

Matematik, KTH

Bengt Ek

januari 2014

preliminär version

MATERIAL TILL KURSEN  
SF1662, DISKRET MATEMATIK FÖR CLGYM1, TSVDK2:

# Om grupperns verkan på mängder

## Inledning.

Som en ”tillämpning” av den gruppteori vi har lärt oss skall vi studera ett sätt att använda den för att bl.a. lösa vissa kombinatoriska problem.

**Ett typiskt exempel:** Antag att vi skall färga varje sida av en kub med en av två färger, röd och blå. På hur många olika sätt kan det ske? Två färgningar betraktas här som olika precis om man inte kan rotera kuber med de färgningarna så att kuberna efter rotation ser exakt lika ut.

Det finns förstås bara ett sätt att färga alla sidor röda och också ett sätt att färga alla blåa. Med en sida blå och resten röda kan man också bara färga på ett sätt (man kan ju rotera kuben t.ex. så, att den blå sidan är överst), liksom med en röd och resten blåa. Med två blåa och fyra röda går det på två sätt, med de två blåa mittemot varandra eller kant i kant. Likaså med två röda och fyra blåa. Återstår fallet med tre av varje färg. Också i det fallet går det på precis två olika sätt, två röda måste ligga kant i kant och bara två val av den tredje röda ger väsentligt olika färgningar (antingen med alla sidor kring ett hörn röda eller med två motstående sidor och en till röda). Totalt blir det  $1 + 1 + 2 + 2 + 2 + 1 + 1 = 10$  olika färgningar.

Så, det gick bra att få fram antalet med lite funderande, men hur många olika färgningar finns det om man har tre färger (röd, blå och grön)? Om man har  $k$  färger? Om man färgar sidorna av en ikosaeder i stället? Om man färgar både hörnen och sidorna (med  $k$  respektive  $l$  färger)?

Det går förstås att lösa de mer komplicerade problemen med resonemang, liknande det vi gjorde nyss, men det blir ganska krångligt. Nedan skall vi se hur man kan lösa den typen (och en del andra) av problem systematiskt, med hjälp av gruppteori. För det behöver vi först studera hur en grupp kan verka på en mängd (som t.ex. elementen i kubens symmetrigrupp roterar kuben).

## Grupper som verkar på mängder

Flera av de grupper vi bekantat oss med i kursen har varit definierade som mängder av funktioner, med gruppoperationen tolkad som sammansättning av funktioner. T.ex. består  $G_{\square}$  av vissa funktioner (rotationer och speglingar) som avbildar planet på sig själv och  $S_n$  består av bijektioner av mängden  $\{1, 2, \dots, n\}$  på sig själv. Vi formaliserar nu vad vi menar med att en grupp verkar på en mängd.

**Definition:** En **verkan av gruppen  $G$  på mängden  $X$**  består av en funktion  $\varphi : G \times X \rightarrow X$  med egenskaperna

- 1:  $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ , för alla  $g, h \in G$  och alla  $x \in X$ ,
- 2:  $\varphi(1, x) = x$  för alla  $x \in X$  (1 är identitets-elementet i  $G$ )

Normalt använder man ett enklare skrivsätt och undviker  $\varphi$ , genom att skriva  $gx$  i stället för  $\varphi(g, x)$ . Kom dock ihåg att  $gx$  (oftast) **inte** står för en produkt i gruppen  $G$ , i allmänhet är  $x \notin G$ . Med detta enklare skrivsätt blir villkoren ovan

- 1:  $g(hx) = (gh)x$ , för alla  $g, h \in G$  och alla  $x \in X$ ,
- 2:  $1x = x$  för alla  $x \in X$  (1 är identitets-elementet i  $G$ )

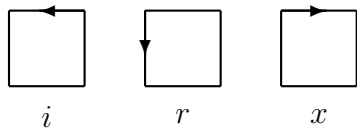
Elementen i  $G$  "tolkas" alltså som bijektioner ( $g^{-1}(gx) = g(g^{-1}x) = 1x = x$  för alla  $g \in G, x \in X$ ) av  $X$  på  $X$  (dvs permutationer), med gruppoperationen "representerad" som sammansättning av funktioner.

**Definition:** Om  $G$  verkar på  $X$  och  $x \in X$  kallas  $G_x = \{g \in G \mid gx = x\}$  för **stabilisatorn för  $x$** .

