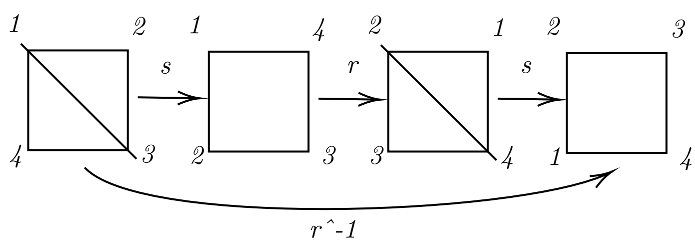
Trabalho 1

Grupos e Corpos

Yuri Kosfeld

Abril 2025

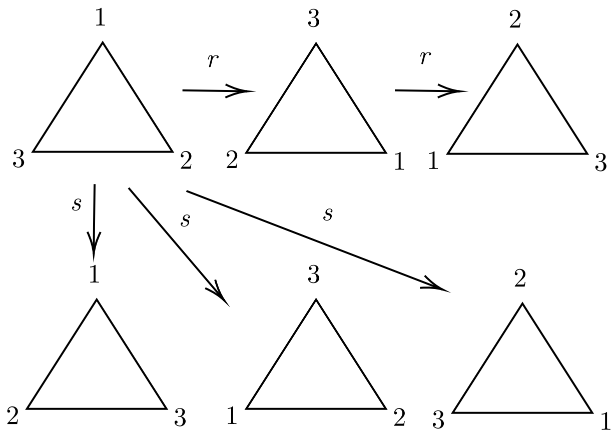
Exercício (Semana 1 - 13)**.** *(a) Para facilitar a explicação, vamos numerar os vértices do poligono de maneira ordenada de 1 até n. Uma rotação nesse poligono é uma forma de ciclar entre os vértices. Então se o nosso poligono tem 4 lados, temos 4 vértices: 1, 2, 3, 4. Se aplicarmos uma rotação nesse poligono os vértices agora trocam de indexação e vao de 1234 para 4123. Aplicando mais uma vez vamos para 3412 e assim por diante. A relação $r^n = 1$ é equivalente a dizer aplicar n rotações no poligono é a mesma ação de não aplicar rotação nenhuma. Visualmente é intuitivo pensar dessa forma, por exemplo, no nossa caso de n = 4, se olharmos o vértices da primeira posição, apos 4 rotações voltamos ao 1, ou seja, é igual a não ter feito rotação alguma. As reflexões no poligono são equivalentes a espelhamentos sobre um eixo do poligono de simetria desse poligono. Ou seja, as reflexões sobre um dado eixo não podem "mudar" o nosso poligono. De modo geral temos duas possibilidades de reflexões, as que fixam vértices e as que não vixam vértice algum. Em ambos os casos não é dificil notar que aplicando a mesma reflexão duas vezes seguidas voltamos ao estado inicial. Assim vem a relação de $s^2 = 1$.*



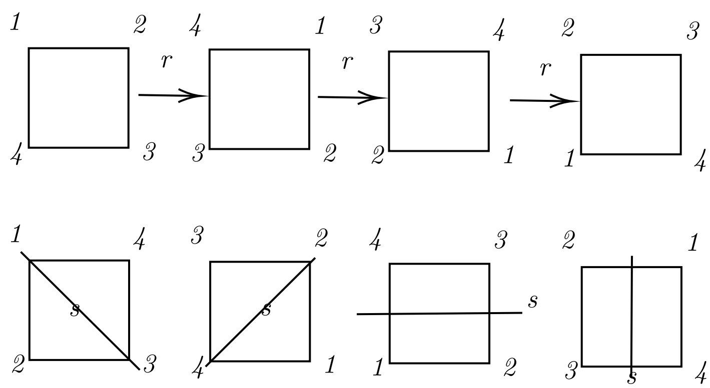
(b) Como D_n é gerado por todos os possiveis produtos de rotações e reflexões, para calcular a ordem de D_n é suficiente contar quantas rotações e quantas reflexões são possiveis a depender de n. Pela relação $r^n = 1$ segue que temos n rotações em D_n. Agora para as reflexões, precisamos separar nos casos, n par e n impar. Se n for par, então temos dois tipos de reflexões, as que fixam dois vértices e as que não vixam nenhum. Para as que fixam 2 vértices, temos então $n/2$ reflexões possiveis. Já para as reflexões que não fixam nenhum vértice, elas são as reflexões cujos eixos passam pelos pontos medios de lados opostos. Assim também temos $n/2$ reflexões. Logo o número total de reflexões é n. Para n impar, é mais simples. As únicas reflexões são aquelas que fixam um vértice, logo temos n reflexões. Assim

$$|D_n| = |\textit{rotações}| + |\textit{reflexões}| = n + n = 2n$$

(c)



