3 Product sets in nonabelian groups

In this section we shall consider general groups. Accordingly, we now let G denote a (possibly nonabelian) multiplicative group. Extending our earlier notation, if A, B are nonempty subsets of G and $g \in G$ then we define the *product set* $AB = \{ab : a \in A \text{ and } b \in B\}$, we set $A^{-1} = \{a^{-1} : a \in A\}$, and we define $gA = \{g\}A$, $Ag = A\{g\}$ - and call the latter two sets *shifts* of A.

Our two theorems for the group $\mathbb{Z}_p$, Cauchy-Davenport and Vosper, rely on similar but subtlely different tools. In Cauchy-Davenport, the key was a transform which replaced the pair of sets A, B with the pair $A \cap B$, $A \cup B$. This transform has two useful properties: first $(A \cap B) + (A \cup B) \subseteq A + B$, and second, $|A \cap B| + |A \cup B| = |A| + |B|$. Although the second of these properties is quite universal, the first property required our group to be abelian. On the other hand, the transform used in the proof of Vosper's theorem does not require the group to be abelian, and we shall now formulate this transform in general. Given a pair of finite subsets A, B of G and an element g, we may replace the pair of sets A, B by either $A \cap Ag, B \cup g^{-1}B$ or by $A \cup Ag, B \cap g^{-1}B$. As before, the product set from either of these two new pairs is a subset of AB, and now the average size of our new pair of sets is $\frac{1}{2}(|A \cap Ag| + |A \cup Ag| + |B \cap g^{-1}B| + |B \cup g^{-1}B|) = |A| + |B|$. We will shortly use this property to prove a theorem in general groups.

In both $\mathbb{Z}$ and $\mathbb{Z}_p$ we have proved lower bounds of the form $|A + B| \geq |A| + |B| - 1$ for nontrivial pairs (A, B). It is easy to see that such a bound will no longer hold when we study groups which have nontrivial (finite, proper) subgroups - if H is a finite subgroup of G, then $|H + H| = |H|$. Later in the notes we will prove a theorem of Kneser which gives a natural lower bound on the size of a sumset in a general abelian group, and will offer further insight into this situation. For now, we shall prove a theorem due to Kempermann/Scherk? which gives a similar bound as above, and applies to any group, but has the disadvantage of requiring an additional assumption which will prevent $A = B = H < G$.

Theorem 3.1 *Let A, B be finite nonempty subsets of G and assume that $\{(a, b) \in A \times B : ab = 1\} = \{(1, 1)\}$. Then $|AB| \geq |A| + |B| - 1$.*

Proof: Let A, B be a counterexample to the theorem so that

(i) $|AB|$ is minimum

(ii) $|A| + |B|$ is maximum (subject to (i))

(iii) $|A|$ is minimum (subject to (i),(ii))

Note that $|A| + |B| \leq |AB|$, so the maximum in (ii) is bounded.

If $A \cap B = \{1\}$, then we have $|AB| \geq |A \cup B| = |A| + |B| - 1$, a contradiction. Thus, we may choose $x \in A \cap B$ with $x \neq 1$. Now consider the sets $A' = A \cap Ax^{-1}$, $B' = B \cup xB$, $A'' = A \cup Ax$, $B'' = B \cup x^{-1}B$. It is immediate from our construction that all four of these sets contain 1, that $A'B' \subseteq AB$, and $A'', B'' \subseteq AB$. Let $y \in A'$ and assume that $y^{-1} \in B'$. If $y^{-1} \in B$, then $y \in A$ so $y = 1$. If $y^{-1} \in xB$, then $y \in Ax^{-1}$, so we may choose $a \in A$ and $b \in B$ with $y = ax^{-1}$ and $y^{-1} = xb$. Now we have $1 = yy^{-1} = ax^{-1}xb = ab$, so assumption $a = b = 1$. Thus $x^{-1} = y \in A' \subseteq A$ and we have a contradiction (since $x \in B$ and $x \neq 1$). Therefore $\{(a', b') \in A' \times B' : a'b' = 1\} = \{(1, 1)\}$. Similarly, $\{(a'', b'') \in A'' \times B'' : a''b'' = 1\} = \{(1, 1)\}$.

Now $|A'| + |A''| = |A \cap Ax^{-1}| + |A \cup Ax| = |Ax \cap A| + |A \cup Ax| = 2|A|$, and similarly $|B'| + |B''| = 2|B|$. If $|A''| + |B''| > |A| + |B|$, then this pair contradicts our choice of A, B for assumption (ii). Otherwise $|A'| + |B'| \geq |A| + |B|$ and this pair contradicts our choice of A, B for assumption (ii) or (iii). This completes the proof. □