Direct products and direct sums

This short section gives a useful construction which can be applied to both groups and rings.

Direct products of groups

Let $(G, \circ)$ and $(H, \Box)$ be groups. Put

$$G \times H = \{(g,h) : g \in G,\ h \in H\}$$

with the operation $(g_1,h_1) \times (g_2,h_2) = (g_1 \circ g_2, h_1 \Box h_2)$. Then $G \times H$ is a group, with identity $(1_G, 1_H)$ and $(g,h)^{-1} = (g^{-1}, h^{-1})$. It is called the *external direct product* of G and H.

Put

$$\begin{aligned} G_1 &= \{(g, 1_H) : g \in G\} \\ H_1 &= \{(1_G, h) : h \in H\} \end{aligned}$$

and define $\phi\colon G \times H \to H$ by $(g,h)\phi = h$. Then ϕ is a homomorphism, $\mathrm{Im}(\phi) = H$ and $\ker(\phi) = G_1$, so $G_1 \trianglelefteq G \times H$ and $(G \times H)/G_1 \cong H$. Similarly, $H_1 \trianglelefteq G \times H$ and $(G \times H)/H_1 \cong G$.

If $g \in G$ and $h \in H$ then $(g, 1_H)(1_G, h) = (g,h) = (1_G, h)(g, 1_H)$, so all elements of G_1 commute with all elements of H_1. Obviously, $G_1 H_1 = G \times H$ and $G_1 \cap H_1 = \{(1_G, 1_H)\}$. Therefore $G \times H$ is the internal direct product of G_1 and H_1.

We also have $G \cong G_1$ and $H \cong H_1$.

Theorem Let G and H be groups.

(a) If G and H are finite then $|G \times H| = |G| \times |H|$.

(b) If G and H are Abelian then $G \times H$ is Abelian.

(c) If G and H are cyclic of coprime order then $G \times H$ is cyclic.

(d) If $N \leqslant G$ and $K \leqslant H$ then $N \times K \leqslant G \times H$.

(e) If $N \trianglelefteq G$ and $K \trianglelefteq H$ then $N \times K \trianglelefteq G \times H$ and

$$(G \times H)/(N \times K) \cong (G/N) \times (H/K).$$

Proof Exercise.

Given three (or more) groups G_1, G_2, G_3, we have

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3).$$

We generally regard both of these as being $G_1 \times G_2 \times G_3$, which is

$$\{(g,h,k) : g \in G_1,\ h \in G_2,\ k \in G_3\},$$

with coordinatewise multiplication.

Theorem If a finite group G is Abelian then G is the internal direct product of its Sylow subgroups. (Note that if G is Abelian then all its subgroups are normal so there is exactly one Sylow p-subgroup for each prime p dividing $|G|$.)

Proof Suppose that P and Q are Sylow subgroups for different primes. Then $|P \cap Q|$ divides $|P|$ and $|Q|$, so $|P \cap Q| = 1$, so $P \cap Q = \{1_G\}$. Therefore PQ is a subgroup of G and is the internal direct product of P and Q. Continue similarly, using PQ and R, where R is another Sylow subgroup. □

Theorem If a finite Abelian group G has order a power of the prime p then G is a direct product of cyclic groups, each of which has order a power of p. If n_i is the number of factors in the product which have order p^i, then all ways of writing G as a direct product of cyclic groups have precisely n_i factors isomorphic to C_{p^i}.

Proof Beyond the scope of this course.

Corollary If G is a finite Abelian group then G is a direct product of cyclic groups, each of which has prime-power order. If n_{pi} is the number of factors in the product which have order p^i, where p is prime, then all ways of writing G as a direct product of cyclic groups have precisely n_{pi} factors isomorphic to C_{p^i}.

Direct sums of rings

Given rings $R_1, \ldots, R_n$, the *external direct sum* $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ is

$$\{(r_1, r_2, \ldots, r_n) : r_i \in R_i \text{ for } 1 \leqslant i \leqslant n\},$$

with addition and multiplication defined by

$$(r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n) = (r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n)$$

and

$$(r_1, r_2, \ldots, r_n) \times (s_1, s_2, \ldots, s_n) = (r_1 s_1, r_2 s_2, \ldots, r_n s_n),$$

where the operation in the i-th coordinate position is the relevant operation in R_i. It can be checked that this is a ring.

If $R_1, \ldots, R_n$ are all commutative then so is $R_1 \oplus \cdots \oplus R_n$.

If R_i has an identity 1_i for $i = 1, \ldots, n$ then $R_1 \oplus \cdots \oplus R_n$ has identity $(1_1, 1_2, \ldots, 1_n)$.

