtimes_\gamma P_3 \simeq K \rtimes_\gamma \langle(1\ 2\ 3)\rangle \simeq A_4$, (where the last $\simeq$ holds by the semi-direct handout).

(b) Suppose $P_3 \lhd G$.

Then by Semi-Direct product handout, we have that $P_3 \rtimes_\gamma P_2 \simeq G$ and $\gamma : P_2 \to \mathrm{Aut}(P_3) = U(3) = \{1, 2\}$.

If γ is the trivial map, that is we have that for all $x \in P_2$ and $y \in P_3$ that $xyx^{-1} = y$ hence $xy = yx$. So that $xP_3x^{-1} = P_3$ for all $x \in P_2$ hence $P_3 \lhd G$ so that this is $P_3 \times P_2 \simeq G$, in direct product so that $G \simeq \mathbb{Z}_{12}$.

Suppose $P_2 = \langle x\rangle$ for some $x \in P_2$. Then we have that $\gamma(x)$ determines the map. Suppose $\gamma(a) = 2$, then $axa^{-1} = x^2$ where $|a| = 3$ and $|x| = 4$. That is all we know about this group, call it G_1:

$$G_1 \simeq P_3 \rtimes_\gamma P_2 = \langle a, x : |x| = 3, |a| = 4, axa^{-1} = x^2\rangle.$$

Suppose P_2 is not cyclic. Since $|P_2| = 4$, this implies that $P_2 \simeq K_4 \simeq \langle(1,0),(0,1)\rangle$. So then we have our action is a map $\gamma : K_4 \to \mathrm{Aut}(\mathbb{Z}_3) = U(3)$. So a homomorphism from K_4 to $U(3) = \{1, 2\}$, since $K_4 \simeq \langle(1,0),(0,1)\rangle$, γ is completely determined by where $(1,0)$ and $(0,1)$ are sent in $U(3) = \{1, 2\}$.

We have 3 possibilities (we have already considered the trivial map):

$$\gamma(1,0) = 2 \qquad \gamma(0,1) = 1 \tag{2}$$
$$\gamma(1,0) = 1 \qquad \gamma(0,1) = 2 \tag{3}$$
$$\gamma(1,0) = 2 \qquad \gamma(0,1) = 2 \tag{4}$$

Homework 4

So all three of the groups defined by the 3 relations above, give us the same relations: $axa^{-1} = x^{-1}$ where $|x| = 3$ and $|a| = 2$. That is all the groups defined by the 3 possibilities are D_3.

We have covered every possible case of P_2 and P_3 giving us 5 groups:

(a) D_3

(b) A_4

(c) $G_1 = \langle a, x : |x| = 3, |a| = 4, axa^{-1} = x^2 \rangle$

(d) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

(e) $\mathbb{Z}_6 \times \mathbb{Z}_2$

Note that (d) and (e) are Abelian, and that (e) is cyclic and (d) isn't so they are not isomorphic. For the 3 non-abelian groups, note there is a $x \in G_1$ that is order 4, but that D_3 and A_3 have only elements of order 3 and 2. Finally A_4 has $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$, 6 elements of order 2, while D_3 has 3 elements of order 2. □

Homework 4

8. Let P be a p-Sylow subgroup of G, and suppose $H \leq G$ contains $N(P)$. Prove that $N(H) = H$.

Proof. Let P be a $p-$Sylow subgroup of G. Suppose $H \leq G$ and $N(P) \subseteq H$.

$(\supseteq)$

Let $h \in H$. Then $hH = Hh = H$ implies $hHh^{-1} = H$. So that $h \in N(H)$.

$(\subseteq)$

Let $h \in N(H)$. Then $hHh^{-1} = H$. Note that $P \leq N(P) \subseteq H \leq G$. So since $N(P) \leq G$, we have $N(P) \leq H$. Additionally since $P \leq H$, we have $hPh^{-1} \leq hHh^{-1} = H$. So that $hPh^{-1} \leq H$ and $|hPh^{-1}| = |P|$. By Sylow II., we know there must be a $x \in H$ such that $xPx^{-1} = hPh^{-1}$; that is, $P = x^{-1}hP(x^{-1}h)^{-1}$. So that $x^{-1}h \in N(P)$ and hence $x^{-1}h \in H$. Finally, since $x^{-1} \in H$, we have that $h \in xH = H$ so that $h \in H$.

Thus $H = N(H)$ as required. □

Homework 4

9. Prove that if G is a simple group of order 60, then $G \simeq A_5$. [Hint: See Aluffi's hints on p.205]

Proof. Let G be a simple group of order 60. So let $n_2 = |Syl_2(G)|, n_3 = |Syl_3(G)|, n_5 = |Syl_5(G)|$. So that by Sylow III. we have that $n_2 \equiv 1 \mod 2$ and $n_2|30$, so that $n_2 = 1, 3, 5, 15$, similarly $n_3 \equiv 1 \mod 3$ and $n_3|20$ hence $n_3 = 1, 4, 10$, and finally $n_5 = 1, 6$. Note that any of these equaling 1 can be ruled out since this would imply we have a non-trivial normal subgroup of G. So we have $n_2 = 3, 5, 15$, $n_3 = 4, 10$ and $n_5 = 6$.

Suppose $n_2 = 3$, then by Generalized Cayley's Theorem that would imply there exists a non-trivial homomorphism $\phi : G \to S_3$. However, since G is a simple group that implies that $\ker(\phi) = \{e\}$, hence ϕ is a $1-1$ function from G to S_3. This is a contradiction since $|G| = 60$ and $|S_3| = 6$.

So that implies that $n_2 = 5, 15$. If $n_2 = 5$, then $[G : N_{P_2}(G)] = 5$. Suppose $n_2 = 15$. Then there are $P_1, P_2, \ldots, P_{15}$ groups of order 4 this gives us that there are 45 elements of order 2 or 4 and since $n_3 = 4$ we must have 8 elements of order 3 and since $n_5 = 6$ there must be 24 elements of order 5. Since $|G| = 60$, we must have overlap between P_i and P_j, for some $j, i \in \{1, \ldots, 15\}$, that is there exists at $g \in P_i \cap P_j$ such that $|g| = 2$ or 4, we can rule out 4 since this would imply that $P_i = P_j$. So we have $g \in P_i \cap P_j$ and $|g| = 2$.

Note that $P_i, P_j \simeq K_4$ or $\mathbb{Z}_4$, since there are only two groups of order 4. Moreover, note that both K_4 and $\mathbb{Z}_4$ are Abelian. So since $g \in P_i \cap P_j$ and $g \in N_G(g) = \{a : aga^{-1} = g\}$ hence $N_G(g)$ has a subgroup of order 4 and $|N_G(g)| \geq 6$ since $P_i \neq P_j$ and both are abelian hence all elements in $P_i \cup P_j$ commute with g.

So that $4||N_G(g)|$ and $|N_G(g)||60$. So $|N_G(g)|$ divides $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$. So $|N_G(g)| = 12, 20$. Suppose $|N_G(g)| = 20$, then $[G : N_G(g)] = 3$. However, by the important source of homomorphisms this implies there's a non-trivial homomorphism from G to S_3. However, since G is simple this implies that the kernel of this homomorphism is $\{e\}$ so that the homomorphism is injective from G to S_3. An impossibility since $|G| = 60$ and $|S_3| = 6$. Implying that $|N_G(g)| \neq 20$. Thus $[G : N_G(g)] = \dfrac{60}{12} = 5$. So by the important source of homomorphisms we have there exists a non-trivial $\phi : G \to S_5$. So that since G is simple this implies that $\ker(\phi) = \{e\}$, so that $G/\ker(\phi) \simeq G$. Hence by the first isomorphism theorem, we have that $G \simeq \phi(G)$.

But note that $|\phi(G)| = 60$ and $\phi(G) \leq S_5$.

Finally, note that $A_5 \lhd S_5$. Suppose $H \neq A_5$ and $H \leq S_5$ and $|H| = 60$. Then $[S_5 : H] = 2$, so that H is normal in S_5 and so must be the union of conjugacy classes in S_5. We know the conjugacy classes of S_5 are as follows (The size of the conjugacy

Homework 4

class and representative element):

1	(1)
10	(1 2)
20	(1 2 3)
15	(1 2)(3 4)
30	(1 2 3 4)
20	(1 2)(3 4 5)
24	(1 2 3 4 5)

Let's construct H and see the possibilities: Note then $(1) \in H$ so that we must have $[(1\ 2)(3\ 4)] \subseteq H$, since we need to reach an even number 60. So that we have 16 elements now, we need to include $[(1\ 2\ 3\ 4\ 5)] \subseteq H$ so now we have 40 elements of H. So to reach 60 we can either choose to include $[(1\ 2\ 3)]$ or $[(1\ 2)(3\ 4\ 5)]$, the first gives us A_5 so we'll consider if $(1\ 2)(3\ 4\ 5) \in H$. Since H is a subgroup, we must have:

$$(1\ 2)(3\ 4\ 5) \circ (1\ 2)(3\ 4\ 5) = (3\ 5\ 4) \in H.$$

That would imply that $[(3\ 5\ 4)] \subseteq H$, a contradiction that $H \neq A_5$.

So the only subgroup of order 60 in S_5 is A_5. Hence $G \simeq A_5$. □

Name: Joseph McGuire
Instructor: Eric Brussel

HW 5

Math 561 (Fall 2021)

1. Let $(S, \leq)$ be a partially ordered set. Make it into a category, verifying the definition.

   Proof. Let C be the resulting category that we will now construct.

   - $\text{Obj}(C) = \mathbb{Z}$
   - Then let $\text{Hom}_C(A, B) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \leq b\}$.

   We'll show this satisfies the necessary conditions of a morphism:

   (a) (Identity on Objects) Let $a \in \mathbb{Z}$. Then $(a, a) \in \text{Hom}_C(A, A)$ since $a \leq a$ for any $a \in \mathbb{Z}$. Thus $(a, a) = 1_a$ is our identity for each $a \in \mathbb{Z}$.

   (b) (Composition) Let $a, b, c \in \mathbb{Z}$ and morphisms

   $$f \in \text{Hom}(a, b) \qquad g \in \text{Hom}(b, c).$$

   Then we'll define:

   $$fg = (a, c)$$

   where we obtain this by $a \leq b$ and $b \leq c$ implying $a \leq c$. So $fg \in \text{Hom}(a, c)$, as needed.

   (c) (Associativity) Let $a, b, c \in \mathbb{Z}$. So that (ab) gives $a \leq b$ and so (bc) gives $b \leq c$ so that:

   $$(ab)c = a \leq c = a(bc).$$

   (d) (Identity of Compositions) Let $f \in \text{Hom}(A, B)$ for some $A, B \in \mathbb{Z}$. Then define 1_A to be given by $A \leq A$ and 1_B to be the given by $B \leq B$. Hence $f1_A = A \leq A \leq B = A \leq B = f$ and $1_B f = A \leq B \leq B = A \leq B = f$. As required.

   Hence $a \xrightarrow{\phi} b$ only if $a \leq b$ defines a morphism on $\mathbb{Z}$. □

HW 5

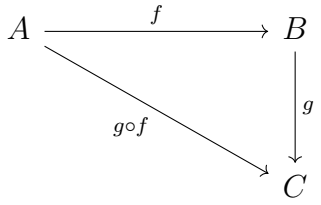
2. Let $\mathbf{Set}_*$be the collection of pairs (A, X), where A is a set and $X \subset A$ is a subset, with functions $(A, X) \to (B, Y)$ consisting of set maps $A \to B$ taking X into Y. Show $\mathbf{Set}_*$ is a category.

   Proof. Define the class $\mathbf{Set}_*$ as we have in the problem statement. Let C be the category in which we're constructing.

   - Let $Obj(C) = \mathbf{Set}_*$
   - Let $Mor_C((A, X), (B, Y))$ to be functions $(A, X) \to (B, Y)$ where $f : A \to B$ and $f|_X : X \to Y$.

   (a) (Identity on Objects) Let $(A, X), (B, Y)$ be objects in C. Then define the function $f : A \to A$ to be the identity map, $f(x) = x$ for all $x \in A$. Clearly, this send X to X since $X \subseteq A$, so we have $f = id_{(A,X)} \in \mathrm{Hom}_C((A, X), (A, X))$.

