Groupe produit-Groupe quotient
Factorisation des morphismes

I. Groupe produit

Théorème
Soient $(E,*)$ et $(F,\perp)$ deux groupes.
L'ensemble $E\times F=\{(a,b)\ /\ a\in E, b\in F\}$ muni de la loi de composition $\otimes$ suivante :
Pour $(a,b)\in E\times F$, $(a',b')\in E\times F$, $(a,b)\otimes(a',b')=(a*a', b\perp b')$
est un groupe appelé groupe produit direct des groupes $(E,*)$ et $(F,\perp)$.

Preuve. à faire en exercice.

Exemples
1) Le groupe $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$, appelé groupe de Klein, est le groupe direct des groupes $(\mathbf{Z}/2\mathbf{Z},+)$ et $(\mathbf{Z}/2\mathbf{Z},+)$.
Donner la table de Cayley du groupe de Klein

2) $\Omega_n{}^2$ est le groupe direct des groupes $(\Omega_n,\times)$ et $(\Omega_n,\times)$ où $\Omega_n=\{z\in\mathbf{C}\ /\ z^n=1\}$
Donner la table de Cayley du groupe $\Omega_2{}^2$

II. Groupe quotient

Pour simplifier la présentation (éviter de parler des sous-groupes distingués) on se place dans la **suite dans le cas où la loi de composition « $*$ » est commutative.**

Soit $(G,*)$ un groupe **abélien** et $(H,*)$ un sous-groupe de $(G,*)$.
On définit sur G la relation binaire suivante :
Pour $(x,y)\in G^2$, $x\,\mathrm{R}\,y$ si et seulement si $(x*y^{-1})\in H$

Propriété et définition
La relation R est une relation d'équivalence sur G.
L'ensemble quotient $G/\ \mathrm{R}\ =\{\overline{x}\ /\ x\in G\}$ est noté G/H où $\overline{x}=\{y\in G\ /\ x\,\mathrm{R}\,y\}$

Preuve.
Vérifier que R est réflexive, symétrique et transitive

Remarques (importantes)
1) $a\in G/H \Leftrightarrow \exists x_a\in G, a=\overline{x_a}$
Idem $b\in G/H \Leftrightarrow \exists x_b\in G, b=\overline{x_b}$
de plus si $x'_a\in G$ tel que $a=\overline{x_a}=\overline{x'_a}$ et $x'_b\in G$ tel que $b=\overline{x_b}=\overline{x'_b}$
Alors on a $(x_a*x'_a{}^{-1})\in H$ et $(x_b*x'_b{}^{-1})\in H$ D'où $(x_a*x'_a{}^{-1})*(x_b*x'_b{}^{-1})\in H$ car $(H,*)$ est un groupe.

Et puisque la loi « $*$ » est commutative, alors $(x_a * x_b) * (x'_a * x'_b)^{-1} \in H$

C'est-à-dire $\overline{x_a * x_b} = \overline{x'_a * x'_b}$

Ainsi on peut définir une loi de composition interne dans G/H notée aussi « $*$ » par :

Pour $\overline{x_a} \in G/H$ et $\overline{x_b} \in G/H$, $\overline{x_a} * \overline{x_b} = \overline{x_a * x_b}$

2) La propriété ci-dessus est encore vrai si la loi « $*$ » n'est pas commutative et en supposant que $(H,*)$ est un sous-groupe distingué de $(G,*)$, c'est-à-dire, si pour tout

$\forall a \in G, \forall h \in H, (a * h * a^{-1}) \in H$

Théorème

Soient $(G,*)$ un groupe **abélien** et $(H,*)$ un sous-groupe de $(G,*)$, alors l'ensemble $(G/H,*)$ est un groupe abélien.

De plus l'application canonique $\pi : G \to G/H$ définie par $\forall x \in G, \pi(x) = \overline{x}$ est un homomorphisme surjectif

Preuve. à faire en exercice

Exemple

Soit $n \in \mathbf{N}^*$, $(\mathbf{Z},+)$ est un groupe abélien et $(n\mathbf{Z},+)$ est un sous-groupe de $(\mathbf{Z},+)$.

