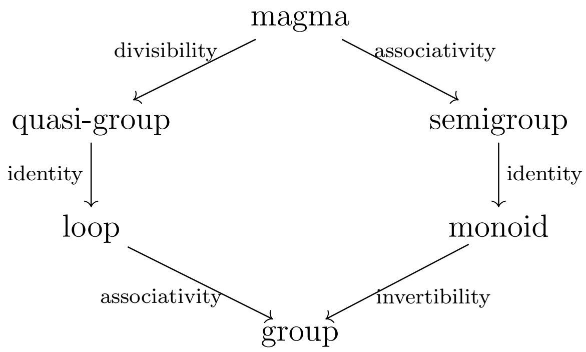
Inverslization

Wang-Hsiuan Pahngerei

2013.06.24

There're two usual ways to "go" from a magma to a group, as the diagram below,



where "divisibility" means for any a, b, $ax = b$ and $ya = b$ admits a unique solution.

Recall that a monoid is a pair $(M, *)$ such that $*$ is associative and has an identity e. Elements of a monoid need not have an inverse, so we hope to "extend" it to a group in some conditions. In fact, this action helps us contruct the Zahlen from the set of natural numbers.

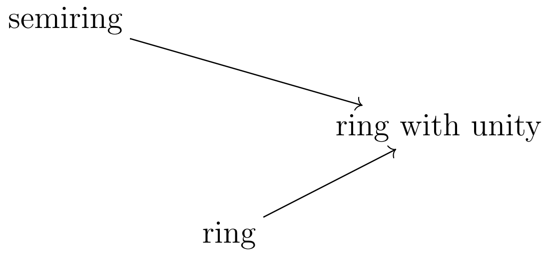
Let us focus on commutative monoids with cancellation law (i.e. $ax = ay$ implies $x = y$). In fact, this is really near a group. Firstly, define a relation $\sim$ on $M \times M$ by $(a, b) \sim (x, y)$ if and only if $a*y = b*x$. This is an equivalence relation because, (i) $a*b = a*b$ so $(a, b) \sim (a, b)$, (ii) $(a, b) \sim (c, d)$ means $a * d = b * c$, so $c * b = a * d$, that is $(c, d) \sim (a, b)$, and (iii) whenever $(a, b) \sim (c, d) \sim (e, f)$, $a * d = b * c$ and $c * f = e * d$, so $c * d * a * f = c * d * b * e$, indicating $a * f = b * e$.

Secondly, let G be the set of equivalence classes. Then we define operation: $[(a, b)] * [(x, y)] = [(a*x, b*y)]$. This is well-defined because, written $(a, b) \sim (a', b')$ and $(x, y) \sim (x', y')$, so we have $a * x * b' * y' = b * a' * x * y' = b * a' * y * x' = b * y * a' * x'$.

Thirdly, $[(1, 1)]$ is the identity of the new "group", and for $[(a, b)] \in G$, $[(b, a)]$ is the inverse. We're going to show that $h : M \to G$ by $a \mapsto [(1, a)]$ is the embedding (one-to-one monoid homomorphism). It's enough to show that h is one-to-one, but this is routine because $[(1, a)] = [(1, b)]$ implies $1 * b = a * 1$.

Now we hope to add in another operation. Recall that a semiring is a pair $(S, +, \cdot)$ such that $(S, +)$ is a commutative monoid with identity 0, $(S, \cdot)$ is a monoid with identity 1, it has both side multiplicative distrubution over addition, and multiplication by 0 annihilates S

$(0 \cdot a = a \cdot 0 = 0)$. We now consider a commutative semiring $(S, +, \cdot)$.



Let $(R, +)$ be the equivalence classes as mentioned above. We hope to add multiplication so that $(R, +, \cdot)$ is a ring. Define

$$[(a, b)] \cdot [(x, y)] = [(ay + bx, ax + by)].$$

It's routine to check well-defined. If $(a, b) \sim (a', b')$ and $(x, y) \sim (x', y')$, then

$$\begin{aligned}(ay + bx)(a'x' + b'y') &= aa'yx' + yy'ab' + xx'ba' + bb'xy' \\ &= aa'xy' + yy'a'b + xx'ab' + bb'x'y = (a'y' + b'x')(ax + by).\end{aligned}$$

Note that the mapping h is again an embedding. Thus we view S as a semi-subring of R. Again, throughout this method, we have the conclusion that $\mathbb{N} \subset \mathbb{Z}$.