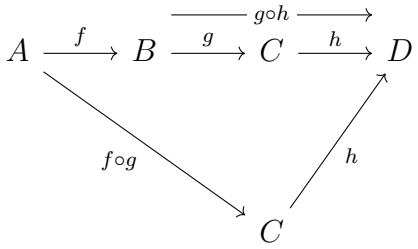
   (b) (Composition)
   Let $(A, X), (B, Y), (C, Z)$ be objects in C, and $f \in \mathrm{Hom}_C((A, X), (B, Y)), g \in \mathrm{Hom}_C((B, Y), (C, Z))$. Then we'll define gf to be the set map $gf = g \circ f$. The diagrams commute, so gf is well-defined:

   Furthermore if $f|_X : X \to Y$ and $g|_Y : Y \to Z$, then $gf|_X : X \to Z$ as required. So our composition is defined, as required.

   (c) (Associativity) Let $(A, X), (B, Y), (C, Z), (D, W)$ be objects in C and $h \in \mathrm{Hom}_C((A, X), (B, Y))$ $\mathrm{Hom}_C((B, Y), (C, Z)), f \in \mathrm{Hom}_C((C, Z), (D, W))$. The following diagram com-

mutes



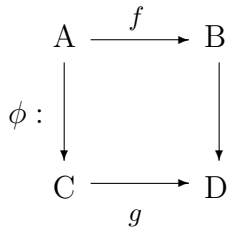
Hence we have associativity, as required.

(d) (Identity of Composition) Let $f \in \mathrm{Hom}((A, X), (B, X))$ and define the $id_{(A,X)} : A \to A$ to be the identity map on A and $id_{(B,X)} : B \to B$ to be the identity map on B. Giving us $fid_A = f$ and $id_B f = f$, as required.

So we have C is a category. □

HW 5

3. Let $\mathcal{C}$ be a category. Show that if we define the objects of $\mathbf{Mor}(\mathcal{C})$ to be morphisms in $\mathcal{C}$ and morphisms in $\mathbf{Mor}(\mathcal{C})$ to be commutative diagrams



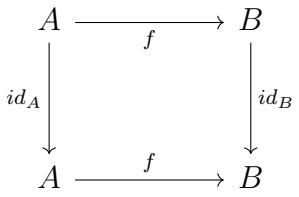
then $\mathbf{Mor}(\mathcal{C})$ is a category.

Proof. Let $\mathcal{C}$ be a category. Let $\mathbf{Mor}(\mathcal{C})$ be the morphisms of C.

- Let our objects be $\mathbf{Mor}(\mathcal{C})$
- Morphisms to be the commutative diagrams as shown above. That is $\phi \in \mathbf{Mor}(\mathcal{C})$ can be identified by ordered-pairs $\phi = (f, g) \in \hom_{\mathcal{C}}(A, B) \times \hom_{\mathcal{C}}(C, D)$, where their diagrams commute as seen above.

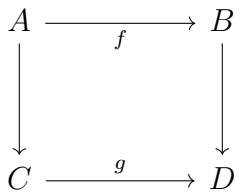
Now to show these morphisms satisfy the necessary conditions for morphisms:

(a) (Identity for Objects) Let $f \in \mathbf{Mor}(\mathcal{C})$ with $f \in \hom_{\mathcal{C}}(A, B)$. Then since $\mathcal{C}$ is a category, we have there exists $1_A \in \hom(A, A)$ and $1_B \in \hom(B, B)$. So we get the following diagram:



Call this morphism ϕ_f, hence $\phi_f \in \hom(f, f)$.

(b) (Composition)
Consider the morphisms in our category $\phi = (f, g)$ and $\psi = (g, h)$, so that their diagrams are:



and

$$\begin{array}{ccc} C & \xrightarrow[g]{} & D \\ \downarrow & & \downarrow \\ E & \xrightarrow{h} & F \end{array}$$

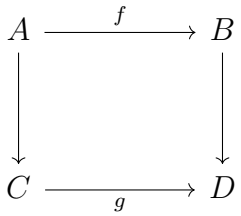
, respectively. So we define $\psi \circ \phi$ to be given by the following diagram:

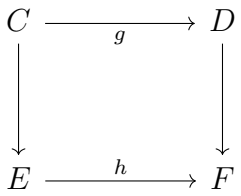
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ C & \xrightarrow[g]{} & D \\ \downarrow & & \downarrow \\ E & \xrightarrow{h} & F \end{array}$$

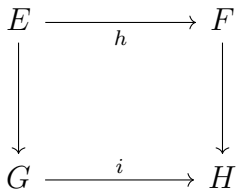
The diagram commutes, hence $\psi \circ \phi$ is defined as needed.

(c) (Associativity)
Consider morphisms ϕ, ψ, σ in our category with diagrams listed below (in their

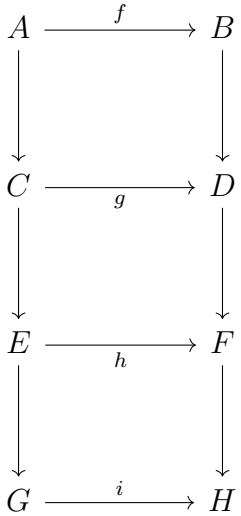
respective order):







Note that we may stack these with the identity morphism giving the following diagram:



This diagram commutes, hence we have $\sigma \circ (\psi \circ \phi) = (\sigma \circ \psi) \circ \phi$, as required.

(d) (Identity for Morphisms)
Let ϕ have the following diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ C & \xrightarrow[g]{} & D \end{array}$$

Then define the morphism 1_f by the following diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A & \xrightarrow[f]{} & B \end{array}$$

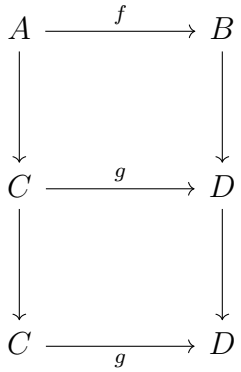
And define the morphism 1_g by the following diagram:

$$\begin{array}{ccc} C & \xrightarrow{g} & D \\ \downarrow & & \downarrow \\ C & \xrightarrow[g]{} & D \end{array}$$

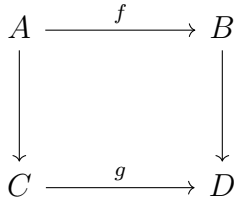
Hence we have $1_f \circ \phi$ has the following diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ A & \xrightarrow{f} & B \\ \downarrow & & \downarrow \\ C & \xrightarrow[g]{} & D \end{array}$$

And $\phi \circ 1_g$ has the following diagram:



Both of these diagrams 'collapse' to simply:



So that we have $\phi \circ 1_g = 1_f \circ \phi = \phi$ as required.

That is this definition of morphisms on our category is consistent with all the required properties, hence this is a category. □

HW 5

4. Let $\mathcal{C}$ be a category. An *initial object* in $\mathcal{C}$ is an object in I such that for any A in C, there's a unique morphism $i : I \to A$. Suppose I is an initial object. Show that I is unique up to isomorphism.

   Proof. Let $\mathcal{C}$ be a category. Let I_1 and I_2 be initial objects in $\mathcal{C}$.

   We have both I_1 and I_2 are initial, so we have that $\hom(I_1, I_1)$ is a singleton, and we know $1_{I_1} \in \hom(I_1, I_1)$, so that $\hom(I_1, I_1) = \{1_{I_1}\}$. Similarly, we have $\hom(I_2, I_2) = \{1_{I_2}\}$.

   Additionally, there must be a unique morphism $g : I_1 \to I_2$ and $f : I_2 \to I_1$. But note that since these are morphisms, we have their composition is defined and is a map such that $fg : I_1 \to I_1$. So since $\hom(I_1, I_1) = \{id_{I_1}\}$, we have $fg = id_{I_1}$. Similarly, we'll have $gf = id_{I_2}$. Hence $f : I_1 \to I_2$ and $g : I_2 \to I_1$ are isomorphisms between I_1 and I_2.

   Thus $I_1 \simeq I_2$. So there is only one initial object I (up to isomorphism) for each category $\mathcal{C}$. □

5. Identify the product and co-product of two objects in **Set**.

Proof. We'll show that products in **Set** are exactly Cartesian Products:

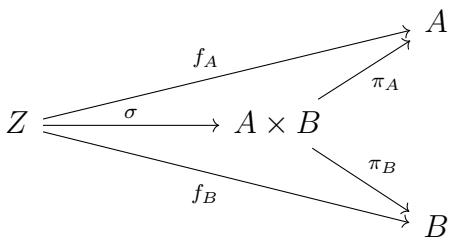
$$A \prod B = A \times B \qquad \text{for sets } A \text{ and } B$$

And that Disjoint Unions are exactly the coproducts of **Set**:

$$A \coprod B = A \sqcup B$$

(Products)

We'll need to show there exists a σ such that the following diagram commutes:



That is, for any set Z and set maps $f_A : Z \to A$ and $f_B : Z \to B$, and where $\pi_A : A \times B \to A$ is a projection on A and $\pi_B : A \times B \to B$ is a projection on B, there exists $\sigma : Z \to A \times B$ such that $f_A = \pi_A \circ \sigma$ and $f_B = \pi_B \circ \sigma$. That is, for every $z \in Z$, $f_A(z) = \pi_A(\sigma(z))$ and $f_B(z) = \pi_B(\sigma(z))$.

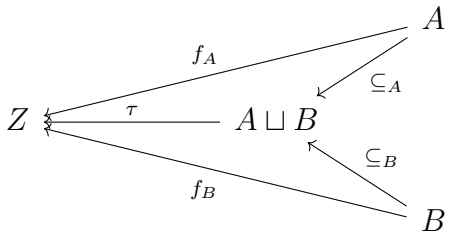
So we'll define $\sigma : Z \to A \times B$ such that $\sigma(z) = (f_A(z), f_B(z))$ for all $z \in Z$.

Then we'll have $\pi_A(\sigma(z)) = \pi_A((f_A(z), f_B(z)) = f_A(z)$ and $\pi_B(\sigma(z)) = \pi_B((f_A(z), f_B(z)) = f_B(z)$, for all $z \in Z$. So we have σ exists and that the diagram commutes.

Hence, for any sets A and B, $A \prod B = A \times B$.

(Co-products)

Similarly, for coproducts, we need to show for any set Z and set maps $f_A : A \to Z$ and $f_B : B \to Z$ there exists a map $\tau : A \sqcup B \to Z$ such that we have the following diagram:



Define $\subseteq_A : A \to A \sqcup B$ to be $\subseteq_A (a) = a$ for all $a \in A$ and similarly $\subseteq_B : B \to A \sqcup B$ to be $\subseteq_B (b) = b$ for all $b \in B$. So we need to show there exists a $\tau : A \sqcup B \to Z$ such that $\tau \circ \subseteq_A = f_A$ and $\tau \circ \subseteq_B = f_B$. So define $\tau : A \sqcup B \to Z$ by:

$$\tau(c) = \begin{cases} f_A(c) & \text{if } c \in A \\ f_B(c) & \text{if } c \in B. \end{cases}$$

This is well-defined, only because $A \cap B = \emptyset$. Additionally, we have for $a \in A$ that $\tau(\subseteq_A (a)) = \tau(a) = f_A(a)$. Similarly, for $b \in B$, we have $\tau(\subseteq_B (b)) = \tau(b) = f_B(b)$. Hence $\tau \circ \subseteq_A = f_A$ and $\tau \circ \subseteq_B = f_B$, as required.

Hence for sets A and B in **Set**:

$$A \coprod B = A \sqcup B \qquad A \prod B = A \times B.$$

□

Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 6

1. Let $I \subset R$ be an ideal, M is an $R-$Module. Prove $IM = \{\sum a_i m_i : a_i \in I, m_i \in M, \text{ finite sum}\}$ is a submodule of M.

   Proof. Let $I \subset R$ be an ideal and M be an $R-$Module and $IM = \{\sum a_i m_i : a_i \in I, m_i \in M, \text{finite sum}\}$.

   Since M is a module over R, it is stable under the ring action of R. That is $R \cdot M = M$ and so we must have $I \cdot M \subseteq M$, since $I \subset R$.

   Then to show the result, we'll need to show that $IM \leq (M, +)$ and that IM is stable under R-action's; that is, if $x, -y \in IM \implies x - y \in IM$ and $R \cdot IM = IM$.