Pour $(a,b) \in \mathbf{Z}^2$, $a \equiv b\,[n] \Leftrightarrow n \mid (b-a) \Leftrightarrow \exists k \in \mathbf{Z}, b-a = k\,n \Leftrightarrow (a-b) \in n\mathbf{Z}$

$(\mathbf{Z}/n\mathbf{Z},+)$ est le groupe quotient muni de la loi additive définie par :

Pour $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ et $\overline{y} \in \mathbf{Z}/n\mathbf{Z}$, $\overline{x} + \overline{y} = \overline{x+y}$

III. Factorisation des morphismes

Théorème

Soient $(G,*)$ un groupe et $(H,*)$ un sous-groupe distingué de $(G,*)$, alors l'ensemble $(G/H,*)$ est un groupe.

De plus l'application canonique $\pi : G \to G/H$ définie par $\forall x \in G, \pi(x) = \overline{x}$ est un homomorphisme surjectif

Théorème

Soients $(G,*)$ et $(\mathrm{F},\perp)$ deux groupes et $\varphi : G \to F$ un morphisme de groupes,

Alors $(Ker\varphi,*)$ est un sous-groupe distingué de $(G,*)$.

Preuve. à faire en exercice

Théorème d'isomorphisme

Soients $(G,*)$ et $(\mathrm{F},\perp)$ deux groupes et $\varphi : G \to F$ un morphisme de groupes,

Alors il existe un morphisme bijectif (c-à-d isomorphisme) $\tilde{\varphi} : G/Ker\varphi \to \mathrm{Im}(\varphi)$ vérifiant :

$\varphi = i \circ \tilde{\varphi} \circ \pi$ où $\pi : G \to G/Ker\varphi$, $\forall x \in G,\ \pi(x) = \overline{x}$ et $i : \mathrm{Im}(\varphi) \to F$, $\forall x \in \mathrm{Im}(\varphi),\ i(x) = x$

$$
\begin{array}{ccc}
G & \overset{\varphi}{\rightarrow} & F \\
\pi \downarrow & & \uparrow i \\
G/Ker\varphi & \underset{\tilde{\varphi}}{\rightarrow} & \mathrm{Im}(\varphi)
\end{array}
$$

Preuve. à faire en exercice

Définition
Soient $(G,*)$ et $(\mathrm{F},\perp)$ deux groupes, on dit que $(G,*)$ et $(\mathrm{F},\perp)$ sont isomorphes, s'il existe un morphisme bijectif $\varphi : G \to F$, on note alors $G \approx F$

Exemples
1) Soit $\varphi : (\mathbf{R},+) \to (\mathbf{C}^*,\times)$ définie par $\forall \theta \in \mathbf{R},\ \varphi(\theta) = e^{i\theta}$
φ est un morphisme de groupes,
$Ker\varphi = \{2k\pi / k \in \mathbf{Z}\} \overset{noté}{=} 2\pi\,\mathbf{Z}$ et
$\mathrm{Im}(\varphi) = \{e^{i\theta} / \theta \in \mathbf{R}\} = \{z \in \mathbf{C} / |\mathbf{z}| = 1\}$: ensemble des complexes de module 1.
D'où d'après le théorème d'isomorphisme, on a $\mathbf{R}/2\pi\,\mathbf{Z}\ \approx \{z \in \mathbf{C} / |\mathbf{z}| = 1\}$

2) $Ln : (]0,+\infty[,\times) \to (\mathbf{R},+)$ est un isomorphisme de groupes donc $]0,+\infty[\approx \mathbf{R}$

Théorème (caractérisation des groupes cycliques)
Soit $(G,*)$ un groupe cyclique
a) Si G est infini alors G est isomorphe à $\mathbf{Z}$
b) Si G est fini et $ord(G) = n$ alors G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$