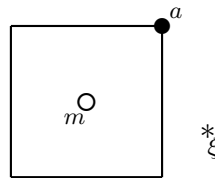
**Sats:** Om  $G$  verkar på  $X$  och  $x \in X$  är  $G_x$  **en delgrupp** till  $G$ .

**Ty:** 1.  $G_x \neq \emptyset$  ( $1x = x$ ), 2.  $g, h \in G_x \Rightarrow gh \in G_x$  ( $(gh)x = g(hx) = gx = x$ ) och 3.  $g \in G_x \Rightarrow g^{-1} \in G_x$  ( $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1x = x$ ) visar att  $G_x \subseteq G$  är en delgrupp till  $G$ .

**Exempel:** Minns  $G_{\square} = \{i, r, r^2, r^3, x, xr, xr^2, xr^3\}$  där  $x$  och  $r$  verkar enligt:



Punkterna  $a, m, \xi$  i figuren t.h. har stabilisatorerna  $G_a = \{i, xr\}$ ,  $G_m = G_{\square}$ ,  $G_{\xi} = \{i\}$



**Exempel:** Om  $S_3$  som vanligt är gruppen av permutationer av  $\{1, 2, 3\}$ , är  $(S_3)_1 = \{id, (23)\}$ .

**Definition:** Om  $G$  verkar på  $X$  och  $x \in X$  är **banan** för  $x$  (eller trajektorian, eng. orbit) mängden  $Gx = \{gx \mid g \in G\}$ .

Observera att beteckningarna är förrädiskt lika, men medan  $G_x \subseteq G$  (t.o.m. en delgrupp) är  $Gx \subseteq X$ .

Om man definierar en binär relation  $\sim$  på  $X$  enligt  $x \sim y$  omm det finns  $g \in G$  med  $y = gx$  är  $\sim$  en ekvivalensrelation och  $Gx$  ekvivalensklassen som innehåller  $x$ .

**Definition:** Om  $G$  verkar på  $X$  och  $x, y \in X$ , låt

$$G_{x \rightarrow y} = \{g \in G \mid gx = y\}.$$

Speciellt är tydligen  $G_{x \rightarrow x} = G_x$ .

**Sats:** Om  $G$  verkar på  $X$  och  $x, y \in X$ ,  $h \in G_{x \rightarrow y}$  gäller

$$G_{x \rightarrow y} = hG_x = G_yh.$$

**Ty:**  $g \in hG_x \Rightarrow g = hg'$  med  $g' \in G_x$ , så  $gx = h(g'x) = hx = y$  och  $g \in G_{x \rightarrow y}$ ,  
 $g \in G_{x \rightarrow y} \Rightarrow h^{-1}g \in G_x$ , och  $g \in hG_x$ . Så både  $hG_x \subseteq G_{x \rightarrow y}$  och  $G_{x \rightarrow y} \subseteq hG_x$ .  
 $G_{x \rightarrow y} = G_yh$  visas på motsvarande sätt.

$G_{x \rightarrow y}$  är alltså både vänster- och högersidoklass, normalt till olika delgrupper.

Man får att  $|G_{x \rightarrow y}| = \begin{cases} |G_x| & \text{om } y \in Gx \\ 0 & \text{om } y \notin Gx, \end{cases}$  ty i det första fallet är  $G_{x \rightarrow y}$  en sidoklass till  $G_x$  och i det andra fallet är  $G_{x \rightarrow y} = \emptyset$ , ty  $y \neq gx$  för alla  $g \in G$ .

**Sats:** Om gruppen  $G$  verkar på mängden  $X$  och  $x \in X$  gäller

$$|G| = |G_x| \cdot |Gx|.$$

**Ty:** Varje vänstersidoklass till  $G_x$  har  $|G_x|$  st element och är som vi sett  $hG_x = G_{x \rightarrow hx}$ . Deras antal är lika med antalet olika  $hx$ , dvs  $|Gx|$ .

**Exempel:** Hur många rotationssymmetrier har en kub?

Kalla gruppen av kubens rotationssymmetrier för  $G$  och låt  $x$  vara ett av kubens hörn. Då består  $G_x$  av de rotationer som lämnar  $x$  invariant, dvs de tre rotationerna  $(0, \pm \frac{2\pi}{3})$  kring en axel genom kubens medelpunkt och hörnet  $x$ . Så  $|G_x| = 3$ . Banan för  $x$  består av alla punkter som  $x$  kan roteras till av symmetrier, tydligen alla kubens hörn, så  $|Gx| = 8$ . Alltså är  $|G| = 3 \cdot 8 = 24$ .