   $(IM \leq (M, +))$

   Suppose $x, -y \in IM$, so that $x = a_1 m_1 + \ldots + a_n m_n$ and $y = b_1 n_1 + \ldots + b_k n_k$, where $m_i, n_i \in M$ and $a_i, b_j \in I$. So that since M is an R module, we have distributivity of scalars over sums and hence:

   $$-y = -b_1 n_1 - \ldots - b_k n_k.$$

   Since $I \subset R$ is an ideal of R, we have that $-I = I$, so that I contains all its negatives; that is if $b \in I$, then $-b \in I$. Then we'll have:

   $$x - y = a_1 m_1 + \ldots + a_n m_n - b_1 n_1 - \ldots - b_k n_k.$$

   So we me relabel this with $a_{n+1} = -b_1, a_{n+2} = -b_2, \ldots, a_{n+k} = -b_k$ and $m_{n+1} = n_1, \ldots, m_{n+k} = n_k$. So that we may write this as the re-indexed sum:

   $$x - y = \sum_{i=1}^{n+k} a_i m_i \in IR.$$

   Hence $IR \leq (M, +)$.

   $(R \cdot IR = IR)$

   Let $r \in R$ and $x \in IR$. Then there are $a_i \in I$ and $m_i \in M$ such that:

   $$x = \sum_{i=1}^{n} a_i m_i.$$

   So that:

   $$r \cdot x = r \cdot \sum_{i=1}^{n} a_i m_i = \sum_{i=1}^{n} r \cdot (a_i m_i) = \sum_{i=1}^{n} (r a_i) m_i,$$

   this follows by distributivity of scalars in M. So since $a_i \in I$ and $r \in R$, and we have $rI = I$ for all $r \in R$ since I is an ideal of R, we have $ra_i \in I$ for all $i \in \{1, \ldots, n\}$. Hence

Homework 6

$r \cdot x \in IR$. Thus $R \cdot IR \subseteq IR$. Conversely, we have that if $x \in IR$, then $x = \sum_{i=1}^{n} a_i m_i$ for $a_i \in I$ and $m_i \in M$. So that $1_R \cdot x = 1_R \cdot \sum_{i=1}^{n} a_i m_i = \sum_{i=1}^{n} (1_R a_i) m_i = x$. That is, $x \in R \cdot IR$.

Thus $R \cdot IR = IR$, and IR is stable under $R-$Action's.

Thus IR is a submodule of M. $\square$

Homework 6

2. If N is a submodule of M, the annihilator of N in R is $\text{Ann}_R(N) = \{r \in R : rn = 0 \forall n \in N\}$.

   (a) Prove $\text{Ann}_R(N)$ is a $2-$Sided ideal of R

   (b) Suppose $M = \mathbb{Z}_{24} \times \mathbb{Z}_{15} \times \mathbb{Z}_{50}$. Compute $\text{Ann}_{\mathbb{Z}}(M)$.

   (a) *Proof.* Let M be an $R-$Module and N be a submodule of M. Let $I = \text{Ann}_R(N) = \{r \in R : rn = 0 \forall n \in N\}$.
   To show I is a two-sided ideal, we'll show that I is an ideal of R, and I is both a left and right ideal of R.

   - $(I \leq (M, +))$
     Take $x, -y \in I$ and $n \in N$.
     Then $xn = 0$ and $-yn = 0$, so that $xn + (-yn) = 0 + 0 = 0$. Giving us $(x - y)n = 0$, since N is a module over R. Hence $x - y \in I$ for all $x, -y \in I$.
   - (Left Ideal)
     Let $r \in R$ and $x \in I$. Then $xn = 0$ for all $n \in N$. Hence $r(xn) = r(0) = 0$ and so $(rx)n = 0$ because R is associative. Hence $rx \in I$ for all $r \in R$.
     Thus I is a left ideal of R.
   - (Right Ideal)
     Let $r \in R$ and $x \in I$. Then $xn = 0$ for all $n \in N$. So that since N is a submodule of M, we have that $rn \in N$ hence:
     $$x(rn) = 0 \iff (xr)n = 0 \qquad \forall n \in N.$$
     Thus $xr \in I$. Hence I is a right-ideal of R.

   Thus I is a 2-Sided Ideal of R. □

   (b) *Proof.* Let $M = \mathbb{Z}_{24} \times \mathbb{Z}_{15} \times \mathbb{Z}_{50}$.
   Let $n \in \text{Ann}_{\mathbb{Z}}(M)$. So that $n \in \mathbb{Z}$ and $n([a]_{24}, [b]_{15}, [c]_{50}) = ([0]_{24}, [0]_{15}, [0]_{50})$. That is:
   $$\begin{aligned} na &\equiv 0 \mod 24 \\ nb &\equiv 0 \mod 15 \\ nc &\equiv 0 \mod 50. \end{aligned}$$
   That is na, nb, nc is a multiple of $24, 15, 50$, respectively.
   Furthermore, since $a < 24$, $b < 15$, and $c < 50$. This implies that n divides $24, 15$ and 50. That is $n = k\text{lcm}(24, 15, 50) = k600$.
   Hence $n \in \{k600 : k \in \mathbb{Z}\} = \mathbb{Z}600$. So that $\text{Ann}_{\mathbb{Z}}(M) \subseteq \mathbb{Z}600$.
   Conversely, we'll also end up with $\mathbb{Z}600 \subseteq \text{Ann}_{\mathbb{Z}}(M)$, since for all $x \in \mathbb{Z}600$, $xa \equiv 0 \mod 24, xb \equiv 0 \mod 15$, and $xc \equiv 0 \mod 50$ for all $(a, b, c) \in \mathbb{Z}_{24} \times \mathbb{Z}_{15} \times \mathbb{Z}_{50}$.
   So that $\mathbb{Z}600 = \text{Ann}_{\mathbb{Z}}(M)$. □

Homework 6

3. Show that M is an irreducible R-Module if and only if M is $R-$Isomorphic to R/m, for some maximal (2-sided) ideal m.

Proof. Let R be a ring.

($\implies$) Suppose M is an irreducible $R-$Module. Then since every irreducible $R-$Module is a cyclic R-Module, then there exists a $a \in M$ such that $a \neq 0$ and $R \cdot a = M$.

Define the map:

$$\phi : R \to M \qquad \phi(r) = ra \qquad \text{for all } r \in R.$$

Then clearly for $r, s \in R$

$$\phi(r+s) = (r+s)a = ra + sa = \phi(r) + \phi(s)$$

$$\phi(rs) = (rs)a = r(sa) = r\phi(s).$$

Hence ϕ is $R-$Linear in M.

Moreover, note that $\phi(R) = R \cdot a = M$. So then, by the first Isomorphism theorem for Modules, we have that:

$$R/\ker(\phi) \simeq \phi(R) = M \iff R/\ker(\phi) \simeq M.$$

Now suppose that there exists an ideal J such that: $\ker(\phi) \subset J \subset R$.

Then by the Third Isomorphism Theorem for Modules we have:

$$\frac{R/\ker(\phi)}{J/\ker(\phi)} \simeq R/J.$$

But note that $R/\ker(\phi) \simeq M$ as we have shown, so that:

$$\frac{M}{J/\ker(\phi)} \simeq R/J.$$

Hence $J/\ker(\phi)$ is isomorphic to some submodule of M. But there are only 2 submodules of M, M and (0). That implies $J/\ker(\phi) \simeq M$ or $J/\ker(\phi) \simeq (0)$.

If $J/\ker(\phi) \simeq (0)$, this corresponds to the case when $J = \ker(\phi)$.

If $J/\ker(\phi) \simeq M$, then we would have $M/(J/\ker(\phi)) \simeq M/M = (0) \simeq R/J$. Implying that $J \simeq R$.

Hence $\ker(\phi)$ is maximal in R.

($\impliedby$)

Assume that M is $R-$Isomorphic to R/m for some two-sided ideal m.

Homework 6

Then suppose we have a submodule $N \subset M$. So that means since $M \simeq R/\mathrm{m}$, we have that N is isomorphic to some sub-ring of R/m. But since m is a field, since m is maximal.

Hence the only ideals of a field are (0) and $R/\mathrm{m} \simeq M$. Thus $N \simeq M$ or $N \simeq (0)$. Hence M is an irreducible $R-$Module. $\square$

Homework 6

4. Suppose $N \subset M$ is a submodule. Prove that if N and M/N are finitely generated, then M is finitely generated.

   Proof. Let M be an R-Module and $N \subset M$ a submodule. Suppose N and M/N are finitely generated.

   Consider $m \in M$, so that $m + N \in M/N$. Hence there exists a $N' \in M/N$ such that:

   $$m + N = N'$$

   So that since M/N is finitely generatedd:

   $$m + N = \sum_{i=1}^{\alpha_{n'}} (a_i r_i + N) = \left(\sum_{i=1}^{\alpha_{n'}} a_i r_i \right) + N.$$

   So that since N is finitely generated:

   $$m + \sum_{i=1}^{\alpha_1} b_i s_i = \sum_{i=1}^{\alpha_{n'}} a_i r_i + \sum_{i=1}^{\alpha_2} c_i t_i \iff m = \sum_{i=1}^{\alpha_{n'}} a_i r_i + \sum_{i=1}^{\alpha_2} c_i t_i - \sum_{i=1}^{\alpha_1} b_i s_i.$$

   That is for any $m \in M$, we have that m is generated by a finite sum of elements in R and M.

   Thus M is finitely generated. □

Homework 6

5. Any ring R with 1 can be viewed as an $R-$Module. Consider $R = \mathbb{R}[x, y]$ viewed as a module over itself. Prove that it's free of rank 1, but that the submodule $I = (x, y)$ is not free, and needs at least two generators.

Proof. Let $R = \mathbb{R}[x, y]$ and M be an $R-$Module.

Then $M = R \cdot 1 = \mathbb{R}[x, y] \cdot 1 = \mathbb{R}[x, y]$. Hence $1 \in \mathbb{R}[x, y]$ is a basis for M and so $M = \mathbb{R}[x, y]$ has rank 1.

($\langle x, y\rangle$ is not free)

Let $I = \langle x, y\rangle = \{r_1(x, y)x + r_2(x, y)y : r_1(x, y), r_2(x, y) \in \mathbb{R}[x, y]\}$.

Then to show that I is not free, we'll show that any spanning set of $I = \langle x, y\rangle$ is not linearly independent, hence I has no basis and thus I is not a free submodule.

Suppose we have a spanning set of I, call it $\{a_1, \ldots, a_n\}$.

Then we'll show this is necessarily not linearly independent over $\mathbb{R}[x, y]$. Consider:

$$r_1a_1 + r_2a_2 + \ldots + r_na_n = 0$$

Then let $r_3 = r_4 = \ldots = r_n = 0$ and then let $r_2 = -a_1$ and $r_1 = a_2$, which are all ring elements since $R = M$. So that:

$$a_1a_2 - a_1a_2 = 0,$$

but $r_1 \neq 0$ and $r_2 \neq 0$.

Thus $\{a_1, \ldots, a_n\}$ is a spanning set, but not linearly independent.

(Need 2 generators)

Suppose $a \in I$ is a generator of I, then $\mathbb{R}[x, y] \cdot a = I$.

So note that x is in I, so there exists a $r(x, y) \in \mathbb{R}[x, y]$ such that:

$$a(x, y) = \frac{x}{r(x, y)},$$

by the division algorithm of polynomials, since $a(x, y)$ is a polynomial and $r(x, y)$ is a polynomial. We must have $r(x, y) = \text{Constant} = C$, hence $a(x, y) = Dx$ for some $D \in \mathbb{R}$. So then there's a $d(x, y) \in \mathbb{R}[x, y]$ such that:

$$d(x, y)Dx = y.$$

This would imply that x divides y, in the since of polynomial division, a clear contradiction.

Thus we must have at least 2 generators of $I = \langle x, y\rangle$ □

Homework 6

6. Let I be an index set and let $R^I = \coprod_{i \in I} R_i$ be the free $R-$Module, where $R_i = R \cdot 1_i$ is the free module of rank 1 on basis 1_i. The universal property of R^I is that for any set $\{m_i\}_I$ in an $R-$Module M, there's a unique R-Module homomorphism $R^I \to M$ taking $1_i \to m_i$. Prove that this is the same as the universal property of the coproduct $\coprod_I R_i$: Given any co-cone $(M, \{\psi_i\})$ of the $\{R_i\}_I$, there's a unique map of co-cones $(\coprod_I R_i, \{\iota_i\}) \to (M, \{\psi_i\})$

   Proof. Collaborated with Kelsey Lowrey, Zach Gelber, and Caroline Semmons.