D_3



D_4

(d) Para D_4 ser ciclico, ele deve ser gerado por um único elemento de D_4. Vamos mostrar que isso não é possivel. Tome primeiro r uma rotação. Pela relação $r^n = 1$, temos que $\langle r \rangle = \{1, r, r^2, r^3\}$, e então faltam as reflexões. Tome então uma s uma reflexão de D_4. Novamente pela relação $s^2 = 1$, temos que $\langle s \rangle = \{1, s\}$, assim faltando todas as demais reflexões e todas as rotações. Logo nenhum elemento de D_4 gera todo as simetrias e portanto D_4 não é ciclico. (e) Antes de mostrarmos que $D_n < S_n$, vamos ver que toda simetria em D_n é uma permutação dos vértices. Para isso, vamos mostrar que rotações e reflexões são permutação, e como esses são os geradores das simetrias em D_n, mostramos que todas são. Uma rotação em um poligono de n lados é uma permutação ciclica nos vertices do poligono. Então r uma rotação leva $r(i) = i + 1$. Por exemplo, em D_4, uma rotação de $90°$ no sentido horário é a permutação dos vértices (1234). Já uma reflexão é uma permutação que age nos vertices em pares. Note que em ambos os casos de reflexão isso vale, já que uma reflexão que fixa um vertice (caso n ímpar), temos $n - 1$ vértices para mudar e como n é impar, n-1 é par, logo temos $\frac{n-1}{2}$ mudanças. Para o caso n par, isso também vale, seja fixando um par de vértices ou não fixando nenhum. Como as simetrias são geradas por rotações e reflexões, qualquer produto de duas simetrias ainda é uma simetria em D_n, logo é fechado para o produto. Temos também um elemento neutro, a simetria identidade. Além disso, toda simetria tem um elemento inverso. Para mostrar isso vamos mostrar que toda rotação e toda reflexão possuem inversos. Tome r_k uma rotação, sabemos que vale a relação $r^n = 1$, então

se r é uma rotação dada por $r_k(i) = i + k$, segue que $r_k = r^k$ e então o inverso de r_k é r^{n-k}, uma vez que, $r_k r^{n-k} = r^k r^{n-k} = r^{n-k+k} = r^n = 1$. Para as reflexões, basta notar que segue da relação $s^2 = 1$ que o inverso é ela mesma. Assim D_n é um subgrupo de S_n.

Exercício (Semana 2 - 4)**.** *Primeiro precisamo mostrar que G/G' é um grupo. Para isso, basta verificar se $G' \lhd G$. Tome então um comutador de G, ou seja, $[x, y] \in G'$ e vamos mostrar que vale a inclusão para todo $g \in G$. Lembre que vale $[x, y] = xyx^{-1}y^{-1}$, então segue*

$$g[x, y]g^{-1} = g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1})$$

Vamos mostrar que $(gxg^{-1})^{-1} = gx^{-1}g^{-1}$. Seja então d o inverso de gxg^{-1}, segue então

$$\begin{aligned} gxg^{-1}d &= 1 \\ xg^{-1}d &= g^{-1} \\ g^{-1}d &= x^{-1}g^{-1} \\ d &= gx^{-1}g^{-1} \end{aligned}$$

Note que o mesmo vale para y. Então temos que

$$g[x, y]g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = [gxg^{-1}, gyg^{-1}] \in G'$$

Logo $G' \lhd G$. Agora que garantimos que G/G' é um grupo, vamos mostrar que ele é abeliano. Queremos mostrar então para $g_1, g_2 \in G$

$$(g_1G')(g_2G') = (g_2G')(g_1G') \Leftrightarrow g_1g_2G' = g_2g_2G'$$

Ou seja, queremos ver ser $g_1g_2(g_2g_1)^{-1} \in G'$. Mas note que, $g_1g_2(g_2g_1)^{-1} = g_1g_2g_2^{-1}g_1^{-1} = [g_1, g_2] \in G'$. Logo G/G' é abeliano.

