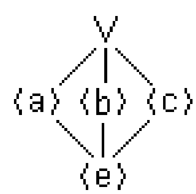
Section 5: Subgroups

In the last section, we learned that a nonempty subset S of a group G was a "subgroup" iff it was closed under the operation in G and under inverses. The text wisely points out that a subset which is a group need not be a subgroup, because the operation may be differqent. For example, $(\mathbb{Q}, +)$ and $(\mathbb{Q}^+, \cdot)$ are both groups, and $\mathbb{Q}^+ \subset \mathbb{Q}$, but $\mathbb{Q}^+$ is not called a subgroup of $\mathbb{Q}$.

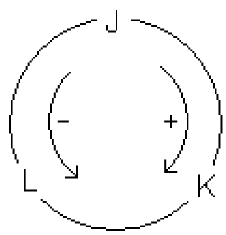
We have already seen that, for any element x of any group G, $\langle x \rangle$ is a subgroup of G. In particular, $\{e\}$ is a subgroup of any group (the "trivial subgroup"); and of course any group is a subgroup of itself. Here are a few other examples:

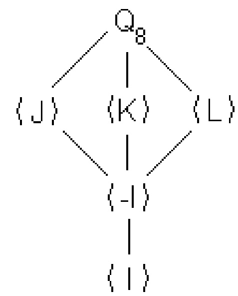
Examples:

- $\mathbb{Z}$ is a subroup (under addition) of $\mathbb{Q}$, which is a subgroup of $\mathbb{R}$, which is a subgroup of $\mathbb{C}$.
- $\mathbb{Q}^+$ is a subgroup under multiplication of $\mathbb{Q} - \{0\}$, which is a subgroup of $\mathbb{R} - \{0\}$, which is a subgroup of $\mathbb{C} - \{0\}$. Another subgroup of $\mathbb{R} - \{0\}$ is $\mathbb{R}^+$, and of course $\mathbb{R}^+ \cap (\mathbb{Q} - \{0\}) = \mathbb{Q}^+$. We will soon see that any intersection of subgroups is another subgroup.
- Any subspace of any vector space is a subgroup under addition, as well as being closed under scalar multiplication, as we learn in Math 214. In particular, a plane through the origin of $\mathbb{R}^3$ is a subgroup of $\mathbb{R}^3$ under addition.
- $GL(n, \mathbb{R})$ has many subgroups. One of the best known is $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}$, called the the *special linear group* of degree n. (Verify this is a subgroup. The mathematician Serge Lang has written a book titled $SL(2, \mathbb{R})$.) The set of upper triangular matrices is an additive subgroup of $M_n(\mathbb{R})$, and the set of upper triangular matrices with no zeros on the main diagonal is a multiplicative subgroup of $GL(n, \mathbb{R})$. Replace "upper triangular" (both times) in the last sentence with "lower triangular" or by "diagonal", and the sentence remains true.
- The Klein Four-Group $V = \{e, a, b, c\}$ is so small that its subgroups aren't very interesting, but at least it is easy to write them all down: $\langle e \rangle, \langle a \rangle, \langle b \rangle, \langle c \rangle, V$. A "subgroup diagram" or "subgroup lattice" displays their containment relationships: a line angling up means the higher contains the lower as a subgroup.



- The text introduces the group $Q_8 = \{I, J, K, L, -I, -J, -K, -L\}$ of *unit quaternions,* where $J^2 = K^2 = L^2 = -I$. The multiplication could have been determined by a table; but as the text points out, it would be necessary to check associativity, so it uses the connection to matrices in $GL(2, \mathbb{C})$. (It also could have been done in $GL(4, \mathbb{R})$, but the text avoids matrices that large.) The diagram below to the left is a mnemonic (memory aid) for the operation: clockwise is a positive product and counterclockwise is negative: $JK = L$, but $KJ = -L$, etc. The diagram below to the right is the subgroup lattice:





I saw this group first in the context of the "algebra of quaternions", in the more common notation 1 for I, i for J, j for K and k for L. The algebra of quaternions is the set of expressions

$$a + bi + cj + dk \ , \text{ where } a, b, c, d \in \mathbb{R} \ .$$

It is an extension of $\mathbb{C}$ over $\mathbb{R}$. Our text would deal with it as a "subalgebra of $M_{2\times 2}(\mathbb{C})$ over $\mathbb{R}$".