   Let I be an index set and let $R^I = \coprod_{i \in I} R_i$ be the free $R-$Module, where $R_i = R \cdot 1_i$.

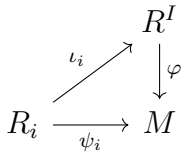
   Then consider the co-cone $(M, \{\psi_i\}_I)$ to $\{R_i\}_I$. So that is for all $i \in I$:

$$\psi_i : R_i \to M.$$

   Then for each $i \in I$, $\psi_i(1_i) = m_i$, where m_i is just some labeling of M with $i \in I$, determines the map ψ_i.

   Let $\iota_i : R_i \to R^I$ be given by $\iota_i(r_i) = r_i = r \cdot 1_i$. Then $(R^I, \{\iota_i\})$ is a co-cone to $\{R_i\}_I$.

   Finally, define $\varphi : R^I \to M$ by $\varphi(1_i) = m_i$, this is a well-defined map since R^I is a Free-Module. So that $(\varphi \circ \iota_i)(r_i) = \varphi(\iota(r_i)) = \varphi(r_i) = \varphi(r \cdot 1_i) = r\varphi(r_i) = rm_i = r\psi_i(1_i) = \psi_i(r \cdot 1_i) = \psi_i(r_i)$, hence the diagram below commutes:



   Moreover, suppose there's a $\psi' : R^I \to M$ such that:

$$\psi' \circ \iota_i = \psi \circ \iota_i$$

   Then we would have:

$$\iff \psi'(\iota_i(r_i)) = \psi(\iota_i(r_i)) \iff \psi'(r_i) = \psi(r_i)$$

   Hence $\psi' = \psi$, ψ is a unique map such that the above diagram commutes. □

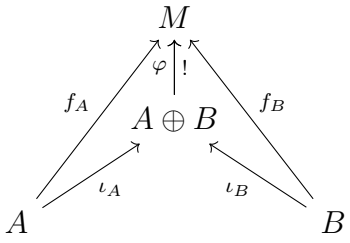
Homework 6

7. Let A, B, M, N be $R-$Modules. Use the universal properties to prove:

   (a) There's a natural isomorphism $\hom_R(A \oplus B, M) \to \hom_R(A, M) \times \hom_R(B, M)$

   (b) There's a natural isomorphism $\hom_R(A, M \times N) \to \hom_R(A, M) \times \hom_R(A, N)$.

   (a) *Proof.* Let A, B, M, N be $R-$Modules.
   By the property of co-products we have that for any A, B, M being $R-$Modules that there exists a unique $\varphi : A \oplus B \to M$ such that the diagram below commutes:



   That is:

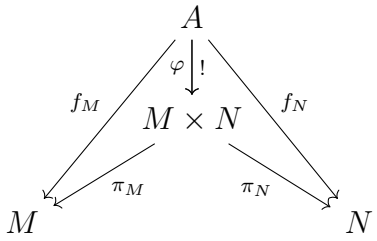
$$\varphi \circ \iota_A = f_A \qquad \varphi \circ \iota_B = f_B.$$

   We'll define $\psi : \hom_R(A \oplus B, M) \to \hom_R(A, M) \times \hom_R(B, M)$ with this commutative diagram. Define $\psi(\varphi) = (f_A, f_B)$, where $\varphi : A \oplus B \to M$, $f_A : A \to M$ and $f_B : B \to M$, then clearly $(f_A, f_B) \in \hom_R(A, M) \times \hom_R(B, M)$ and $\varphi \in \hom_R(A \oplus B, M)$.
   Moreover, ψ is well-defined because φ is unique for any pair (f_A, f_B) by the Universal Property of Co-Products. That is φ is the only function such that both $\varphi \circ \iota_A = f_A$ and $\varphi \circ \iota_B = f_B$.
   To show this is an isomorphism, we'll show that there exists a map $\psi^{-1} : \hom_R(A, M) \times \hom_R(B, M) \to \hom_R(A \oplus B, M)$ such that $\psi \circ \psi^{-1}$ is the identity map on $\hom_R(A, M) \times \hom_R(B, M)$ and $\psi^{-1} \circ \psi$ is the identity map on $\hom_R(A \oplus B, M)$.
   Define $\psi^{-1} : \hom_R(A, M) \times \hom_R(B, M) \to \hom_R(A \oplus B, M)$ be $\psi^{-1}(f_A, f_B) = \varphi_{f_A, f_B}$ where φ_{f_A, f_B} is the unique homomorphism such that the Co-Product diagram commutes. This is well-defined, since we have there exists a unique φ_{f_A, f_B} for each $f_A : A \to M$, $f_B : B \to M$ pair.
   Then $\psi(\psi^{-1}(f_A, f_B)) = \psi(\varphi_{f_A, f_B}) = (f_A, f_B)$ and $\psi^{-1}(\psi(\varphi_{f_A, f_B})) = \psi^{-1}((f_A, f_B)) = \varphi_{f_A, f_B}$. Thus $\psi \circ \psi^{-1}$ and $\psi^{-1} \circ \psi$ are identity morphisms on their respective categories.
   Thus we have that $\psi : \hom_R(A \oplus B, M) \to \hom_R(A, M) \times \hom_R(B, M)$ defined by $\psi(\varphi_{f_A, f_B}) = (f_A, f_B)$ defines an isomorphism on the two categories. □

Homework 6

(b) *Proof.* Let A, B, M, N be $R-$Modules.

By the property of co-products we have that for any A, N, M being $R-$Modules that there exists a unique $\varphi : A \to M \times N$ such that the diagram below commutes:



That is:

$$\varphi \circ \pi_M = f_M \qquad \varphi \circ \pi_N = f_N.$$

We'll define $\psi : \hom_R(A, M \times N) \to \hom_R(A, M) \times \hom_R(B, N)$ with this commutative diagram. Define $\psi(\varphi) = (f_M, f_N)$, where $\varphi : A \to M \times N$, $f_N : A \to N$ and $f_M : A \to M$, then clearly $(f_M, f_N) \in \hom_R(A, M) \times \hom_R(A, N)$ and $\varphi \in \hom_R(A, M \times N)$.

Moreover, ψ is well-defined because φ is unique for any pair (f_M, f_N) by the Universal Property of Co-Products. That is φ is the only function such that both $\varphi \circ \pi_N = f_N$ and $\varphi \circ \pi_M = f_M$.

To show this is an isomorphism, we'll show that there exists a map $\psi^{-1} : \hom_R(A, M) \times \hom_R(A, N) \to \hom_R(A, M \times N)$ such that $\psi \circ \psi^{-1}$ is the identity map on $\hom_R(A, M) \times \hom_R(A, N)$ and $\psi^{-1} \circ \psi$ is the identity map on $\hom_R(A, M \times N)$.

Define $\psi^{-1} : \hom_R(A, M) \times \hom_R(A, N) \to \hom_R(A, M \times N)$ be $\psi^{-1}(f_M, f_N) = \varphi_{f_M, f_N}$ where φ_{f_M, f_N} is the unique homomorphism such that the Co-Product diagram commutes. This is well-defined, since we have there exists a unique φ_{f_M, f_N} for each $f_M : A \to M$, $f_N : A \to N$ pair.

Then $\psi(\psi^{-1}(f_M, f_N)) = \psi(\varphi_{f_M, f_N}) = (f_M, f_N)$ and $\psi^{-1}(\psi(\varphi_{f_M, f_N})) = \psi^{-1}((f_M, f_N)) = \varphi_{f_M, f_N}$. Thus $\psi \circ \psi^{-1}$ and $\psi^{-1} \circ \psi$ are identity morphisms on their respective categories.

Thus we have that $\psi : \hom_R(A, M \times N) \to \hom_R(A, M) \times \hom_R(A, N)$ defined by $\psi(\varphi_{f_M, f_N}) = (f_M, f_N)$ defines an isomorphism on the two categories. □

Homework 6

8. Let R be a commutative ring with 1. A short exact sequence of R-Modules is a diagram of the form

$$1 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 1$$

such that the kernel of each map equals to image of the preceding map, where applicable. Thus ι is injective, π is surjective, and $\iota(M') = \ker(\pi)$, so that $M/\iota(M') \simeq M''$.

Suppose given an exact sequence of modules as above. We say the sequence splits if there's a morphism $\sigma : M'' \to M$ such that $\pi \circ \sigma = id_{M''}$. Use the universal property of free modules to prove that if M'' is free then the sequence splits, and then $M \simeq M' \oplus M''$.

Proof. I collaborated with Zachary Gelber, Kelsey Lowrey, and Caroline Semmons.

Suppose we have a short exact sequence of $R-$Modules:

$$1 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 1$$

and suppose M'' is a free $R-$Module. So we have $\ker(\iota) = 1$ and $\pi(M) = M''$.

With M'' being free we have there exists an index set I such that:

$$M'' = \coprod_{i \in I} R_i,$$

with $R_i = R \cdot 1_i$, where $\{1_i\}_I$ is a basis of M''. So that for any $m \in M$ we have there exists a_i's in R such that:

$$\pi(m) = \sum_{\substack{i \in I \\ \text{Finite}}} a_i 1_i.$$

In fact, since π is a surjection, for each $i \in I$, a $m_i \in M$ such that $\pi(m_i) = 1_i$. Moreover, by the universal property of Free Modules we have that there's a unique R-Module homomorphism: $\sigma : M'' \to M$ such that $\sigma(1_i) = m_i$ for all $i \in I$.

Homework 6

So consider $y \in M''$, so $y = \sum_{i \in I \text{Finite}} a_i 1_i$. So consider the following:

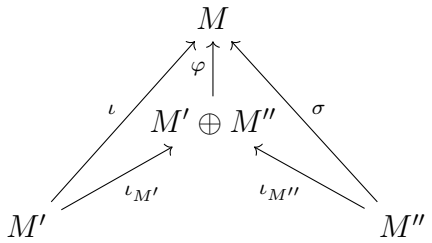
$$\begin{aligned}
(\pi \circ \sigma)(y) &= \pi(\sigma(y)) \\
&= \pi\left(\sigma\left(\sum_{\substack{i \in I \\ \text{Finite}}} a_i 1_i\right)\right) && \text{Definition of y} \\
&= \pi\left(\sum_{\substack{i \in I \\ \text{Finite}}} a_i \sigma(1_i)\right) && \sigma \text{ is a R-Module Homomorphism} \\
&= \pi\left(\sum_{\substack{i \in I \\ \text{Finite}}} a_i m_i\right) && \text{Definition of } \sigma \\
&= \sum_{\substack{i \in I \\ \text{Finite}}} a_i \pi(m_i) && \pi \text{ is a R-Module Homorphism} \\
&= \sum_{\substack{i \in I \\ \text{Finite}}} a_i 1_i && \text{Definition of } \pi \\
&= y
\end{aligned}$$

Hence We have $\pi \circ \sigma = id_{M''}$, as required. So that:

$$1 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 1$$

is a split sequence.

By the universal property of co-products: We have there exists a $\varphi : M' \oplus M'' \to M$ such that the following diagram commutes:



That is:

$$\varphi \circ \iota_{M'} = \iota \qquad \varphi \circ \iota_{M''} = \sigma.$$

So we'll show that φ is an $R-$Module Isomorphism.

Note that from this fact we have that if $m' \in M'$ that:

$$\iota(m') = \varphi(\iota_{M'}(m')) = \varphi(m')$$

so that $\varphi(m') = \iota(m')$. Similarly, if $m'' \in M''$, then $\varphi(m'') = \sigma(m'')$. So that for any $m' + m'' \in M' \oplus M''$ we have:

$$\varphi(m' + m'') = \iota(m') + \sigma(m'').$$

In fact, this defines $\varphi : M' \oplus M'' \to M$, since both $\iota : M' \to M$ and $\sigma : M'' \to M$ are well-defined $R-$Module morphisms.

Furthermore, we have that φ is a unique $R-$Module homomorphism, by the Universal Property of Co-Products, hence we just need to show that φ is a $1-1$ correspondence between $M' \oplus M''$ and M.