If at least two of $R_1, \ldots, R_n$ are not just $\{0\}$ then $R_1 \oplus \cdots \oplus R_n$ has zero-divisors:

$$(r, 0_2, 0_3, \ldots, 0_n) \times (0_1, s, 0_3, \ldots, 0_n) = (0_1, 0_2, \ldots, 0_n).$$

Define $\phi_i \colon R_1 \oplus \cdots \oplus R_n \to R_i$ by

$$(r_1, r_2, \ldots, r_n)\phi_i = r_i.$$

This is a ring homomorphism with $\mathrm{Im}(\phi_i) = R_i$ and

$$\begin{aligned} \ker(\phi_i) &= R_1 \oplus \cdots \oplus R_{i-1} \oplus \{0_i\} \oplus R_{i+1} \oplus \cdots \oplus R_n \\ &\cong R_1 \oplus \cdots \oplus R_{i-1} \oplus R_{i+1} \oplus \cdots \oplus R_n. \end{aligned}$$

Put $J_i = \{(0_1, \ldots, 0_{i-1}, r_i, 0_{i+1}, \ldots, 0_n) : r_i \in R_i\}$. Then $J_i \trianglelefteq R_1 \oplus \cdots \oplus R_n$ and $J_i \cong R_i$.

Theorem If $I_i \trianglelefteq R_i$ for $i = 1, \ldots, n$, then $I_1 \oplus \cdots \oplus I_n$ is an ideal of $R_1 \oplus \cdots \oplus R_n$.

Proof (a) Since $I_i \neq \emptyset$ for $i = 1, \ldots, n$, $I_1 \oplus \cdots \oplus I_n$ is not empty.

(b) Suppose that $(a_1, \ldots, a_n) \in I_1 \oplus \cdots \oplus I_n$ and $(b_1, \ldots, b_n) \in I_1 \oplus \cdots \oplus I_n$. Then a_i and b_i are in I_i, so $a_i - b_i \in I_i$, so

$$(a_1, \ldots, a_n) - (b_1, \ldots, b_n) = (a_1 - b_1, \ldots, a_n - b_n) \in I_1 \oplus \cdots \oplus I_n.$$

(c) Suppose that $(a_1, \ldots, a_n) \in I_1 \oplus \cdots \oplus I_n$ and $(r_1, \ldots, r_n) \in R_1 \oplus \cdots \oplus R_n$. Then $r_i a_i$ and $a_i r_i$ are both in I_i, so

$$(r_1, \ldots, r_n)(a_1, \ldots, a_n) = (r_1 a_1, \ldots, r_n a_n) \in R_1 \oplus \cdots \oplus R_n$$

and

$$(a_1, \ldots, a_n)(r_1, \ldots, r_n) = (a_1 r_1, \ldots a_n r_n) \in R_1 \oplus \cdots \oplus R_n. \quad \square$$

Theorem If R_i is a ring with identity 1_i, for $i = 1, \ldots, n$, and if J is an ideal of $R_1 \oplus \cdots \oplus R_n$ then there is an ideal I_i of R_i, for $i = 1, \ldots, n$, such that $J = I_1 \oplus \cdots \oplus I_n$.

Proof Put $I_i = (J)\phi_i$. Then I_i is a subring of R_i.

If $a_i \in I_i$ and $r \in R_i$ then $(0_1, \ldots, 0_{i-1}, r, 0_{i+1}, \ldots, 0_n) \in R_1 \oplus \cdots \oplus R_n$ and there is some $(a_1, \ldots, a_i, \ldots, a_n)$ in J and therefore

$$(0_1, \ldots, 0_{i-1}, r, 0_{i+1}, \ldots, 0_n)(a_1, \ldots, a_i, \ldots, a_n) = (0_1, \ldots, 0_{i-1}, ra_i, 0_{i+1}, \ldots, 0_n) \in J,$$

so $ra_i \in I_i$. Similarly, $a_i r \in I_i$. Hence $I_i \trianglelefteq R_i$.

Clearly, $J \subseteq I_1 \oplus \cdots \oplus I_n$.

Because R_i has an identity 1_i, we have $(0_1, \ldots, 0_{i-1}, 1_i, 0_{i+1}, \ldots, 0_n) \in R_1 \oplus \cdots \oplus R_n$ so if $(a_1, \ldots, a_i, \ldots, a_n) \in J$ then

$$(0_1, \ldots, 0_{i-1}, 1_i, 0_{i+1}, \ldots, 0_n)(a_1, \ldots, a_i, \ldots, a_n) = (0_1, \ldots, 0_{i-1}, a_i, 0_{i+1}, \ldots, 0_n) \in J.$$

Therefore if $a_i \in I_i$ for $i = 1, \ldots, n$ then $(0_1, \ldots, 0_{i-1}, a_i, 0_{i+1}, \ldots, 0_n) \in J$ for $i = 1, \ldots,$ n and so $(a_1, \ldots, a_n) \in J$. This shows that $I_1 \oplus \cdots \oplus I_n \subseteq J$, and so $J = I_1 \oplus \cdots \oplus I_n$. $\square$

Example In $2\mathbb{Z} \oplus 2\mathbb{Z}$,

$$\{(2n, 2m) : n \in \mathbb{Z},\ m \in \mathbb{Z},\ n + m \in 2\mathbb{Z}\}$$

is an ideal, but it is not of the form $I_1 \oplus I_2$ for any ideals I_1 and I_2 of $2\mathbb{Z}$.