Exercício (Semana 2 - 11)**.** *Primeiro vamos notar o que acontece com*

Exercício (Semana 2 - 12)**.** *Queremos mostrar que existe $x \in G$ tal que a ordem de x é p. Para isso vamos provar usando indução na ordem de G. Denotaremos $|G| = n$. Como caso base, vamos verificar quando $n = p$. Segue pelo corolario do Teorema de Lagrange, que G é ciclico, logo $G = \langle x \rangle$, e portanto $o(x) = |G|$, equivalente a $x^p = e_G$. Assim provado para o caso base. Lembre que G é abeliano. Tome então $a \in G$ tal que $a \neq e_G$ e defina $H = \langle a \rangle$. Se $p||H|$ então $a^{|H|/p}$ é um elemento de ordem p, e novamente temos solução. Se $p \nmid |H|$ então pelo Teorema de Lagrange, $p|(G : H)$. Mas $(G : H) = |G/H|$ e portanto $p||G/H|$. Logo pela hipotese de indução, tem um elemento de xH para algum $x \in G$ que tem ordem p. Seja m é a ordem de x em G, então $(xH)^m = eH \in G/H$. Donde segue que $p|m$ e então $x^{m/p}$ tem ordem p.*

Exercício (Semana 3 - 7)**.** *Queremos mostrar que $Z(G)$ não é trivial. Para isso, vamos provar que*

$$|Z(G)| > 1$$

já que se $Z(G)$ fosse trivial, teriamos $Z(G) = \{e_G\}$ e então $|Z(G)| = 1$. Sabemos que a ordem de G é uma potência de p, então p divide a ordem de G. Então pela Equação das Classes Conjugadas de G, todos os termos $(G : C(g_i))$ são diviseis por p. Pelo Teorema de Lagrange, $(G : C(g_i))$ é um divisor da ordem de G e portanto é uma potência de p. Novamente, pela Equação das Classes Conjugadas de G, temos

$$p^n = |G| = |Z(G)| + \sum p_i^m$$

em que cada m_i é o expoente de cada $(G : C(g_i))$. Logo,

$$|Z(G)| \equiv p^n - \sum p_i^m \equiv 0 \mod p$$

Como $|Z(G)| \geq 1$ e $|Z(G)| \equiv 0 \mod p$ temos que $|Z(G)| \geq p > 1$. Assim $Z(G)$ é não trivial.

Exercício (Semana 3 - 8)**.** *Para provarmos esse resultado, primeiro vamos notar primeiro que G é abeliano se somente se $G = Z(G)$. Não é dificl notar isso dado a definição do centro de G. Dadas as hipoteses de G, vamos mostrar que G é abeliano. Suponha por contradição que $Z(G) \neq G$. Tome então $a \in G \setminus Z(G)$. Assim $C(a)$ é subgrupo de G que contém a e Z(G), já que todos os elementos de Z(G) comutam. Como vimos no exercicio anterior, Z(G) não é trivial e mais, $|Z(G)| \geq p$. Além disso, temos também que $|C(a)| \geq |Z(G)| + 1 = p + 1$. Pelo Teorema de Lagrange, a ordem de C(a) deve dividir a ordem de G. Logo temos duas, possibilidades: ou $|C(a)| = p$ ou $|C(a)| = p^2$. Mas como visto anteriormente, $|C(a)| \geq p + 1$ assim a única possibilidade válida é $|C(a)| = p^2$. Então $C(a) = G$ e então todos os elementos de G comutam e portanto $a \in Z(G)$ uma contradição.*

Exercício (Semana 3 - 12)**.** *Vamos analisar os p-subgupos de Sylow para G. Segue do Terceiro Teorema de Sylow que $n_q \equiv 1 \mod q$ e $n_q | p$. Temos então duas possibilidades para n_q. Se $n_q = p$ então $p \equiv 1 \mod q$, o que não pode acontecer, já que $p < q$ e são primos. Logo, por força $n_q = 1$. Ou seja, existe um unico q-subgrupo de sylow. Seja Q esse subgrupo, e então sabemos que Q é normal pela unicidade. Vamos analisar agora n_p. $n_p \equiv 1 \mod p$ e $n_p | q$. Nessas condições, vamos ver que $n_p = 1$ ou $n_p = q$. Se $n_p = q$ então $q - 1 \equiv 0 \mod p$, o que contradiz a hipotese de $p \nmid q - 1$. Logo $n_p = 1$ e também tem um unico P p-sugrupo de sylow em G e portanto P é normal. Sabemos que $P \cap Q = \{e_G\}$. Queremos mostrar agora que $PQ = QP$, ou seja, que PQ é abeliano. Para todo $x \in P$ e $y \in Q$ considere $xyx^{-1}y^{-1}$. Como Q é normal, segue que $xyx^{-1} \in Q \Rightarrow xyx^{-1}y^{-1} \in Q$. Também temos que P é normal, portanto $yxy^{-1} \in P \Rightarrow xyx^{-1}y^{-1} \in P$. Mas como vimos pela interseção de P e Q, segue então $xyx^{-1}y^{-1} = 1 \Rightarrow xy = yx$. Finalmente, temos que $|PQ| = pq = |G|$ e então $G = PQ$ e G é abeliano.*