- (Injective)
  Let $m' + m'' \in \ker(\varphi)$, then consider the following:

$$\begin{aligned}
\varphi(m' + m'') &= 0 && \text{m' and m'' are in the kernel of } \varphi \\
\iota(m') + \sigma(m'') &= 0 && \text{Definition of } \varphi \\
\pi(\iota(m') + \sigma(m'')) &= \pi(0) && \text{Applying } \pi \text{ to both sides of the equation} \\
\pi(\iota(m')) + \pi(\sigma(m'')) &= 0 && \pi \text{ is R-Linear} \\
0 + m'' &= 0 && \text{Recall we had: } \ker(\pi) = \iota(M') \text{ and } \pi \circ \sigma = id_{M''} \\
m'' &= 0
\end{aligned}$$

  Hence $m'' = 0$, and so:

$$\iota(m') = 0$$

  but we had $\ker(\iota) = \{0\}$, hence $m' = 0$, so $m' = 0_{M'}$ and $m'' = 0_{M''}$, so that $\ker(\varphi) = \{0_{M'} + 0_{M''}\}$. So $\varphi : M' \oplus M'' \to M$ is a 1-1 R-Module homomorphism.
- (Surjective)
  Consider $y \in M$. Then we may write $y = y - \sigma(\pi(y)) + \sigma(\pi(y))$.
  Note then that $\pi(y - \sigma(\pi(y))) = \pi(y) - \pi(\sigma(\pi(y))) = \pi(y) - \pi(y) = 0$, where we used the fact that π is $R-$Linear and $\pi \circ \sigma = id_M$. So that since $\ker(\pi) = \iota(M')$ we have that there exists a $m' \in M'$ such that: $\iota(m') = y - \sigma(\pi(y)) \in \iota(M')$. So that, since $\pi(y) \in M''$, we have that:

$$m' + \pi(y) \in M' \oplus M''.$$

  Hence:

$$\varphi(m' + \pi(y)) = \iota(m') + \sigma(\pi(y)) = y - \sigma(\pi(y)) + \sigma(\pi(y)) = y.$$

  Thus y is in the range of $\varphi : M' \oplus M'' \to M$ and hence φ is onto.

Homework 6

Thus $\varphi : M' \oplus M'' \to M$ is an isomorphism and thus $M' \oplus M'' \simeq M$. $\square$

Name: Joseph McGuire
Instructor: Eric Brussel

Homework 7

Math 561 (Fall 2021)

1. An *idempotent* e of a ring R (with 1) is any element satisfying $e^2 = e$. We usually assume an idempotent is nontrivial, meaning $e \neq 0, 1$. Suppose R has nontrivial idempotent e. Prove that there's a $R-$Module isomorphism:

$$Re \oplus R(1-e) \simeq R.$$

Proof. Let R be a ring (with 1) and let $e \in R \setminus \{0,1\}$ such that $e^2 = e$.

Consider the map $\varphi(re + s(1-e)) = re + s(1-e)$.

First note that if $x \in Re \cap R(1-e)$, then $x = re$ and $x = s(1-e)$ for some $r, s \in R$. Hence $re = s(1-e) \iff re + se = s \iff re^2 + se^2 = se \iff re + se = se \iff re = 0$ and since $x = re$ we have $x = 0$. That is:

$$Re \cap R(1-e) = \{0\}$$

Then note that for any $r \in R$, we have that $re + r(1-e) = re + r - re = r$, hence $r \in Re + R(1-e)$. So that $R = Re + R(1-e)$.

Finally we have $R-$Linearity:

$$R(re+s(1-e)+xe+y(1-e)) = (r+x)e+(s+y)(1-e) = R((r+x)e+(s+y)(1-e))$$

and

$$R(a(re+s(1-e)) = R(are+as(1-e)) = are+as(1-e) = a(re+s(1-e)) = aR(re+s(1-e)).$$

So we have

$$R \simeq Re \oplus R(1-e).$$

□

Homework 7

2. (a) Show the matrix unit e_{11} is an idempotent of the ring $M_2(k)$, and that the left ideals $I_1 = M_2(k)e_{11}$ and $I_2 = M_2(k)(1 - e_{11})$ are irreducible left $M_2(k)$-Modules. Conclude that we have a module decomposition $M_2(k) \simeq I_1 \oplus I_2$ into simple (irreducible) left ideals.

Proof. Define:

$$M_2(k) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} : a_{ij} \in k \right\}.$$

Then

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, e_{11}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = e_{11}.$$

Note that $M_2(k)$ is clearly a ring under matrix multiplication/addition. So that $M \simeq Me_{11} \oplus M(I_2 - e_{11}) = I_1 \oplus I_2$ from (1). □

Homework 7

(b) Prove $M_2(k)$ has no proper nonzero 2−Sided Ideals.

Proof. Suppose that $M_2(k)$ has a proper nonzero 2−Sided Ideal, call it $J \subset M_2(k)$ with $rJ = Jr$ for all $r \in k$.

So that $xJx^{-1} = J$ for all $x \in M_2(k)$.

I worked with Zach Gelber on this idea:

Note that J is nonempty hence there's some element $x \in J \setminus \{0\}$. So that this element can be written in the form:

$$x = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then the matrix multiplication gives us:

$$\frac{1}{a} e_{11} x e_{11} = e_{11}.$$

Hence $e_{11} \in J$. So because J is closed under addition/subtraction/multiplication, we have that:

$$I_2 - e_{11} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = e_{22}.$$

And so we have that $me_{11} + ne_{22} \in J$ for all $m, n \in M_2(k)$, which in (a) we have shown this is exactly $M_k(2)$. Hence $J = M_k(2)$.

So $M_2(k)$ has no proper nonzero 2-sided Ideals. □

Homework 7

3. Let R be a PID, and suppose M is a finitely generated $R-$module. Then we have a surjective $R-$Module homomorphism $\pi : R^n \to M$ with kernel $K \subset R^n$. Use the Homomorphism Correspondence Theorem to show that any submodule of M is finitely generated. This has a name: Any module whose submodules are all finitely generated is called *noetherian*. The ring R, being a PID, has the property that all of its ideal are finitely generated, and so it too is called *noetherian*. There is a theorem, that we now don't need to prove, that says a finitely generated module over a noetherian ring is notherian.

   Proof. Let R be a PID, suppose M is a finitely generated $R-$Module. Let $\pi : R^n \to M$ with $K \subset R^n$ be our surjective $R-$Module homomorphism.

   Suppose $N \subset M$ is a submodule of M. Since homomorphisms preserve structure and submodules:

   $$\pi^{-1}(N) \subset R^n$$

   is a submodule of R^n. Well wait, R^n is finitely generated and has a basis:

   $$\{x_1, \ldots, x_n\}.$$

   So $\pi^{-1}(N)$ must be free and have rank $m \leq n$; that is it has some basis:

   $$\{x_1, \ldots, x_m\}.$$

   So that $\{\pi(x_1), \ldots, \pi(x_m)\}$ will generated $N \subset M$. Hence N is finitely generated. $\square$

Homework 7

4. Let R be a PID and suppose M is a finitely generated $R-$Module. The *torsion submodule* of M is by definition: $M_{tor} = \{m \in M : am = 0 \text{ for some } 0 \neq a \in R\}$.

   (a) Show M_{tor} is a submodule of M.

   Proof. Let R be a PID, suppose M is a finitely generated $R-$Module. Define $M_{tor} = \{m \in M : am = 0 \text{ for some } 0 \neq a \in R\}$.
   To show that it's a submodule, we need to show it's a subgroup under addition and stable under R.

   - Let $a, -b \in M_{tor}$, then there exists elements $m_a, m_b \in M \setminus \{0\}$ such that:

     $$m_a a = 0 \qquad m_b(-b) = 0.$$

     So that since R is a PID, it is a commutative ring, hence:

     $$m_b m_a a = 0 \qquad m_b m_a(-b) = 0 \iff m_b m_a(a - b) = 0.$$

     Since $m_b \neq 0$ and $m_a \neq 0$ and R is Integral Domain, it must not contain zero-divisors, hence $a - b \in M_{tor}$.
   - Let $r \in R$ and $m \in M_{tor}$. Then there exists an $a \in R$ such that $am = 0$ so that $r(am) = 0 \iff a(rm) = 0$, by commutativity of R. Thus $rm \in M_{tor}$. So that M_{tor} is stable under R.

   Thus M_{tor} is a submodule of M. □

Homework 7

(b) Show that M/M_{tor} is a free $R-$Module of finite rank, and if the rank is f then $M \simeq M_{tor} \oplus R^f$.

Proof. Let R be a PID, suppose M is a finitely generated $R-$Module. Define $M_{tor} = \{m \in M : am = 0 \text{ for some } 0 \neq a \in R\}$.
By (a) we have that M/M_{tor} is well-defined since M_{tor} is a submodule of M.
By the Structure Theorem of finitely generated modules over a PID, we have that:

$$M \simeq R^n / \ker(\pi),$$

where $\pi : R^n \to M$ given by:

$$\sum_{i=1}^{n} r_i e_i \longmapsto \sum_{i=1}^{n} r_i x_i.$$

Clearly if $\sum_{i=1}^{n} r_i x_i = 0 \iff r_i = 0 \ \forall i$ since x_i is a basis of R^n. That is $\ker(\pi) = \{0\}$.
So that:

$$M/M_{tor} \simeq \frac{M_{tor} \oplus R^f}{M_{tor}} \simeq \frac{R^f}{\{0\}} = R^f.$$

Where the last Isomorphism comes from the 2nd Isomorphism Theorem for Modules. So that since R^f is of finite rank $f < \infty$, we have that:

$$M \simeq M_{tor} \oplus M/M_{tor} \simeq M_{tor} \oplus R^f.$$

As we wished to prove. □

Homework 7

5. Let R be a PID, and let M be a finitely generated $R-$module. Then $M \simeq M_{tor} \oplus R^f$, by the previous problem. Show that there's an element $a \in R$ such that $aM \simeq R^f$, and use this to show f is uniquely determined for M. Thus M has a 'rank'.

Proof. Let R be a PID and let M be a finitely generated $R-$Module. By the previous problem, we have that $M \simeq M_{tor} \oplus R^f$.

Then for all elements $m_i \in M_{tor}$ we have that there's a $r \in R$ such that $r_i m_i = 0$. So define:

$$a = \prod_{i \in I} r_i,$$

so that $am_i = 0$ for all $i \in I$.

Then we have a correspondence between the left-cosets:

$$aM \simeq aM_{tor} aR^f \iff aM \simeq aR^f,$$

since we have $aM_{tor} = \{0\}$ since for all $am_i = 0$ for all i.

Thus $aM \simeq aR^f$, but note that R^f is precisely the elements of M that satisfy:

$$ar = 0 \iff a = 0.$$

Moreover, R^f has a basis:

$$\{x_1, \ldots, x_f\}$$

so that a basis of aR^f is exactly:

$$\{ax_1, \ldots, ax_f\}.$$

This is in fact as basis, since it is linearly independent:

$$ar_1x_1 + \ldots + ar_fx_f = 0 \iff a(r_1x_1 + \ldots + r_fx_f) = 0 \iff a = 0 \text{ or } r_1 = \ldots = r_f = 0,$$

and we can full out $a = 0$ so that $\{ax_1, \ldots, ax_f\}$ is a maximal linearly independent subset of aR^f, hence is a basis. So that $f = f$ hence $aR^f \simeq R^f$. Thus $R^f \simeq aM$, as required.

Suppose that $M \simeq M_{tor} \oplus R^f \simeq M_{tor} \oplus R^g$. Hence $R^f \simeq R^g$ and so $f = g$, as required. □

Homework 7

6. Let k be a field, V a $k-$Vector Space, and $T \in \mathrm{End}_k(V)$ a linear transformation. Make V a $k[x]-$ Module 'V_T' by letting x act as T. Prove that V_T is a finitely generated torsion $k[x]-$Module if and only if $\dim_k(V)$ is finite.

Proof. I worked with Zach Gelber closely on the majority of this problem.

Let k be a field, V be a $k-$Vector Space, and $T \in \mathrm{End}_k(V)$ be a Linear Transformation. Let V_T be a $k[x]-$Module obtained by letting x act as T in $k[x]$.