Alternativt: Låt  $x$  vara mittpunkten på en av kubens sidor. Då är i stället  $|G_x| = 4$  (rotationer  $0, \pm \frac{\pi}{4}, \pm \frac{3\pi}{4}$  kring en axel genom medelpunkten och  $x$ ) och  $|Gx| = 6$  (banan består av alla sidornas medelpunkter). Så  $|G| = 4 \cdot 6 = 24$ .

Om man låter  $x$  vara mittpunkten på en kant får man p.s.s.  $|G| = 2 \cdot 12 = 24$ .

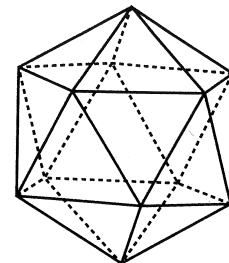
Man kan också räkna elementen i  $G$ : 1 identitetsavbildning, 8 rotationer  $\frac{2\pi}{3}$  kring axlar genom motstående hörn, 6 rotationer  $\frac{\pi}{2}$  och 3 rotationer  $\pi$  kring axlar genom motstående sidoytors mittpunkter och 6 rotationer  $\pi$  kring axlar genom motstående kanters mittpunkter.  $|G| = 1 + 8 + 6 + 3 + 6 = 24$ .

**Exempel:** Hur många rotationssymmetrier har en ikosaeder?

Kalla ikosaederns symmetrigrupp för  $G$  och låt  $x$  vara ett av hörnen. Då består  $G_x$  av de rotationer som lämnar  $x$  invariant, dvs de fem rotationerna  $(0, \pm \frac{2\pi}{5}, \pm \frac{4\pi}{5})$  kring en axel genom ikosaederns medelpunkt och hörnet  $x$ . Så  $|G_x| = 5$ . Banan för  $x$  består av alla punkter som  $x$  kan roteras till av symmetrier, tydligen alla hörnen, så  $|Gx| = 12$ . Alltså är  $|G| = 5 \cdot 12 = 60$ .

Som för kuben kan man alternativt låta  $x$  vara mittpunkten på en sidoyta eller en kant och få  $|G| = 3 \cdot 20$  respektive  $|G| = 2 \cdot 30$ .

Man kan också räkna elementen i  $G$ : 1 identitetsavbildning, 12 rotationer  $\frac{2\pi}{5}$  och 12 rotationer  $\frac{4\pi}{5}$  kring axlar genom motstående hörn, 20 rotationer  $\frac{2\pi}{3}$  kring axlar genom motstående sidoytors mittpunkter och 15 rotationer  $\pi$  kring axlar genom motstående kanters mittpunkter.  $|G| = 1 + 12 + 12 + 20 + 15 = 60$ .



## Bevis med hjälp av gruppverkan

Vi ger två exempel på hur man kan använda resonemang om gruppverkan och deras banor för att bevisa satser, dels för ett resultat om centrum för grupper av ordning  $p^n$ ,  $p$  ett primtal och  $n \geq 1$ , och dels Fermats sats om primtal som kan skrivas som en summa av två kvadrater.

### Grupper av ordning $p^n$ , $p$ primtal

Låt  $p$  vara ett primtal och  $G$  en grupp med  $|G| = p^n$ , där  $n \in \mathbb{Z}_+$ .

Vi minns att  **$Z(G)$ , centrum för  $G$** , består av de element i  $G$  som kommuterar med alla  $G$ 's element, dvs  $Z(G) = \{z \in G \mid zg = gz \text{ för alla } g \in G\}$ .

$G$  verkar på sig själv med **konjugering**,  $g(h) = ghg^{-1}$  för  $g \in G$ ,  $h \in X(=G)$  (vi skriver förstås  $g(h)$ , i stället för  $gh$ , för att inte förväxla det med gruppoperationen). Eftersom  $ghg^{-1} = h \Leftrightarrow gh = hg$  är med denna verkan  $G_h = \{g \in G \mid gh = hg\} = C(h)$ , centralisatorn till  $h$  i  $G$ . Speciellt gäller, om  $G(h)$  betecknar banan för  $h$ , att

$$h \in Z(G) \Leftrightarrow |G(h)| = 1,$$

ty  $|G| = |G_h| \cdot |G(h)| = |C(h)| \cdot |G(h)|$  och  $h \in Z(G) \Leftrightarrow C(h) = G$ .