- The symmetric group on n letters, $\mathcal{S}_n$, i.e., the set of one-to-one functions from $\{1, 2, \ldots, n\}$ onto itself, a group under composition, has a subgroup: the set of all elements f of $\mathcal{S}_n$ for which $f(n) = n$ — i.e., the functions that don't move n. It is fairly clear that this subgroup "behaves exactly like" $\mathcal{S}_{n-1}$. And there is nothing special here about the set $\{1, 2, \ldots, n\}$ and the subset $\{n\}$: For any set X and subset Y of X, the symmetric group $\mathcal{S}(X)$ has a subgroup consisting of the set of all elements f of $\mathcal{S}(X)$ for which $f(y) = y$ for every y in Y, which "behaves exactly like" $\mathcal{S}(X - Y)$. The subset of all elements f of $\mathcal{S}(X)$ for which $f(y) \in Y$ for every y in Y and $f(z) \in X - Y$ for every $z \in X - Y$ is another subgroup of $\mathcal{S}(X)$. (If Y is finite, then we don't need the extra part about z's in $X - Y$, because if f takes all of Y to itself, then $f(Y)$ is all of Y, so z's outside of Y must go to elements outside of Y. But if Y is infinite, then a function may take Y into Y but not onto it, so its inverse would not take Y into Y. Example: The "add one" function $f(x) = x + 1$ is an element of $\mathcal{S}(\mathbb{Z})$ for which $f(\mathbb{Z}^+) \subseteq \mathbb{Z}^+$; but its inverse, the "subtract one" function, takes 1 to 0, outside of $\mathbb{Z}^+$. So the subset of $\mathcal{S}(\mathbb{Z})$ consisting of functions f for which $f(\mathbb{Z}^+) \subseteq \mathbb{Z}^+$ is not a subgroup of $\mathcal{S}(\mathbb{Z})$, because it is not closed under inverses.)

- Let G be any group and x be a fixed element of G. Then $Z(x) = \{g \in G : gx = xg\}$, the set of all elements that "commute with" x, is easily checked to be a subgroup of G, called the *centralizer* of x. Again, there is nothing special about a single-element set $\{x\}$: For any subset X of G, the "centralizer of X", $Z(X) = \{g \in G : gx = xg \ \forall x \in X\}$, is a subgroup of G. (We could make this a corollary of the result below that an intersection of a family of subgroups is again a subgroup, because $Z(X) = \bigcap\{Z(x) : x \in X\}$.) In particular, the centralizer of G itself, $Z(G)$, the set of all elements of G that commute with every element of G, is a subgroup, called the *center* of G.

  Some examples of centers and centralizers:

  * If G is abelian, then of course $Z(G) = G$ and for each element x of G, $Z(x) = G$. More generally, if $x \in Z(G)$, then $Z(x) = G$.
  * In the group Q_8 of unit quaternions, $Z(Q_8) = \langle -I \rangle$, because none of the other 6 elements commute with everything. But $Z(\langle J \rangle) = \langle J \rangle$; the powers of J commute with J, but none of the other four elements of Q_8 do.

* I claim that $Z(GL(2,\mathbb{R})) = \{aI : a \in \mathbb{R} - \{0\}\}$, the set of nonzero "scalar matrices". It is easy to see that these matrices commute with every element of $GL(2,\mathbb{R})$, so we need to see that no other elements do so: Suppose $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(GL(2,\mathbb{R}))$; then

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \Rightarrow \qquad \begin{pmatrix} c & d \\ a & b \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix},$$

so $c = b$ and $a = d$. Also

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \Rightarrow \qquad \begin{pmatrix} a & b \\ b+a & a+b \end{pmatrix} = \begin{pmatrix} a+b & b \\ b+a & a \end{pmatrix}$$

so $a = a + b$, and hence $b = 0$. So $A = aI$ for some nonzero scalar a.

* We can list the $3! = 6$ elements of $\mathcal{S}_3$, and one of them is $f : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. We can check that $f^2 : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$ and that $f^3 = e$, the identity function. The other three elements of $\mathcal{S}_3$ reverse two of the numbers $1, 2, 3$ and leave the third fixed; and we can check that they do not commute with f. For example, letting $g : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$:

$$f \circ g : 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1, \qquad \text{but} \qquad g \circ f : 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2\ .$$

So $Z(\langle f \rangle) = \langle f \rangle$. And $Z(\mathcal{S}_3) = \{e\}$.

Prop: Let $\{H_\lambda : \lambda \in \Lambda\}$ be a family of subgroups of the group G. Then the subset $H = \bigcap\{H_\lambda : \lambda \in \Lambda\}$ of G, consisting of the elements that are in every one of the H_λ's, is also a subgroup of G.