$(\implies)$

Suppose V_T is a finitely generated torsion $k[x]-$Module. Then, note that since k is a field we have shown in previous classes that $k[x]$ is a principal ideal domain. So by The Fundamental Theorem of Finitely Generated Modules over a PID:

$$V_T \simeq \coprod_{i=1}^{r} k[x]/(d_i) \oplus (k[x])^f.$$

However, we assumed that V_T is a torsion module, hence $(k[x])^f = \emptyset$, so that:

$$V_T \simeq \coprod_{i=1}^{r} k[x]/(d_i)$$

Then for each i we have $\mathrm{Deg}_k(k[x]/(d_i)) = \deg(d_i)$. So that since V_T is finitely generated we have that each d_i has finite degree or $\deg(d_i) < \infty$, for each i. Furthermore, by Remark 5.4.1 on Handout 9 we have that

$$\dim_k(V) = \sum_{i=1}^{r} \deg(d_i) < \infty.$$

That is the desired result.

$(\impliedby)$ Let $\dim_k(V) = n < \infty$.

Note that the $k[x]-$Module V_T is generated by polynomials in $k[x]$ where x is replaced by T, that is $V_T = k[x] \cdot 1$, where the action is replacing x with T. So V_T is finitely generated $k[x]$-Module, so that since $k[x]$ is a PID, we have that:

$$V_T \simeq \coprod_{i=1}^{r} k[x]/(d_i(x)) \oplus (k[x])^f.$$

where $d_i | d_j$ when $i < j$.

Suppose that we have some free element of V_T, that is there's a $p(x) \in k[x]$ and $m \in V_T \setminus \{0\}$ such that:

$$p(x) \cdot m = 0 \iff p(x) \sum_{i \in I} a_i T^i = 0 \iff \sum_{i \in I} p(x) a_i T^i = 0.$$

Homework 7

Since $m \neq 0$, and k is a field and hence an integral domain it follows that $p(x) = 0$. That is, $([k[x])^f = \emptyset$ and hence $V_T \simeq \coprod_{i=1}^{r} k[x]/(d_i)$, and so V_T is a finitely generated torsion $k[x]$-Module, as desired. $\square$

Homework 7

7. Suppose k is a field, V is a finite-dimensional k-Vector Space, $A, B \in M_n(k)$, and V_A and V_B are the $k[x]$-Modules determined by A and B. We say A and B are similar if $B = PAP^{-1}$ for some $P \in GL_n(k)$. Show that V_A and V_B are isomorphic as $k[x]-$Modules if and only if A and B are similar.

Proof. Let k be a field, V a finite-dimensional $k-$Vector Space (with dimension n), $A, B \in M_n(k)$ and V_A,V_B be $k[x]-$Modules determined by A and B.

$(\implies)$

Suppose V_A and V_B are $k[x]-$Isomorphic to each other. That is, we have a $k[x]-$Linear Isomorphism $P : V_A \to V_B$ such that for all $v \in V_A$:

$$P(f(x) \cdot v) = f(x) \cdot P(v) \qquad \forall f(x) \in k[x].$$

Note that under x in V_A, $x \cdot v = Av$ and in V_B $x \cdot v = Bv$. That is:

$$P(x \cdot v) = xP(v) \iff P(Av) = BP(v) \iff PA = BP \iff A = P^{-1}BP,$$

which is the result we wished to prove.

$(\impliedby)$

Suppose there exists a $P \in GL_n(k)$ such that $A = PBP^{-1}$.

Then define the map:

$$\pi : V_A \to V_B$$

by $\pi(v) = Pv$. Then note that for any $x, y \in V_A$ and $r \in k[x]$:

$$\pi(x + y) = Px + Py = \pi(x) + \pi(y)$$

and

$$\pi(rx) = P(rx) = r(Px) = r\pi(x)\checkmark.$$

Hence π is $k[x]-$Linear. To show that it's bijective:

- $(1 - 1)$
  Let $x \in \ker(\pi)$. Then $\pi(x) = 0$:
  $$Px = 0 \iff x = 0,$$
  since P is invertible and so $\ker(P) = \{0\}$. Hence $x = 0$.
- (Onto)
  Let $y \in V_B$, then $x = P^{-1}y$ exists since P^{-1} is defined so that:
  $$\pi(P^{-1}y) = P(P^{-1}y) = y\checkmark$$
  Thus π is onto V_B.

That is $\pi : V_A \to V_B$ defined by $\pi(v) = Pv$ is a $R-$Linear Isomorphism and hence $V_A \simeq V_B$, the result we wished to show. □

Name: Joseph McGuire
Instructor: Eric Brussel

Math 561 (Fall 2021)

Homework 7

1. Determine the structure of the abelian group G defined by generators a and b, and relations $2a + 4b = 0$ and $3b = 0$ and find generators for a direct sum decomposition of G into cyclic factors.

   Proof. Let be an abelian group such that $G = \langle a, b \rangle$ such that:

   $$2a + 4b = 0$$

   $$3b = 0.$$

   So that the module is:

   $$[T]_e = \begin{bmatrix} 2 & 0 \\ 4 & 3 \end{bmatrix} \qquad e = \{e_1, e_2\},$$

   where e is the standard ordered basis of $\mathbb{Z}^2$.

   Then we'll have:

   $$d_1 = \Delta_1 = \gcd(0, 2, 3, 4) = 1$$

   and

   $$d_2 = \Delta_2 \Delta^{-1} = 6/1 = 6.$$

   So that:

   $$G \simeq \coprod_{i=1}^{2} \mathbb{Z}/(d_i) = \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z}6 \simeq \{0\} \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_6.$$

   Hence $G \simeq \mathbb{Z}_6$ is our only cyclic factor of G.

   Finally, we a new generator in terms of the old generators, which we can obtain by finding P such that $T = P\text{Diag}\{1, 6\}P^{-1}$ by finding the elementary row operations that give the diagonal matrix.

   With the row Operations $R_2 \iff 2R_2$:

   $$\begin{bmatrix} 2 & 0 \\ 8 & 6 \end{bmatrix}$$

   then take $R_2 \iff R_2 - 4R_1$ and $R_1 \iff \frac{1}{2}R_1$ gives $\text{Diag}\{1, 6\}$. That is a transition matrix of:

   $$P = \begin{bmatrix} 2 & 0 \\ 4 & \frac{1}{2} \end{bmatrix}.$$

   So that our new generators satisfy:

   $$a' = 2a + 4b = 0 \qquad b' = \frac{1}{2}b.$$

Homework 7

So that $a' = 0$ and $6b' = \frac{6}{2}b = 3b = 0$, hence $|b'| = 6$ so that:

$$G \simeq \langle b' : |b'| = 6 \rangle.$$

□

Homework 7

2. Determine the structure of the abelian group G defined by generators a, b, c, d and relations $2a + 3b = 4a - 5c + 11d = 0$.

Proof. In a similar process to (1), establish a map $T : \mathbb{Z}^4 \to \mathbb{Z}^4$ given by:

$$(e_1, e_2, e_3, e_4) \longmapsto (2e_1 + 3e_2, 4e_1 - 5e_3 + 11e_4, 0, 0).$$

This has a matrix:

$$[T]_e = \begin{bmatrix} 2 & 4 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & -5 & 0 & 0 \\ 0 & 11 & 0 & 0 \end{bmatrix}.$$

We find that:

$$\Delta_1 = \gcd(2, 4, 3, -5, 11, 0) = 1 \qquad \Delta_2 = 1 \qquad \Delta_3 = 0 \qquad \Delta_4 = 0$$

then this has a Smith Normal Form of:

$$[T]_e \sim \mathrm{Diag}\{1, 1, 0, 0\}.$$

Giving us:

$$G \simeq \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/0 \oplus \mathbb{Z}/0 \simeq 0 \oplus 0 \oplus \mathbb{Z}^2 \simeq \mathbb{Z}^2.$$

□

Homework 7

3. Suppose k is a field, F is a field containing k, and V is a $k[x]$-Module via some $T \in \mathrm{End}_k(V)$.

   (a) Prove that T may be diagonalizable over F but not over k.

   Counter-Example. Let

   $$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

   and consider this in $M_2(\mathbb{R})$, it's characteristic polynomial is then :

   $$\det(xI - A) = x^2 + 1.$$

   By Theorem 6.3 on handout 9, we have that A is diagonalizable over $\mathbb{R}$ iff its characteristic polynomial splits over $\mathbb{R}$ into distinct linear factors, which it does not. But consider $A \in M_2(\mathbf{C})$ it does split, so A is diagonalizable over $\mathbf{C}$ but not $\mathbb{R}$ and we have $\mathbb{R} \subset \mathbf{C}$. □

Homework 7

(b) Prove that T's rational canonical forms over k and F are the same.

Proof. Let k be a field, $F \supset k$ be a field, V be a $k[x]$-Module and $T \in \mathrm{End}_k(V)$. Note that by Theorem 3.4(Handout 9) we have that the invariant factors of T are uniquely determined over a ring $R = k$, that is T is a $k-$Module and hence a linear transformation, and each $d_i \in k$. So that since the rational canonical form of T is uniquely determined by the invariant factors of T, we have that T's rational canonical form is the same in k and F. Since $d_i(x) \in k[x] \subset F[x]$ determine the companion matrices $C(d_i(x))$ in which:

$$T = \bigoplus_{i=1}^{r} C(d_i(x)).$$

□

Homework 7

(c) Prove that matrices A and B are similar over k if and only if they are similar over F.

Proof. Let k be a field, $k \subset F$ is a field, and V is a $k[x]$-Module via some $T \in \mathrm{End}_k(V)$. Without loss of generality, assume that $\dim_k(V) = n$.
($\implies$) Let A be similar to B over k, then there exists $P \in GL_n(k)$ such that:

$$A = PBP^{-1}.$$

Since $k \subset F$ we have that $P \in GL_n(F)$ and hence $A = PBP^{-1}$. Thus A and B are similar in F.
($\impliedby$) Assume that A and B are similar over F, by Theorem 5.11, we have that V_A and V_B have the same invariant factors over F and hence have the same rational canonical form. So that by part (b) we have that V_A and V_B have the same rational canonical form in k. That is each companion matrix $C(d_i(x))$ is the same as in k as they are in F, and hence V_A and V_B have the same invariant factors in k as in F. So that by Theorem 5.11, we have that A and B are similar in k. □

Homework 7

4. Prove that there are no $A \in M_3(\mathbb{Q})$ with $A^8 = I$ but $A^4 \neq I$.

   Proof. Let $A \in M_3(\mathbb{Q})$ and $A^8 = I$, then we will show that $A^4 = I$.

   Since we have $A^8 = I$ we also have that $A^8 - I = 0$. So that by Cayley-Hamilton, we must have $m_A(x)$ divides $x^8 - 1$. So that $m_A(x)$ divides $(x^4-1)(x^4+1)$, if $m_A(x)$ divides $x^4 - 1$, then we're done since this implies $m_A(x)p(x) = x^4 - 1$ and so $m_A(A)p(A) = A^4 - I$, but by Cayley-Hamilton $m_A(A) = 0$ hence:

   $$A^4 - I = 0 \iff A^4 = I.$$

   So suppose that $m_A(x)$ doesn't divide $x^4 - 1$.

   Since $m_A(x)$ must divide $x^8 - 1$, this implies that $m_A(x)$ divides $x^4 + 1$. But note that $x^4 + 1$ is irreducible in $\mathbb{Q}$, so that either $m_A(x) = 1$ or $x^4 + 1$. If $m_A(x) = 1$, then we would have $m_A(A) = 0 = 1$, a contradiction. So then $m_A(x) = x^4 + 1$, but we run into another problem, namely that $m_A(x)$ divides $p_A(x) = \det(xI - A)$. However, since $A \in M_3(\mathbb{Q})$, we have that $\deg(p_A(x)) \leq 3$ but $\deg(m_A(x)) = 4$, a contradiction.

   Thus $m_A(x)$ must divide $x^4 - 1$, and hence $A^4 = I$. □

Homework 7

5. Suppose V is a n-Dimensional vector space, $T \in \mathrm{End}_k(V)$, and the $k[x]-$Module V_T is isomorphic to $k[x]/(d(x))$, i.e V_T is a cyclic $k[x]-$Module. We may assume that d is monic. Recall an *eigenvector* $v \in V$ is a vector satisfying $T(v) = \lambda \cdot v$ for some $\lambda \in k$, and λ is then its *eigenvalue*. Pretend we know nothing about characteristic polynomials and eigenvalues.

   (a) Prove that λ is an eigenvalue of T if and only if $x - \lambda | d(x)$.