Eftersom  $|G_h| \cdot |G(h)| = |G| = p^n$  är  $|G(h)| = p^k$  för något  $k \geq 0$ , alla  $h \in G$ . Om vi tar ett element  $h_i$  i varje bana och sätter  $|G(h_i)| = p^{k_i}$ , består  $Z(G)$  precis av de  $h_i$  som har  $k_i = 0$ .  $X(=G)$  är en disjunkt union av banorna, så

$$p^n = |G| = \sum_i |G(h_i)| = \sum_i p^{k_i} = |Z(G)| + \sum_{i \text{ med } k_i > 0} p^{k_i}.$$

Här är VL och andra termen i HL båda delbara med  $p$ , så det är  $|Z(G)|$  också!  $1 \in Z(G)$ , så  $|Z(G)| > 0$  och vi har visat

**Sats:** Om  $G$  är en grupp,  $|G| = p^n$ ,  $p$  ett primtal och  $n \in \mathbb{Z}_+$ , är  $|Z(G)| \geq p$ .

**Exempel:** För kvadratens symmetrigrupp  $G_\square$  fann vi  $|G_\square| = 8 = 2^3$ , så enligt satsen är  $|Z(G_\square)| \geq 2$ . Det stämmer, vi vet ju att  $Z(G_\square) = \{i, r^2\}$ .

Då  $n = 2$  kan vi säga mer. Om  $|G| = p^2$  är  $|Z(G)|$  enligt ovan  $p$  eller  $p^2$ . Antag att  $|Z(G)| = p$  och att  $g \in G \setminus Z(G)$ .  $Z(G) \subseteq C(g)$  och  $g \in C(g)$ , så  $|C(g)| > p$  och därför  $C(g) = G$  ( $|C(g)| \mid |G|$ , ty  $C(g)$  är en delgrupp till  $G$ ) och alltså  $g \in Z(G)$ , motsägelse. Så  $|Z(G)| = p^2$ , dvs  $Z(G) = G$  och det följer

**Följdsats:** Om  $G$  är en grupp,  $|G| = p^2$  och  $p$  ett primtal, är  $G$  abelsk.

### Om summor av två heltalskvadrater

I materialet "Mer om faktorisering" nämndes Fermats sats att varje primtal  $p$  som är  $\equiv 1 \pmod{4}$  kan skrivas som en summa av två kvadrater (av heltal). Vi skall visa det. Vi kommer att använda resultat om faktorisering i  $\mathbb{Z}[i]$ , så det kan vara bra att repetera det.

**Hjälpsats:** Ett primtal  $p$  kan skrivas som en summa av två kvadrater om och endast om det är reducibelt i  $\mathbb{Z}[i]$ , de gaussiska heltalen.

**Ty:** ( $\Rightarrow$ .) Om  $p = a^2 + b^2$  är  $p = (a + bi)(a - bi)$  och ingen av faktorerna är en enhet i  $\mathbb{Z}[i]$ .

( $\Leftarrow$ .) Om  $p = (a + bi)(c + di)$ , där ingen av faktorerna är en enhet i  $\mathbb{Z}[i]$ , är  $p^2 = |p|^2 = (a^2 + b^2)(c^2 + d^2)$  och  $a^2 + b^2, c^2 + d^2 > 1$ . Då är  $a^2 + b^2 = c^2 + d^2 = p$  (och  $c + di = a - bi$ ).

För att visa att ett godtyckligt primtal  $\equiv_4 1$  är reducibelt i  $\mathbb{Z}[i]$  använder vi ett fiffigt resonemang om banor, liknande det vi förde i det förra avsnittet. Låt  $X$  vara mängden  $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$  och definiera  $\lambda, \mu, \nu : X \rightarrow X$  enligt  $\lambda(x) = -x$ ,  $\mu(x) = x^{-1}$  och  $\nu(x) = -x^{-1}$  (räknat i  $\mathbb{Z}_p$ ). Eftersom  $\lambda^2 = \mu^2 = id$  och  $\lambda\mu = \mu\lambda = \nu$  är  $G = \{1, \lambda, \mu, \nu\}$  en abelsk grupp,  $\approx (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ , och  $G$  verkar på  $X$ .

