例題 15.1. 環としての同型 $\mathbb{Q}[X]/(X^2-2X-4)\cong\mathbb{Q}[\sqrt{5}]$ が存在することを示しなさい。

この問題を <u>理解するため</u> のポイント:

- (X^2-2X-4) とは、X^2-2X-4 で生成される $\mathbb{Q}[X]$ のイデアル、すなわち X^2-2X-4 を含む $\mathbb{Q}[X]$ のイデアルのうち最小のものでした。以下このイデアルを I と書きましょう。
- $\mathbb{Q}[X]/I$ とは、 $\mathbb{Q}[X]$ の剰余環であって、それは $\mathbb{Q}[X]$ に同値関係 (クラス分け) を
$$p\sim q \quad\Leftrightarrow\quad p-q\in I$$
で定めたクラスの全体でした。剰余環は環の構造を持つのでした。
- X の $\mathbb{Q}[X]/I$ におけるクラスを a と書くことにすると、剰余環の定義により、$a^2-2a-4=0$ つまり、a は X^2-2X-4 の根の役割をします。
- X^2-2X-4 の根は、$1\pm\sqrt{5}$.
- $\mathbb{Q}[\sqrt{5}]$ とは、$\mathbb{Q}$ と $\sqrt{5}$ を含む最小の環をさすのでした。

この問題を <u>解くため</u> のポイント:

- 環の準同型定理を使用する、その論理的な大枠がわかっているか否か。
- どのような環準同型 φ を使用するか。
- φ の像は何か。
- 核が (X^2-2X-4) と等しいことを示せるか、とくに、
  - 論理的な枠組みがわかっているか否か。(“$\subset$” と “$\supset$”)
  - 多項式 X^2-2X-4 が $\mathbb{Q}$ 上既約であることを証明できるか。
  - 多項式 X^2-2X-4 が $\mathbb{Q}$ 上既約であることをうまく使用できるか。

例題 15.2. 12345 で割ると 3 あまり、11111 で割ると 4 余る整数をすべて求めよ。

この問題を <u>理解するため</u> のポイント:

- 整数 a と b が互いに素ならばユークリッドの互除法により
$$al+bm=1$$
を満たす整数 l,m が存在することがわかり、具体的に求めることもできるのでした。
- ユークリッドの互除法は、素因数分解に関する諸知識よりも単純で、基本的であることに注意します。
- 上記 l,m を用いると、x が a で割り切れ、 b でも割り切れるならば、x は ab で割り切れる。 という事も証明できます。

この問題を <u>解くため</u> のポイント:

- ユークリッドの互除法により、関係式 $-2224\cdot12345+2471\cdot11111=1$ を導けるか。
- この関係式から、求める解のうち一つを得ることが出来るか。
- 解の全部を挙げることが出来るか否か。もちろん、もれなく数え上げていることを論理的に証明できなければならない。