Exercício (Semana 4 - 6)**.** *Sabemos que em S_4 os únicos subgrupos normais são $\{e\}, V_4, A_4$ e o proprio S_4. Aqui V_4 é o grupo de Klein, dado por*

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

Sabemos que V_4 é abeliano e portanto todo subgrupo dele é normal. Se então construirmos a serie subnormal

$$\{e\} \leq \langle (12)(34) \rangle \leq V_4 \leq S_4$$

satisfaz as condições, dadas as propriedades de V_4, mas tem o grupo $\langle (12)(34) \rangle$ não é normal em S_4. Logo é uma serie subnormal que não é normal.

Exercício (Semana 4 - 7)**.**

Exercício (Semana 4 - 11)**.** *Para isso vamos dividir nossos casos com base nas ordens possiveis que satisfazem certas propriedades. **Caso 1**: $|G| = p$ com p primo. Nesse caso temos que G é ciclico e portanto ciclico. Como G é abeliano sabemos que G é soluvel. Para esse caso, a cardinalidade de G pode ser*

$$|G| = 2, 3, 5, 7, 13, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$$

***Caso 2**: Se G é um p-subgrupo. Como mostramos no exercicio 8 da semana 3, Z(G) não é trivial e também mostramos que G é abeliano. Logo novamente G é soluvel. As cardinalidades que se encaixam nesse caso são as de potencias de primo. Logo as cardinalidades desse caso são*

$$|G| = 4, 8, 9, 16, 25, 27, 32, 49$$

Caso 3: $|G| = pq$ *com* p, q *primos com* $p|q-1$. *Segue do exercicio 12 da semana 3 que* G *é abeliano, logo soluvel. As cardinalidades desse caso são*

$$|G| = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58$$

Caso 4: $|G| = p^2q$. *A prova é semelhante ao caso* pq. *Chegamos a conclusão que* G *tem so um unico* p*-sugrupo de sylow, logo é normal em* G, *e portanto* G *é soluvel. As cardinalidades desse caso são:*

$$|G| = 12, 18, 20, 28, 44, 45, 50, 52$$

Acabaram de certa forma os casos, e agora precisamos verificar as caridinalidades que faltam. $|G| = 24$*: Vamos mostrar que* $|G| = 24$ *não é simples.* $24 = 2^3 3$. *Pelo Terceiro Teorema de Sylow,* $n_2 = 1$ *ou* n_2. *Se* $n_2 = 1$, *então* G *não é simples e portanto é soluvel. Assuma então* $n_2 = 3$ G *agindo por conjugação em 2-subgrupo de sylow, conseguimos um homomorfismo* $\varphi : G \to S_3$. *Como* $24 = |G| > |S_3| = 6$, *temos que o nucleo de* φ *não é trivial e normal.* $|G| = 36$*: Novamente por sylow,* $n_3 = 1$ *ou* $n_3 = 4$. $n_3 = 1$ *é de novo não simples. Seja então* $n_3 = 4$, *e por uma ação por conjugação semelhante ao caso anterior e* G *não é simples e então soluvel.* $|G| = 40 = 2^3 5$*:* $n_5 \equiv 1 \mod 5$ *e* $n_5|2^3$, *então por força* $n_5 = 1$. *Então o 5-sugbrupo de sylow é unico e* G *é normal e portanto soluvel.* $|G| = 48 = 2^4 3$*: Se* $n_2 = 3$ *ou* $n_3 = 4$, *então temos um homomorfismo com kernel não trivial se agirmos* G *por conjugação em 2-subgrupo de sylow de* G *ou 3-subgrupo de sylow de* G, *respectivamente.* $|G| = 54 = 2 \cdot 3^3$*:* $n_3 \equiv 1 \mod 3$ *e* $n_3|2$, *logo* $n_3 = 1$ *e portanto o 3-sugbrupo é unico e normal.* $|G| = 56 = 2^3 \cdot 7$*: Se* $n_2 = 1$ *ou* $n_7 = 1$. *Então* $n_7 = 8$ *Cada 7-subgrupo de sylow tem 7 elementos e todos eles se intersectam somente no elemento neutro, logo* G *tem* $8(7-1) = 48$ *elementos distintos de ordem 7. Logo é normal e portanto soluvel.*