För att se hur stora motsvarande banor  $Gx$  kan vara, ser vi vilka stabilisatorer  $G_x$  som finns. Det finns inget  $x \in X$  med  $x = \lambda(x)$ , ty  $x = -x \Rightarrow 2x = 0$  och det är omöjligt i  $\mathbb{Z}_p$  då  $x \neq 0$  och  $p$  är udda.  $x = \mu(x)$  betyder att  $x = x^{-1}$ , dvs  $x^2 - 1 = (x + 1)(x - 1) = 0$ , med lösningarna  $x = \pm 1$  och inga andra.  $x = \nu(x)$  slutligen betyder  $x = -x^{-1}$ , dvs  $x^2 + 1 = 0$ .  $x^2 + 1 = y^2 + 1 \Leftrightarrow y^2 - x^2 = (y + x)(y - x) = 0 \Leftrightarrow y = \pm x$ . Det finns alltså inget eller precis två  $x \in X$  som uppfyller  $x = \nu(x)$ .

De enda banorna i  $X$  som inte har 4 element är alltså  $\{1, -1\}$  (finns säkert) och  $\{x, -x\}$ , där  $x^2 = -1$  (finns kanske). Men antalet element i  $X$  är  $p - 1$ , som är delbart med 4, och  $X$  är en disjunkt union av banorna. Det betyder att det verkligen finns ett  $x \in \mathbb{Z}_p$  med  $x^2 + 1 = 0$  i  $\mathbb{Z}_p$ .  $x$  som element i  $\mathbb{Z}$  uppfyller alltså  $p \mid x^2 + 1 = (x + i)(x - i)$  i  $\mathbb{Z}[i]$ . Om  $p$  vore irreducibelt i  $\mathbb{Z}[i]$  skulle  $p \mid (x + i)$  eller  $p \mid (x - i)$ , men ingendera kan gälla, ty  $p \nmid 1$ . Med hjälpsatsen ovan får vi alltså

**Sats (Fermat):** Om  $p$  är ett primtal,  $p \equiv_4 1$ , finns  $a, b \in \mathbb{Z}$  så att  $p = a^2 + b^2$ .

(Eftersom faktoriseringen av  $p$  i  $\mathbb{Z}[i]$  är entydig, är  $\{a, b\}$  entydigt bestämd (bortsett från tecken).)

$2 = 1^2 + 1^2$  och eftersom en summa av två heltalskvadrater är  $\equiv_4 0, 1$  eller  $2$ , kan inget tal  $\equiv_4 3$  skrivas som en sådan summa. Å andra sidan är  $21 \equiv_4 1$ , men  $21$  är inte en summa av två kvadrater, och  $65$  är inte ett primtal, men  $65 = 8^2 + 1^2 = 7^2 + 4^2$ . Vilka naturliga tal  $n$ , primtal eller inte, är summor av två kvadrater?

För att besvara den frågan utnyttjar vi våra kunskaper om faktorisering i  $\mathbb{Z}[i]$ . Om  $n = a^2 + b^2 = (a + bi)(a - bi)$ , faktorisera  $a + bi$  i gaussiska primtal.  $a + bi = u(1 + i)^k g_1 \dots g_l \cdot p_1 \dots p_m$ , där  $u$  är en enhet,  $k, l, m \in \mathbb{N}$ ,  $|g_i|^2$  är primtal  $\equiv_4 1$  och  $p_j$  är primtal  $\equiv_4 3$ . Då är den reella primtalsfaktoriseringen  $n = 2^k |g_1|^2 \dots |g_l|^2 p_1^2 \dots p_m^2$  och omvänt, om  $n$  har denna form (med jämna potenser av alla primtal som är  $\equiv_4 3$ ) kan det faktoriseras som  $n = (a + bi)(a - bi) = a^2 + b^2$ , så

**Sats:** Om  $n \in \mathbb{N}$  finns  $a, b \in \mathbb{N}$  så att  $n = a^2 + b^2$  omm alla primtal som är  $\equiv_4 3$  förekommer med jämn potens i  $n$ .

**Exempel:**  $65 = 5 \cdot 13 = (2 + i)(2 - i)(3 + 2i)(3 - 2i) = [(2 + i)(3 + 2i)][(2 - i)(3 - 2i)] = (4 + 7i)(4 - 7i) = [(2 - i)(3 + 2i)][(2 + i)(3 - 2i)] = (8 + i)(8 - i)$ . Som i exemplet inser man att uppdelningen i två kvadrater är (väsentligen) unik precis om högst en primfaktor i  $n$  är  $\equiv_4 1$ .