   Proof. Let V be an $n-$Dimensional Vector Space and $T \in \mathrm{End}_k(V)$ and the $k[x]$-Module $V_T \simeq k[x]/(d(x))$.
   ($\implies$)
   Suppose that λ is an eigenvalue of T. Then we have that $Tv = \lambda v$ for some $v \neq 0$. In our $k[x]-$Module that is:

   $$(x - \lambda)v = 0.$$

   That is, since $V_T \simeq k[x]/(d(x))$, we have that there exists an element:

   $$(x - \lambda)(f(x) + (d(x))) = (d(x)) \iff (x - \lambda)f(x) + (d(x)) = (d(x))$$

   That is $(x - \lambda)f(x) \in (d(x))$, but that would imply that $(x - \lambda)f(x) = g(x)d(x)$. Since $\dim_k(V) = n$ we have that $\deg(d(x)) = n$ and so that $g(x) = C$ for some constant $C \in k$. Hence $(x - \lambda)\frac{1}{C}f(x) = d(x)$ and thus $x - \lambda$ divides $d(x)$, as required for the result.
   ($\impliedby$)
   Suppose that $x - \lambda$ divides $d(x)$. So that $d(x) = f(x)(x - \lambda)$ for some $f(x) \in k[x]$. This would imply that:

   $$f(x)(x-\lambda)+(d(x)) = (d(x)) \iff (x-\lambda)(f(x)+(d(x)) = (d(x)) \iff x(f(x)+(d(x)) = \lambda(f(x)-$$

   This equation in $k[x]/(d(x))$ has an equivalent in V_T:

   $$xv = \lambda v \qquad v \neq 0 \iff Tv = \lambda v$$

   and thus $\lambda \in k$ is an eigenvalue of T, as required for the result. $\square$

Homework 7

(b) If λ is an eigenvalue of T, find the $k-$dimension of the eigenspace $E_\lambda = \{v \in V : T(v) = \lambda \cdot v\}$.

Lemma 1. *$V_T \simeq k[x]/(d(x))$ and λ is an eigenvalue of T then $E_\lambda \subset V_T$ is a submodule.*

Proof. Let $V_T \simeq k[x]/(d(x))$ and λ be an eigenvalue of T, then we need to show that E_λ is a subgroup under addition and stable under the action of $k[x]$.

- Let $v, -w \in E_\lambda$, then $Tv = \lambda v$ and $T(-w) = \lambda(-w)$. With the linearity of T we have:
$$T(v - w) = \lambda(v - w).$$
Hence $v - w \in E_\lambda$
- Let $p(x) = a_0 + a_1x + \ldots + a_mx^m \in k[x]$ and $v \in E_\lambda$, then:
$$(a_0I + a_1T + \ldots + a_mT^m)v = a_0Iv + a_1Tv + \ldots + a_mT^mv$$
$$= (a_0 + a_1\lambda + a_2\lambda^2 + \ldots + a_m\lambda^m)v \in E_\lambda.$$

Hence E_λ is stable under the action of $k[x]$, hence $E_\lambda \subset V_T$ is a submodule of V_T. □

Proof of (b). Let $V_T \simeq k[x]/(d(x))$ and λ be an eigenvalue of T, then note that $E_\lambda \neq \{0\}$. By our lemma $E_\lambda \subset V_T$ is a submodule of V_T but V_T is cyclic, hence V_T is irreducible. Since $E_\lambda \neq \{0\}$, it follows that $E_\lambda = V_T$. □

Homework 7

6. Let

$$A = \begin{bmatrix} 6 & -10 & -10 \\ 3 & -5 & -6 \\ -1 & 2 & 3 \end{bmatrix}.$$

(a) Compute $p_A(x)$.

Proof. We'll use the following trick to compute the characteristic polynomial:

$$p_A(x) = x^3 - c_2x^2 + c_1x - c_0,$$

$$c_2 = 6 + (-5) + 3$$

$$c_1 = \begin{vmatrix} 6 & -10 \\ 3 & -5 \end{vmatrix} + \begin{vmatrix} 6 & -10 \\ -1 & 3 \end{vmatrix} + \begin{vmatrix} -5 & -6 \\ 2 & 3 \end{vmatrix} = 0 + 8 - 3 = 5$$

$$c_0 = \det(A) = 2$$

So that:

$$p_A(x) = x^3 - 4x^2 + 5x - 2 = (x-2)(x-1)^2$$

□

Homework 7

(b) Compute $m_A(x)$.

Proof. We may factor $p_A(x) = x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2)$, so that the invariant factors are either:

$$d_1(x) = (x-1) \qquad \text{and} \qquad d_2(x) = (x-1)(x-2)$$

or

$$d_1(x) = (x-1)^2(x-2).$$

Either $(x-1)(x-2)$ or $p_A(x)$ is our minimal polynomial. We need x acting as T to give us 0. Note that:

$$T-I_3 = \begin{bmatrix} 5 & -10 & -10 \\ 3 & -6 & -6 \\ -1 & 2 & 2 \end{bmatrix} \qquad T-2I_3 = \begin{bmatrix} 4 & -10 & -10 \\ 3 & -7 & -6 \\ -1 & 2 & 1 \end{bmatrix} \qquad (T-I_3)(T-2I_3) = 0.$$

So that $m_A(x) = (x-1)(x-2)$. □

Homework 7

(c) Compute the invariant factors of A.

Proof. By our work in (b) we have that the invariant factors are:

$$d_1(x) = (x-1) \qquad d_2(x) = (x-1)(x-2) = x^2 - 3x + 2$$

□

Homework 7

(d) Find the rational canonical form of A.

Proof. Our companion matrices for the invariant factors are:

$$C(d_1(x)) = [1] \qquad C(d_2(x)) = \begin{bmatrix} 0 & -2 \\ 1 & 3 \end{bmatrix}$$

So that are rational canonical form is:

$$Q = C(d_1(x)) \oplus C(d_2(x)) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{bmatrix}.$$

□

Name: Joseph McGuire
Instructor: Eric Brussel

Homework 9

Math 561 (Fall 2021)

As usual, k is a field

1. A matrix $A \in M_n(k)$ is nilpotent $A^k = 0$ for some $k \geq 1$.

   (a) Characterize the nilpotent matrices in terms of their Jordan canonical forms.

   Proof. Let $A \in M_n(k)$ and suppose there's a $k \geq 1$ such that $A^k = 0$, without loss of generality, assume that m is the least such integer where this condition holds; that is $A^n \neq 0$ for all $n < m$.
   Suppose λ is an eigenvalue for some matrix B with eigenvector v:

   $$Bv = \lambda v,$$

   then we'll have $B^r v = \underbrace{B(B(B \dots (Bv)))}_{\text{r-times}} = \lambda^r v$, for $r \in \mathbb{Z}^+$.
   So suppose λ is an eigenvalue of A with eigenvector $v \neq 0$, so that:

   $$A^m v = \lambda^m v \iff \lambda^m = 0 \iff \lambda = 0.$$

   Implying that the only eigenvalue of A is $\lambda = 0$.
   So any invariant factors of A is simply x^i so that the Jordan blocks of A are of the form: $J_i(0)$ where is the Jordan block with all zeros on the diagonal and 1's on the super-diagonal and rank i. So that $A \simeq \bigoplus_{i=1}^{m} J_{r_i}(0)$. □

Homework 9

(b) Prove that if A is nilpotent, we may assume $A^k = 0$ for some $k \leq n$.

Proof. Suppose A is nilpotent and $A \in M_n(k)$, assume that $k \geq 1$ where $A^k = 0$, and let m be the least such integer where this is true; that is, $A^r \neq 0$ for $r < m$. Let $J(0) = \bigoplus_{i=1}^{m} J_{r_i}(0)$ For sake of contradiction, suppose that $m > n$.

By (1a), we have that A has a Jordan canonical form of $J(0)$; that is the Jordan block of all 0's on the diagonal and 1's in the super-diagonal. So there exists a $P \in GL_n(k)$ such that:

$$A = PJ(0)P^{-1}.$$

That is $A \simeq J(0)$, they are similar.

So by Remark 5.11.1 Handout 9, we have that $p_A(x) = p_{J(0)}(x)$. However, we have $p_{J(0)}(x) = \det(xI_n - J(0)) = x^n$. But, by our assumption, we have that A^m, $m > n$, is the least such integer where this is true. However, by Cayley-Hamilton, we have $p_A(A) = p_{J(0)}(x) = A^n = 0$, a contradiction since $n < m$. □

Homework 9

(c) Prove that if A is nilpotent, then $tr(A) = 0$.

Proof. Suppose $A \in M_n(k)$ and is nilpotent, by our argument in [1b] we have that $p_A(x) = \det(xI_n - A) = x^n$. By Example 5.11.3 in Handout 9, that would imply that $-tr(A) = c_{n-1} = 0$, where c_{n-1} is the coefficient of x^{n-1} in $p_A(x)$. Hence $tr(A) = 0$. □

Homework 9

2. Diagonalize $A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ over $\mathbb{C}$.

Proof. First we need to find the invariant factors of A:

$$\det(A - xI) = (x - (\cos\theta - i\sin\theta))(x - (\cos\theta + i\sin\theta)).$$

So that the eigenvalues for the Jordan Canonical Form are:

$$\lambda = \cos\theta \pm i\sin\theta = e^{\pm i\theta}.$$

So that $A \sim \text{Diag}\{e^{-i\theta}, e^{i\theta}\}$ by Jordan Canonical Form.

Moreover we have eigenvectors of:

$$A(-i, 1)^T = \begin{bmatrix} -i\cos\theta - \sin\theta \\ -i\sin\theta + \cos\theta \end{bmatrix} = \begin{bmatrix} -i(\cos\theta - i\sin\theta) \\ \cos\theta - i\sin\theta \end{bmatrix} = e^{-i\theta} \begin{bmatrix} -i \\ 1 \end{bmatrix},$$

so that $v_1 = (-i, 1)^T$ is our first eigenvector. Similarly, we have that $v_2 = (i, 1)^T$ is an eigenvector. Hence with

$$P = \begin{bmatrix} -i & i \\ 1 & 1 \end{bmatrix},$$

we have:

$$A = P \begin{bmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{bmatrix} P^{-1}.$$

□

Homework 9

3. Recall $SO_3 = \{A \in GL_3(\mathbb{R}) : A^tA = I \text{ and } \det(A) = 1\}$ is the group of rotations in $\mathbb{R}^3$. By definition, these are the matrices whose columns are mutually perpendicular (dot product of different columns is zero), of length one (dot product of a column with it's self is 1). Therefore they take the standard basis, with respect to which A is written in the first place, to another orthonormal basis. From this we can conclude that elements of SO_3 preserve the dot product, and therefore fix lengths and angles. Prove, using just these facts, that any element of SO_3 is diagonalizable over $\mathbb{C}$, [Hint: This will prove SO_3 is the group of rotations.]

Proof. Let $A \in SO_3$.

Then suppose that λ is an eigenvalue of A, with eigenvalue $v \neq 0$, so that:

$$\langle Av, Av\rangle = \langle v, v\rangle \iff \|Av\|^2 = \|v\|^2 \iff |\lambda|^2\|v\|^2 = \|v\|^2 \iff |\lambda| = 1,$$

where the first equality follows from $A = A^T$, the second equality comes from the def. of the norm in an inner-product space, the third from $A = A^T$, and the last the fact that $v \neq 0$ so that $\|v\| \neq 0$. That is $\lambda = e^{i\theta}$ for some $\theta \in [0, 2\pi)$. From this, note that $SO_3 \subset M_3(\mathbb{R})$, and hence $p_A(x) \in \mathbb{R}[x]$. That is, if $\lambda = e^{i\theta}$ is an eigenvalue, then so is $\overline{\lambda} = e^{-i\theta}$.

Moreover, consider the following:

$$\det(A - I) = \det((A - I)^T) \iff \det(A - I) = \det(A^T - I),$$

so that:

$$\det(A - I) = \det(A - AA^T) = \det(A(I - A^T)) =$$
$$\det(A)\det(-(A^T - I)) = -\det(A^T - I) = -\det(A - I).$$

The first equality, coming from $I = AA^T$, the second is factoring, the third is multiplicative property of the det., fourth from $\det(A) = 1$ and det. being homogeneous, so that for this to be true we need $\det(A - I) = 0$. That is $\lambda = 1$ is necessarily an eigenvalue of A.

Thus, if $\theta \neq 0, \pi$, we have three distinct eigenvalues and by Jordan Normal form A is diagonalizable over $\mathbb{C}$.

