推论 6.10.5 回顾

对于任意域F和任意非常数多项式$f \in F[X]$，存在域的嵌入$F \hookrightarrow E_f$，使得f在Ef上分裂。

证明思路

证明的关键在于逐步添加根，并控制每一步扩域的次数。

1. **第一步：添加一个根**

   设$f(X) \in F[X]$，且$degf = n \geq 1$。我们可以找到一个扩域$F1$，使得f在$F1$中有一个根$\alpha 1$。

   - 具体做法：

     考虑f在F上的一个不可约因子$p(X)$。

     令$F1 = F[X]/(p(X))$，则$F1$是一个域，且$F \hookrightarrow F1$是一个域的嵌入。

     在$F1$中，$p(X)$有一个根$\alpha 1$（即$X + (p(X))$）。

     由于$p(X)$是$f(X)$的因子，所以$\alpha 1$也是$f(X)$的根。

   - 此时，$f(X) = (X - \alpha 1)g1(X)$，其中$g1(X) \in F1[X]$，且$degg1 = n - 1$。
   - 并且，$[F1 : F] = degp(X) \leq degf(X) = n$。

2. **第二步：添加第二个根**

   现在，我们在$F1$上考虑$g1(X)$。

   重复上述过程，可以找到一个$F2$，使得$F1 \hookrightarrow F2$，且$g1(X)$在$F2$中有一个根$\alpha 2$。

   - 此时，$g1(X) = (X - \alpha 2)g2(X)$，其中$g2(X) \in F2[X]$，且$degg2 = n - 2$。
   - 并且，$[F2 : F1] \leq degg1(X) = n - 1$。

3. **重复此过程**

   我们不断重复这个过程，直到$f(X)$在某个扩域Ef中完全分解为一次因式的乘积。

   也就是说，

   我们构造了一个域的链$F \subseteq F1 \subseteq F2 \subseteq \ldots \subseteq Ef$，其中$f(X)$在$Ef$中有$n$个根$\alpha 1, \alpha 2, \ldots, \alpha n$，

   并且$f(X) = c(X - \alpha 1)(X - \alpha 2)\ldots(X - \alpha n)$，其中$c \in F$是$f$的首项系数。

4. **计算扩域次数**
   根据扩域次数的乘法公式，我们有

   $$[Ef : F] = [Ef : Fn - 1][Fn - 1 : Fn - 2]\ldots[F2 : F1][F1 : F]$$

   由于每一步的扩域次数都小于等于当前剩余多项式的次数，所以

   $$[Ef : F] \leq n(n-1)(n-2)\ldots 2 \cdot 1 = n!$$

等号成立的条件

现在我们来讨论等号$[Ef:F]=n!$成立的条件。

从上面的分析可以看出，等号成立当且仅当每一步的扩域次数都达到最大值。也就是说，对于每一步，我们添加的根都生成了最大可能的扩域。

具体来说，等号成立的条件是：

- **每一步添加的根都是新的，且其最小多项式次数达到最大值**：
  - 在第一步，我们添加$\alpha 1$，它的最小多项式次数等于f的次数n。这要求f在F上不可约。
  - 在第二步，我们添加$\alpha 2$，它在$F1$上的最小多项式次数等于$g1$的次数$n-1$。这意味着$g1$在$F1$上不可约。
  - 以此类推，在每一步，我们添加的根在当前扩域上的最小多项式次数都等于当前剩余多项式的次数。
  - 换句话说，在每一步，我们添加的根都不能通过之前的根来表示，即它们都是“新的”。
- 等价条件：f的$Galois$群为S_n

  更准确地说，

  当f的分裂域Ef的$Galois$群$textGal(Ef/F)$同构于对称群Sn时，

  等号$[Ef:F]=n!$成立。

  对称群Sn是所有n个元素的置换群，其阶数为$n!$。

总结

- $[Ef:F]\leq n!$这个不等式总是成立的，它来自逐步添加根的过程，并且每一步的扩域次数都有一个上界。
- $[Ef:F]=n!$成立的条件是，每一步添加的根都是新的，且其最小多项式次数达到最大值，这等价于f的$Galois$群为Sn。

例子

- **一般情况，不等号成立：**

  考虑$f(X)=X^2-1\in Q[X]$。它的根是1和-1，分裂域是Q本身，所以$[Q:Q]=1<2!=2$。

- **等号成立：**

  考虑$f(X)=X^3-2\in Q[X]$。它的分裂域Ef是$Q(\sqrt[3]{2},\omega)$，其中ω是一个三次单位根。

  可以证明$[Q(\sqrt[3]{2},\omega):Q]=6=3!$。此时，$f$的$Galois$群同构于$S3$。