## Antalet banor då $G$ verkar på $X$

Vi skall härleda ett enkelt uttryck för antalet banor då gruppen  $G$  verkar på mängden  $X$ . I nästa avsnitt skall vi se hur vi kan använda det för att finna t.ex. antalet väsentligt olika färgningar av kubens sidor.

Om vi summerar  $\frac{1}{|Gx|}$  för alla  $x \in X$  kommer termerna från alla  $x$  i samma bana att ge exakt 1, så hela summan ger antalet banor ( $|Gx|$  är ju antalet element i  $x$ 's bana). Genom att använda att  $|G| = |Gx| \cdot |G_x|$ , så  $\frac{1}{|Gx|} = \frac{|G_x|}{|G|}$ , får vi antalet banor för  $G$ 's verkan på  $X$ :

$$\sum_{x \in X} \frac{1}{|Gx|} = \frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{x \in X} \sum_{\substack{g \in G \\ gx=x}} 1 = \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{x \in X \\ gx=x}} 1 = \frac{1}{|G|} \sum_{g \in G} |X_g|,$$

där  $X_g = \{x \in X \mid gx = x\}$ , de  $x$  som inte ändras då  $g$  verkar, så

**Sats (Burnsides lemma):** Om  $G$  verkar på  $X$  är antalet banor

$$\frac{1}{|G|} \sum_{g \in G} |X_g|, \text{ där } X_g = \{x \in X \mid gx = x\}.$$

(Kallas "Burnsides lemma", trots att Burnside varken upptäckte det eller påstod sig ha gjort det.)

## $G$ verkar på en färgning av en mängd

Hittills har vi betraktat en grupp  $G$  som verkar på en mängd som varit en geometrisk figur eller liknande. För att kunna använda vår teori för att beräkna antal olika färgläggningar av t.ex. en kub, inför vi nu mängden av färgningar av ett objekt (eller en mängd).

Om  $G$  verkar på en mängd  $M$  (t.ex. mängden av de sex sidoytorna på en kub) verkar  $G$  också på  $C^M = \{f : M \rightarrow C\}$ , mängden av  $C$ -värda funktioner på  $M$ , enligt

$$(gf)(m) = f(g^{-1}m),$$

dvs så att värdena "följer med" i  $G$ 's verkan ( $f(g^{-1}m)$  är värdet i den punkt som efter  $g$ 's verkan hamnar i  $m$ ).

Om  $C$  är en mängd färger är  $C^M$  mängden av färgningar av  $M$  och banorna svarar mot de "väsentligt olika" färgningarna (dvs sådana som inte kan överföras i varandra med något  $g \in G$ ).

Detta definierar en verkan på  $C^M$ , ty för  $f, g, 1 \in G$ ,  $f \in C^M$ ,  $m \in M$ :

$$((gh)f)(m) = f((gh)^{-1}m) = f(h^{-1}g^{-1}m) = (hf)(g^{-1}m) = (g(hf))(m), \text{ så } (gh)f = g(hf) \text{ och } (1f)(m) = f(1^{-1}m) = f(m), \text{ så } 1f = f.$$

I exemplen nedan är mängden  $X$  som  $G$  verkar på nu  $C^M$ , mängden av "färgningar" av någon mängd  $M$  (t.ex. sidorna på en kub, pärlor).

**Exempel:** På hur många (väsentligt olika) sätt kan en kubs ytor färgas med högst  $k$  olika färger (ytorna enfärgade, förstås)?

Vi söker nu antalet banor då  $G$  (symmetrigruppen av rotationer för kuben) verkar på mängden  $X$  av färgningar av kubens sidor. Enligt Burnsidess lemma är det antalet  $\frac{1}{|G|} \sum_{g \in G} |X_g|$ , där  $|X_g|$  nu är antalet färgningar som inte ändras då  $g$  roterar kuben.