Pf: Because the identity is in every one of the H_λ's, it is in H, so H is not empty. To see that H is closed under the operation, take x, y in H; then because each H_λ is a subgroup and contains x, y, it also contains their product xy; so their product is also in H. To see that that H is closed under inverses, take x in H; then because x is in each H_λ, so is x^{-1}, so $x^{-1} \in H$.//

The text shows that the union of two subgroups is never a subgroup unless it is one of them (i.e., unless one is contained in the other). The union of more subgroups *may* be a subgroup, but it probably isn't.

We can describe the subgroups of a cyclic group.

Prop: Let $G = \langle x \rangle$ be a cyclic group.

(i) Every subgroup of G is cyclic.

(ii) If G is infinite cyclic, then the subgroups of G are $\{e\}$, $\langle x \rangle (= G)$, $\langle x^2 \rangle$, $\langle x^3 \rangle$, …, all distinct.

(iii) If G is finite cyclic of order n, then for each divisor d of n, G has exactly one subgroup of order d, namely $\langle x^{n/d} \rangle$, and it has no other subgroups.

Pf: (i) The trivial subgroup $\{e\}$ is cyclic (generated by e), so take a nontrivial subgroup H of G. Then H contains some positive power of the generator x; suppose the smallest such power is x^k. We want to show that $H = \langle x^k \rangle$: Because $x^k \in H$, we have $\langle x^k \rangle \subseteq H$. For the reverse inclusion, take any element x^m of H, and long-divide m by k, say $m = dk + r$ where $d, r \in \mathbb{Z}$ and $0 \le r < k$. Then $x^r = x^{m-dk} = x^m(x^k)^{-d} \in H$ (because H is closed under the operation and inverses); but k

was chosen so that x^k was the smallest positive power of x in H, so r can't be positive, i.e., $r = 0$. Thus, $x^m = (x^k)^d \in \langle x^k \rangle$, and so $H \subseteq \langle x^k \rangle$.

(ii) Clearly the sets of powers of x^k and x^{-k} are the same set, so the given list includes all the subgroups of G; so we only have to show that they are distinct if G is infinite cyclic. The text leaves this as an exercise for the reader, so I will, too.

(iii) Now we are supposing that G is finite of order n. From the proof given in (i), any nontrivial subgroup H of G has the form $\langle x^k \rangle$ where k is the smallest positive integer for which $x^k \in H$. We want to show that this k is a divisor of n: We know $x^n = e \in H$, and long-dividing n by k shows, just as in (i), that $k|n$, say $n = kd$. We proved in Section 4 that $o(x^k) = n/\gcd(n, k) = n/k$, so $\langle x^k \rangle$ is a subgroup of G of order n/k. Thus, every subgroup of G has order a divisor $n/k = d$ of n and is generated by $x^k = x^{n/d}$. Conversely, if d is a divisor of n, then we also proved in Section 4 that $x^{n/d}$ is an element of order $n/\gcd(n, (n/d)) = n/(n/d) = d$, so $\langle x^{n/d} \rangle$ is a subgroup of order d.//

Cor: In a finite cyclic group $G = \langle x \rangle$ of order n, $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$. In particular, $\langle x^r \rangle = \langle x^s \rangle$ iff $\gcd(n, r) = \gcd(n, s)$.

Pf: For the first equality, we need to show that each of x^k and $x^{\gcd(n,k)}$ is a power of the other. Because k is a multiple of $\gcd(n, k)$, x^k is a power of $x^{\gcd(n,k)}$; and because $\gcd(n, k) = nr + ks$ for some r, s in $\mathbb{Z}$, we have $x^{\gcd(n,k)} = (x^n)^r (x^k)^s = (x^k)^s$. Thus, $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$. It follows that, if $\gcd(n, r) = \gcd(n, s)$, then $\langle x^r \rangle = \langle x^s \rangle$. Conversely, if $\langle x^r \rangle = \langle x^s \rangle$, then $\langle x^{\gcd(n,r)} \rangle = \langle x^{\gcd(n,s)} \rangle$, and because the subgroups are equal and the exponents are factors of n, the exponents $\gcd(n, r)$ and $\gcd(n, r)$ are also equal.//

The text also includes the following useful fact: If S is a finite nonempty subset of a group G and S is closed under the operation, then S is also closed under inverses and hence is a subgroup of G. The proof is simple: Let $x \in S$; then because S is finite and closed under the operation, the powers of x cannot all be different, say $x^p = x^q$ where $p < q$. We get $x^{q-p} = e$, so x has finite order, and its inverse is a positive power of it, so $x^{-1} \in S$.