Preuve.
$(G,*)$ est un groupe cyclique d'où il existe $a \in G$ tel que $G = < a > = \{a^k / k \in \mathbf{Z}\}$.
On considère $\varphi : (\mathbf{Z},+) \to (G,*)$ définie par : $\forall k \in \mathbf{Z}, \varphi(k) = a^k$
φ est un morphisme de groupes et d'après le théorème d'isomorphisme $\mathbf{Z}/Ker\varphi \approx \mathrm{Im}(\varphi)$
Or $\mathrm{Im}(\varphi) = G$ d'où $\mathbf{Z}/Ker\varphi \approx G$ (1)
De plus $Ker\varphi$ est un sous-groupe du groupe $(\mathbf{Z},+)$ d'où il existe $n \in \mathbf{N}, Ker\varphi = n\mathbf{Z}$

a) Si $n = 0$ alors $\mathbf{Z}/Ker\varphi = \mathbf{Z}/\{0\} \approx \mathbf{Z}$ (car $x \,\mathrm{R}\, y \Leftrightarrow (x-y) \in \{0\} \Leftrightarrow x = y$)
D'où d'après (1) on a : $\mathbf{Z} \approx G$, (G est donc infini)

b) Si $n \neq 0$ alors $\mathbf{Z}/Ker\varphi = \mathbf{Z}/n\mathbf{Z}$
D'où d'après (1) on a : $\mathbf{Z}/n\mathbf{Z} \approx G$, ($G$ est donc fini et $ord(G) = n$)

Conséquence
Deux groupes cycliques de même ordre sont isomorphes

Exemples
1) Soit $\Omega_n = \{z \in \mathbf{C} / z^n = 1\}$, on sait que $(\Omega_n,\times)$ est un groupe cyclique d'ordre n engendré par $e^{\frac{2i\pi}{n}}$ d'où $\mathbf{Z}/n\mathbf{Z} \approx \Omega_n$,

En particulier on a $\Omega_3 = \{1, j, j^2\}$ où $j = e^{\frac{2i\pi}{3}}$ et $\mathbf{Z}/3\mathbf{Z} \approx \Omega_3$

2) Dans S_3 l'ensemble des permutations de $\{1,2,3\}$, on note $A_3 = \{Id, \sigma, \sigma^2\}$ où $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$(A_3,\circ)$ est un groupe cyclique d'ordre 3 car $\sigma^2 \neq Id$ et $\sigma^3 = Id$

D'où $\mathbf{Z}/3\mathbf{Z} \approx A_3$ et d'après 1) on a donc $\mathbf{Z}/3\mathbf{Z} \approx A_3 \approx \Omega_3$

3) Soit $G = \{3^n / n \in \mathbf{Z}\}$, $(G,\times)$ est un groupe cyclique infini d'où $G \approx \mathbf{Z}$ idem $2\mathbf{Z} \approx \mathbf{Z}$

Théorème de Cayley (caractérisation des groupes finis)
Soit $n \in \mathbf{N}^*$ on note S_n l'ensemble des permutations de $\{1, \ldots, n\}$
Si $(G,*)$ est un groupe fini tel que $ord(G) = n$, alors G est isomorphe à un sous-groupe de S_n.

Preuve. ….

Exemples
1) $(\mathbf{Z}/3\mathbf{Z},+)$ est un groupe fini d'ordre 3 et d'après l'exemple 2) ci-dessus on a :
$\mathbf{Z}/3\mathbf{Z} \approx A_3$ où $(A_3,\circ)$ est un sous-groupe de S_3 l'ensemble des permutations de $\{1,2,3\}$.
Idem $\Omega_3 \approx A_3$ où $\Omega_3 = \{z \in \mathbf{C} \ / \ z^3 = 1\}$.
2) Le groupe de Klein $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ est d'ordre 4 donc il est isomorphe à un sous-groupe de S_4. Il faut noté que le groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ n'est pas isomorphe au groupe $\mathbf{Z}/4\mathbf{Z}$ car $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ n'est pas un groupe cyclique puisque pour tout élément
$(a,b) \in \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $(a,b) \neq (0,0)$, $ord((a,b)) = 2$ car $2(a,b) = (0,0)$.
alors que $\mathbf{Z}/4\mathbf{Z}$ est un groupe cyclique.

3) Dans S_4, on considère les éléments suivants :
$Id = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$; $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$; $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ et $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$
On note $G = \{Id, \sigma_1, \sigma_2, \sigma_3\}$ alors $(G,\circ)$ est un sous-groupe de $(S_4,\circ)$ et $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \approx G$.