

素体

Joh @物理のかぎプロジェクト

2006-06-25

有理数体と剰余体は、それぞれ素体であることを **拡大体** で示しました。実は、逆に全ての素体は有理数体が剰余体のどちらかに同型であることが言えるのです。

theorem

全ての素体は、有理数体 Q が剰余体 Z_p に同型です。

証明には準同型定理と商体の知識が必要です。イデアルも少し出てきます。少し長いですが、証明を掲げておきます。

proof

任意の素体 F を考えます。乗法の単位元を 1_F とすると、 1_F の m 個の和 (m は整数) は $m \cdot 1_F$ と書けます。ここで、整数 Z から素体 F への写像 $\phi: Z \rightarrow F$ を、 $\phi(m) = m \cdot 1_F$ と置くと、 ϕ は準同型写像になっています。そこで準同型定理を使うと、 $Z/\text{Ker}(\phi) \sim \phi(Z)$ がなりたちますが、 $\phi(Z)$ は F の部分集合ですので、乗法の零元以外に零因子があるはずはなく、整域になります (**整域** 参照)。すなわち、 $\text{Ker}(\phi)$ は Z の素イデアルであり、 $\text{Ker}(\phi) = 0$ となるか、 $\text{Ker}(\phi) = pZ$ となるか (p は素数) のいずれかだと言えます。前者 $\text{Ker}(\phi) = 0$ の場合、 $Z \sim \phi(Z)$ となります。両辺の商体を考えると、まず Z の商体は Q です。また、 $\phi(Z)$ の商体はどんな体だかよく分かりませんが、とりあえず F の部分体であることは確かです。 $\phi(Z)$ の商体を H と名づけると、 $Q \sim H \subset F$ が言えます。ところが F はいま素体ですので、部分体は F 自身しか存在せず、 $H = F$ ですので、結局 $Q \sim F$ が示せます。 $\text{Ker}(\phi) = 0$ の場合、 F は有理数体 Q と同型です。同様に、 $\text{Ker}(\phi) = pZ$ の場合、 $F \sim Z/pZ$ が示せます。

また、次の定理も重要です。

theorem

任意の体 F は、ただ一つの素体を含みます。

proof

前の定理の証明で、 F を素体だと仮定しなくても Q or $Z_p \sim H \subset F$ の行までは同じ議論ができますので、任意の体には少なくとも一つは素体 H が含まれることは言えます。逆に、含まれる素体は一つしかないことをここから示します。 F に H 以外の素体 H' が含まれるとすると、共通集合 $H \cap H'$ も体であり、 H や H' の部分体になるはずですが、しかし素体が自分自身以外の部分体を含むことはありませんから、 $H \cap H' = H = H'$ が要請されます。すなわち F には一つしか素体は含まれません。

定理と証明だけだと退屈してしまうので、この辺にしておきます。ここで紹介した二つの定理は、とても重要なものですし、定理の意味をよく考えると、体のカラクリが見えてくる部分があると思いますので、もう一度定理の意味を考えてみて下さい。標数の記事で、このあたりの話の続きをまた考えます。

補足

ベクトル空間の考え方で素体を考えてみると、あるいは少し見通しが良くなり、素体に対するイメージが湧くかも知れません。

拡大体を体上のベクトル空間と見る見方は、ここまでもたびたび使って来ました。そこで、ある体 F の元も、素体 $F_0 (\subset F)$ の元 $\{x_1, x_2, \dots, x_{n-1}, x_n, \dots\}$ を使って $a_1x_1 + a_2x_2 + \dots + a_{n-1}x_{n-1} + a_nx_n + \dots$ の形で表現できると考えられます。ここに使われている積や和は、当然 F に定義されている『加法』と『乗法』です。素体は体の最小の部分体ということでしたから、素体はこのベクトル空間の最小の独立なベクトルの集合、つまり基底になっていると考えることができます。