# CoCoA-5 - Bug #1382

## SEGV: should have been harmless

07 Jan 2020 16:06 - John Abbott

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 07 Jan 2020 |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | John Abbott | **% Done:** | 100% |
| **Category:** | bug | **Estimated time:** | 1.01 hour |
| **Target version:** | CoCoA-5.3.0 | **Spent time:** | 0.95 hour |

**Description**

I get a SEGV with the following input (no SEGV if the number of loop iters is 100).

```
use QQ[x,y];

D := 3;
nvars := NumIndets(CurrentRing);
S := support((1+sum(indets(CurrentRing)))^D);

define rndpoly(S)
  return sum([random(-5,5)*t | t in S]);
enddefine; -- rndpoly

for i := 1 to 1000 do
  L := [rndpoly(RandomSubset(S,4)) | j in 1..nvars];
  I := ideal(L);
  RGB := ReducedGBasis(I);
  if len(RGB) = nvars then continue; endif;
  foreach G in subsets(RGB,nvars) do
    if CommonDenom(G) = 1 and ideal(G) = I then println G; endif;
  endforeach;
endfor;
```

**Related issues:**

| | | |
|---|---|---|
| Related to CoCoA-5 - Support #1387: John's visit Feb 2020 | **Closed** | **07 Jan 2020** |

### History

#### #1 - 07 Jan 2020 16:07 - John Abbott

I was using CoCoA-5 to look for some examples to show the students.  It was a surprise when it SEGV'd  :-(

#### #2 - 08 Jan 2020 15:44 - John Abbott

*- Status changed from New to In Progress*

*- % Done changed from 0 to 10*

According to gdb, the program crashed in line 48 of SmartPtrIRC.H
I wonder what that means 8-|

#### #3 - 08 Jan 2020 15:47 - John Abbott

valgrind suggests that the problem arose inside a call to CommonDenom when it called IsPolyRing (which called PolyRingPtr which called myRing::myRawPtr which called SmartPtrIRC::myRawPtr).
Somewhere a NULL ptr cropped up.

#### #4 - 08 Jan 2020 16:05 - John Abbott

*- Status changed from In Progress to Feedback*

*- Assignee set to John Abbott*

*- % Done changed from 10 to 80*

*- Estimated time set to 0.99 h*

The clue from valgrind was very helpful.
The fn CommonDenom did not check for the case of an empty list (and then blithely accessed the first element...)
I have modified the source, and the example input now produces an "Empty list or vector" error (instead of SEGV). Much better!

Now I must add an example to exbugs.

**#5 - 08 Jan 2020 16:41 - John Abbott**

*- % Done changed from 80 to 90*

All tests pass, and I have checked in.

**#6 - 09 Jan 2020 11:21 - Anna Maria Bigatti**

*- Status changed from Feedback to Closed*

*- % Done changed from 90 to 100*

*- Estimated time changed from 0.99 h to 1.01 h*

tested on MacOS. OK.

**#7 - 09 Jan 2020 11:32 - John Abbott**

*- Related to Support #1387: John's visit Feb 2020 added*