当异常处理程序结束后，需要执行异常返回指令恢复进入异常之前的状态.

具体要做的事情包括:

1. 恢复发生异常前的PC
2. 从SPSR中恢复PSTATE寄存器(现场)

异常返回的指令根据当前**执行状态**为AArch32还是AArch64有所不同.

**AArch32**

AArch32的异常返回指令在不同的**模式**下也有所不同:

**若异常是在Hyp模式下处理:** 仅可执行ERET指令从异常返回.

**若异常是在其他模式下处理**, AArch32提供了以下的异常返回指令:

* ERET指令
* 使用带S后缀的数据处理指令直接操作PC(例如, MOVS, PC, LR), 同时恢复PSTATE
* RFE 指令: RFE <Rn>. 从基址寄存器<Rn>指向的地址依次加载PC和PSTATE.
* LDM 指令: LDM <Rn> {pc..}. 若目标寄存器中包含PC, 则会同时恢复PSTATE.

**AArch64**

AArch64下**统一使用**ERET指令进行异常返回.

ERET指令完成了:

1. 从ELR\_ELx中恢复PC指针
2. 从SPSR\_ELx中恢复PSTATE寄存器的状态.

LDM(Load Multiple)

格式: LDM <Rn> {registers}

含义: 从基址寄存器<Rn>指向的地址开始依次加载多个寄存器值. 若目标寄存器中包含PC, 则同时恢复PSTATE.

例如: LDM <r0> {pc, r1} 等价于:

|  |
| --- |
| pc=[r0]  r1=[r0+4]  PSTATE=SPSR ;仅当目标寄存器包含PC时自动完成 |

RFE(Return From Exception)

格式: LDM <Rn>

含义: 从基址寄存器<Rn>指向的地址依次加载PC和PSTATE.

例如: RFE <r0> 等价于:

|  |
| --- |
| pc=[r0]  PSTATE=[r0+4] |