If $\theta = 0$, then $\lambda = 1, 1, 1$ and we have that $p_A(x) = (x - 1)^3$. Let $J_n(1)$, denote the Jordan-Block of rank n with diagonals 1. Hence either

$$V_A \simeq \mathbb{R}[x]/(x - 1) \oplus \mathbb{R}[x]/(x - 1) \oplus \mathbb{R}[x]/(x - 1),$$

then we 're done, or

$$V_A \simeq \mathbb{R}[x]/(x - 1)^2 \oplus \mathbb{R}[x]/(x - 1) \qquad \text{or} \qquad V_A \simeq \mathbb{R}[x]/(x - 1)^3,$$

Homework 9

the first giving us $A \simeq J_2(1) \oplus J_1(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. However, note that $A^T = A^{-1}$, however $(J_2(1) \oplus J_1(1))^T \neq (J_2(1) \oplus J_1(1))^{-1}$. Similarly, if $A \simeq J_3(1)$, thus $A \simeq I_3$.

If $\theta = \pi$, then $\lambda = 1, -1$ are eigenvalues of A. So then $V_A \simeq \mathbb{R}[x]/(x-1) \oplus \mathbb{R}[x]/(x+1) \oplus \mathbb{R}[x]/(x+1)$, in which case we're done, or $V_A \simeq \mathbb{R}[x]/(x-1) \oplus \mathbb{R}[x]/(x+1) \oplus \mathbb{R}[x]/(x+1)^2$. Similar to if $\lambda = 1$ is the only eigenvalue, in the latter case these Jordan blocks are not orthogonal and hence we arrive at a contradiction.

Hence any element $A \in SO_3(\mathbb{R})$ is diagonalizable. $\square$

Homework 9

4. Suppose V is an $n-$dimensional $k-$vector space, and $T \in \mathrm{End}_k(V)$. Show that T has an eigenvalue λ if and only if $x - \lambda$ divides $m_T(x)$. Suppose the invariants of T are $d_1, \ldots, d_r$, and $d_i(x)$ is the smallest one divisible by $x - \lambda$. Compute $\dim_k E_\lambda$.

Proof. Suppose V is an $n-$dimensional $k-$Vector Space and $T \in \mathrm{End}_k(V)$.

($\implies$) Let λ be an eigenvalue of T; that is, there exists $v \neq 0$ such that $Tv = \lambda v$. That is $(T - \lambda I)v = 0$, by the structure theorem: $V_T \simeq \coprod_{i=1}^r k[x]/(d_i(x))$, this is the equation:

$$(x - \lambda)(\oplus_{i=1}^r (f_i(x) + (d_i(x)))) = 0.$$

Since $v \neq 0$, then it's counter part in the polynomial ring: $\oplus_{i=1}^r f_i(x) + (d_i(x)) \neq 0$. Implying there's at least one $f_i(x) + (d_i(x)) \neq 0$. So that:

$$(x - \lambda) \oplus_{i=1}^r (f_i(x) + (d_i(x))) = \oplus_{i=1}^r (x - \lambda) f_i(x) + (d_i(x)) = 0.$$

Hence for at least one i, we have

$$(x - \lambda) f_i(x) \in (d_i(x)).$$

Thus $(x - \lambda)$ divides $d_i(x)$, and we have $d_i(x)$ divides $d_r(x) = m_T(x)$, hence $x - \lambda$ divides $m_T(x)$.

($\impliedby$)

Suppose that $x - \lambda$ divides $m_T(x)$, the minimal polynomial of T. Then $(x - \lambda)f(x) = m_T(x) = d_r(x)$. Hence $(x - \lambda)f(x) + (d_r(x)) = (d_r(x)) \iff (x - \lambda)(f(x) + (d_r(x))) = (d_r(x))$. Since we have the isomorphism with the structure theorem, this implies there's an equivalent equation in V_T; namely:

$$(x - \lambda)v = 0 \iff xv = \lambda v \iff T(v) = \lambda v.$$

So that λ is an eigenvalue of T.

I worked with Zach Gelber on this part of the proof. For the second part, suppose the statement of the problem that $d_1(x), \ldots, d_r(x)$ are the invariant factors of T and $d_s(x)$ is the smallest such that $x - \lambda$ divides $d_s(x)$. Then $d_s(x) = (x - \lambda)f(x)$ for some $f(x) \in k[x]$. Then for all i such that $s \leq i \leq r$ we have $(x - \lambda) | d_s(x) | d_i(x) | d_r(x) = m_T(x)$. Then the number of times $(x - \lambda)$ appears in a $d_i(x)$ with $s \leq i \leq r$ will determine the number of Jordan blocks that of λ there are, which is exactly $\dim_k(E_\lambda)$, there are $r - (s - 1)$ such invariant factors; the 1 factors in the invariant factor of $d_s(x)$. So that:

$$\dim_k(E_\lambda) = r - s + 1.$$

□

Homework 9

5. Determine the number of similarity classes in $M_6(\mathbb{C})$ with characteristic polynomial $(x^4-1)(x^2-1)$.

Proof. If a matrix shares both the same characteristic polynomial and minimal polynomial, then they are similar. So to determine the similarity classes of $M_6(\mathbb{C})$ we need to determine the possible minimal polynomials.

The characteristic polynomial is:

$$(x^4-1)(x^2-1) = (x-1)^2(x+1)^2(x-i)(x+i).$$

This gives us eigenvalues of $\lambda = 1, -1, i, -i$. So that each $x-\lambda$ must divide $m_A(x)$, for some $A \in M_6(\mathbb{C})$. Hence $m_A(x) = (x-1)(x+1)(x-i)(x+i)f(x)$ for some $f(x) \in \mathbb{R}[x]$.

We could choose $f(x) = 1$, in which case:

$$m_A(x) = (x-1)(x+1)(x-i)(x+i),$$

this will give one other invariant factor $d_1(x) = (x-1)(x+1)$ and this will give us:

$$A \simeq Diag\{1, -1, 1, -1, i, -i\}$$

The next possibility is $f(x) = (x-1)$:

$$m_A(x) = (x-1)^2(x+1)(x-i)(x+i),$$

this leads to $d_1(x) = x+1$, hence

$$A \simeq J_1(-1) \oplus J_2(1) \oplus J_1(-1) \oplus J_1(i) \oplus J_1(-i).$$

The next possibility is $f(x) = (x+1)$:

$$m_A(x) = (x-1)(x+1)^2(x-i)(x+i),$$

which leads to $d_1(x) = x-1$ so that:

$$A \simeq J_1(1) \oplus J_1(1) \oplus J_2(-1) \oplus J_1(i) \oplus J_1(-i).$$

The final possibility is:

$$m_A(x) = (x-1)^2(x+1)^2(x-i)(x+i) = p_A(x),$$

which is the only invariant factor so that:

$$A \simeq J_2(1) \oplus J_2(-1) \oplus J_1(i) \oplus J_1(-i).$$

□

Homework 9

6. Let $A = \sum e_{ij} \in M_n(\mathbb{Q})$, the matrix of all 1's. Find $JCF(A)$.

Proof. First we'll find $p_A(x) = \det(xI - A) = \det(xI - \sum_{i,j} e_{i,j}) = x^n - c_{n-1}x^{n-1} + \ldots + (-1)^{n-1}c_1x + (-1)^n c_0$, where c_{n-i} will be the sum of the diagonal minors of rank i. That is $c_{n-1} = trace(A) = n$, however, note that for $i \geq 2$, c_{n-i} will be linear sums of involving:

$$\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} = 0,$$

no matter the coefficients of this sum, each 2×2 minor of A is identically 0. Implying that $c_{n-i} = 0$, for all $2 \leq i \leq n$. Hence $p_A(x) = x^n - nx^{n-1} = x^{n-1}(x - n)$. Hence the only eigenvalues are $\lambda = 0, n$. Moreover, consider

$$A(A - nI) = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 1 \end{bmatrix} \begin{bmatrix} 1-n & 1 & \ldots & 1 \\ 1 & 1-n & \ldots & 1 \\ \vdots & \vdots & \ddots & 1 \\ 1 & \ldots & \ldots & 1-n \end{bmatrix} = 0.$$

So we have that $m_A(x) = x(x - n)$ and hence:

$$JCF(A) = J_1(n) \oplus J_{n-1}(0),$$

where $J_k(\lambda)$ is the Jordan block of rank k for λ. □

Homework 9

7. Computer the characteristic polynomial and Jordan canonical form for the matrices

$$A = \begin{bmatrix} -8 & -10 & -1 \\ 7 & 9 & 1 \\ 3 & 2 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} -3 & 2 & -4 \\ 4 & -1 & 4 \\ 4 & -2 & 5 \end{bmatrix}.$$

Proof. Using the characteristic polynomial trick we have:

$$p_A(x) = x^3 - x^2 - x + 1 \qquad p_B(x) = x^3 - x^2 - x + 1 = p_A(x).$$

These factor as:

$$p_A(x) = p_B(x) = (x-1)^2(x+1).$$

The minimal polynomial is either:

$$(x-1)(x+1) \qquad \text{or} \qquad p_A(x) = p_B(x).$$

We find that: $(A-I)(A+I) \neq 0$ and $(B-I)(B+I) = 0$, so that:

$$m_A(x) = p_A(x) = (x-1)^2(x+1) \qquad m_B(x) = (x-1)(x+1).$$

With A we have that the only invariant factor is $m_1(x) = (x-1)^2(x+1)$ so that we have:

$$A \simeq J_1(-1) \oplus J_2(1) = \begin{bmatrix} -1 & 0 & 00 & 1 & 1 \\ 0 & 0 & 1 & & \end{bmatrix} \qquad B \simeq J_1(1) \oplus J_1(1) \oplus J_1(-1) = Diag\{1, 1, -1\}.$$

□

Homework 9

8. Determine all Jordan canonical forms for matrices with characteristic polynomial $(x-2)^3(x-3)^2$.

Proof. Let $A \in M_5(\mathbb{R})$ such that $p_A(x) = (x-2)^3(x-3)^2$, so that $m_A(x) = (x-2)(x-3)f(x)$ for $f(x) \in \mathbb{R}[x]$. 6 possibilities follow by the Jordan Canonical form:

(a) $m_A(x) = (x-2)(x-3) = d_3(x)$, then $d_1(x) = (x-2)$ and $d_2(x) = (x-2)(x-3)$ so that:

$$A \simeq Diag\{2,2,2,3,3\}.$$

(b) $m_A(x) = (x-2)^2(x-3) = d_2(x)$, then $d_1(x) = (x-2)(x-3)$ so that

$$A \simeq J_1(3) \oplus J_1(2) \oplus J_2(2) \oplus J_1(3).$$

(c) $m_A(x) = (x-2)^2(x-3)^2$ and $d_1(x) = (x-2)$ so that:

$$A \simeq J_1(2) \oplus J_2(2) \oplus J_2(3).$$

(d) $m_A(x) = (x-2)(x-3)^2$ so that $d_1(x) = (x-2)$ and $d_2(x) = (x-2)$ hence:

$$A \simeq J_1(2) \oplus J_1(2) \oplus J_1(2) \oplus J_2(3).$$

(e) $m_A(x) = (x-2)^3(x-3)$ so that $d_1(x) = (x-3)$ and hence:

$$A \simeq J_1(3) \oplus J_3(2) \oplus J_1(3).$$

(f) $m_A(x) = (x-2)^3(x-3)^2$ so that:

$$A \simeq J_3(2) \oplus J_2(3).$$

□

Homework 9

9. Suppose $A \in M_2(\mathbb{Q}), A^3 = I$ and $A \neq I$. Write Jordan canonical form of A over $\mathbb{C}$.

Proof. Suppose $A \in M_2(\mathbb{Q}), A^3 = I, A \neq I$. Then $A^3 - I = 0$ and $A \neq I$ implies that $p_A(x)$ divides $x^3 - 1$ and so $p_A(x)$ divides $(x-1)(x^2+x+1) = x^3 - 1$. Since $p_A(x)$ must be of degree 2 since the rank of A is 2, we have that $p_A(x) = x^2 + x + 1$. Since $p_A(x) = \left(x - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\right)\left(x - \left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right)\right)$, all linear factors, this implies that $m_A(x) = p_A(x)$ and hence the Jordan Canonical form of A is:

$$A \simeq Diag\{\frac{-1}{2} - \frac{\sqrt{3}}{2}i, -\frac{1}{2} + \frac{\sqrt{3}}{2}i\}.$$

□