進階代數(下) 第十三次作業

上課老師: 翁志文

2009 年五月十八日

1. Let F be an extension field of K.
   (a) (黃彥璋) If $[F:K]$ is prime, then there are no intermediate fields between F and K.
   (b) (林志嘉) If $u \in F$ is algebraic of odd degree over K, then so is u^2 and $K(u) = K(u^2)$.
   (c) (陳建文) In the field $K(x)$, let $u = x^3/(x+1)$. Show that $K(x)$ is a finite extension of the field $K(u)$. What is $[K(x) : K(u)]$.

2. A complex number is said to be an *algebraic number* if it is algebraic over $\mathbb{Q}$ and an *algebraic integer* if it is the root of a monic polynomial in $\mathbb{Z}[x]$. (Note. A monic polynomial has leading coefficient 1)
   (a) (羅建峰) The sum and product of two algebraic numbers are algebraic numbers.
   (b) (黃思綸) Find an algebraic number which is not an algebraic integer.
   (c) (陳泓勳) If u is an algebraic number, then there exists an integer n such that nu is an algebraic integer.
   (d) (何昕暘) If $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$. (Gauss Lemma)
   (e) (賴德展) If u is an algebraic integer and $n \in \mathbb{Z}$, then $u+n$ and nu are algebraic integers.
   (f) (劉侖欣) The sum and product of two algebraic integers are algebraic integers.

3. Let G be an abelian group of order n. A *partial difference set* of G is a subset S of G such that the set $\{x-y \mid x, y \in S, x \neq y\}$ contains $|S| \times (|S|-1)$ elements.
   (a) (周彥伶) Let S be a partial difference set of G with $|S| = s$. Then $s^2 - s + 1 \leq n$.
   (b) (洪湧昇) Let $a \in U_p$, the set of units of $\mathbb{Z}_p$, be a multiplication generator. Then $S = \{(i, a^i)\} \mid 0 \leq i \leq p-1\}$ is a partial difference set of $\mathbb{Z}_p \times \mathbb{Z}_p$. (Hint. Find the desired set of $p(p-1)$ elements)
   (c) (林志峰) Let S be as in (b). Then $|(u+S) \cap (v+S)| \leq 1$ for any distinct elements $u, v \in \mathbb{Z}_p \times \mathbb{Z}_p$.
   (d) (黃正一) Let $F = \{u+S \mid u \in \mathbb{Z}_p \times \mathbb{Z}_p\} \cup \{\{(i,j) \mid j \in \mathbb{Z}_p\} \mid i \in \mathbb{Z}_p\}$. Then the union of any $p-1$ elements in F does not contain (cover) another element in F.