

今日のテーマ: ガロア理論とは

ガロア理論とは、体の拡大をガロア群という群の構造を調べることにより明らかにする理論である。これにより代数方程式が手に取るように扱えるようになる。

ガロア理論はそれ自身代数幾何学や数論の重要な道具になったのみならず、数学的対象をそれについての対称性により考察するという一般的原理のもととなって数学の爆発的発展の基礎を与えた。

例えば、 \mathbb{Q} 上の代数方程式

$$x^3 + x + 1 = 0$$

を考えよう。この方程式の解を α とおくと、

$$(1.1) \quad \alpha^3 + \alpha + 1 = 0$$

が成り立つはずである。 \mathbb{Q} と新しい「数」 α を取り入れて、加減乗算を行うには、

$$c_0 + c_1\alpha + c_2\alpha^2 \quad (c_0, c_1, c_2 \in \mathbb{Q})$$

のような数が必要になる。そして、これらの数同士の加減乗算による結果は関係式 (1.1) を用いればまたもや同様の数になる。

このような操作は、実は剰余環を用いることにより上手に扱える。もっと一般に、体 k 上の一変数多項式 f に対して、剰余環

$$R = k[X]/f(X)k[X]$$

を考えると、この環における X のクラス (剰余類) a は $f(a) = 0$ をみたし、 R は k に $f = 0$ の解 a を付け加えて作った環であると言って良い。

つぎに、そのようにして作ったいろいろな環の比較を行う必要がある。

例えば二次方程式

$$x^2 + x + 1 = 0$$

の解は

$$\frac{-1 \pm \sqrt{-3}}{2}$$

で与えられる。これは

$$k[X]/(X^2 + X + 1)k[X]$$

と

$$k[X]/(X^2 + 3)k[X]$$

の間に関係があることを意味している。

問題 1.1. α が \mathbb{Q} 上の方程式 $X^5 - X + 1 = 0$ の解であるとするとき

- (1) α^{10} を α の 4 次以下の \mathbb{Q} 係数の多項式で表しなさい。
- (2) α^{15} を α の 4 次以下の \mathbb{Q} 係数の多項式で表しなさい。
- (3) $(\alpha^3 + \alpha + 1)(\alpha^4 + \alpha^2 + 1)$ を α の 4 次以下の \mathbb{Q} 係数の多項式で表しなさい。