Enligt ett tidigare exempel är  $|G| = 24$  och man får  $|X_g|$  för olika typer av  $g$ :

| rotationsvinkel  | axel genom | antal $g$ | $ X_g $                                    |
|------------------|------------|-----------|--------------------------------------------|
| 0                | —          | 1         | $k^6$ ( $g = 1$ , så alla färgningar)      |
| $\frac{2\pi}{3}$ | hörn       | 8         | $k^2$ (ytorna likfärgade 3 och 3 i $X_g$ ) |
| $\pi$            | sidmitt    | 3         | $k^4$ (2 par av likfärgade ytor)           |
| $\frac{\pi}{2}$  | sidmitt    | 6         | $k^3$ (4 ytor har samma färg)              |
| $\pi$            | kantmitt   | 6         | $k^3$ (ytorna parvis likfärgade)           |

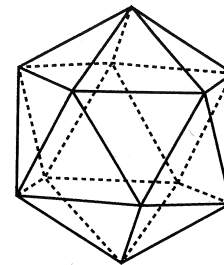
(Alla rotationsaxlarna går förstås genom kubens mittpunkt.)

Det sökta antalet färgningar är alltså

$$\frac{1}{24}(k^6 + 8k^2 + 3k^4 + 6k^3 + 6k^3) = \frac{1}{24}(k^6 + 3k^4 + 12k^3 + 8k^2).$$

$k = 2$  ger 10 (som i exemplet i inledningen),  $k = 3$  ger 57,  $k = 4$  ger 240 etc.

**Exempel:** För vart och ett av de 12 hörnen av en ikosaeder väljs en färg på en kula som placeras där. Hur många (väsentligt olika) fördelningar av färgerna finns det, om man har  $k$  olika färger på kulor att tillgå? (Detta antal är detsamma som antalet sätt att färga sidoytorna på en dodekaeder med högst  $k$  färger.)



Vi söker nu antalet banor då  $G$  (symmetrigruppen av rotationer för ikosaedern,  $|G| = 60$ ) verkar på mängden  $X$  av färgningar av ikosaederns hörn. Som i det förra exemplet, men med ett annat  $G$  fås:

| rotationsvinkel  | axel genom | antal $g$ | $ X_g $                                  |
|------------------|------------|-----------|------------------------------------------|
| 0                | —          | 1         | $k^{12}$ ( $g = 1$ , så alla färgningar) |
| $\frac{2\pi}{5}$ | hörn       | 12        | $k^4$ (hörnen likfärgade 1, 5, 5 och 1)  |
| $\frac{4\pi}{5}$ | hörn       | 12        | $k^4$ (som förra)                        |
| $\frac{2\pi}{3}$ | sidmitt    | 20        | $k^4$ (hörnen likfärgade 3, 3, 3 och 3)  |
| $\pi$            | kantmitt   | 15        | $k^6$ (hörnen parvis likfärgade)         |

(Alla rotationsaxlarna går genom ikosaederns mittpunkt.)

Det sökta antalet färgningar är alltså

$$\frac{1}{60}(k^{12} + 12k^4 + 12k^4 + 20k^4 + 15k^6) = \frac{1}{60}(k^{12} + 15k^6 + 44k^4).$$

$k = 2$  ger 96,  $k = 3$  ger 9099,  $k = 4$  ger 280 832 etc.

**Exempel:** Hur många väsentligt olika armband kan man skapa genom att trä upp 6 svarta, 3 vita och en röd pärla på en tråd (och knyta ihop till en ögla)? Knuten kan röra sig genom pärlorna och har ingen riktning.

Vi kan tänka oss pärlorna i hörnen av en regelbunden (plan) 10-hörning och symmetrigruppen  $G$  består av identiteten, rotationer  $\frac{\pi}{5}, \frac{2\pi}{5}, \dots, \frac{9\pi}{5}$  kring en axel genom mittpunkten vinkelrät mot planet och rotationer  $\pi$  (5 st kring axlar genom motstående hörn och 5 st kring axlar genom motstående sidor).

| rotation         | axel      | antal $g$ | $ X_g $                                                                          |
|------------------|-----------|-----------|----------------------------------------------------------------------------------|
| 0                | —         | 1         | $\binom{10}{6,3,1} = 840$ ( $g = 1$ , så alla färgningar)                        |
| $\frac{n\pi}{5}$ | mitten    | 9         | 0 (den röda flyttas)                                                             |
| $\pi$            | hörn-hörn | 5         | $2 \cdot 4 = 8$ (vilket axelhörn rött? andra vitt, vilket av 4 övriga par vita?) |
| $\pi$            | sida-sida | 5         | 0 (den röda flyttas)                                                             |

Burnsides lemma ger det sökta antalet:  $\frac{1}{20}(840 + 9 \cdot 0 + 5 \cdot 8 + 5 \cdot 0) = \mathbf{44 \text{ st.}}$