POLINOMIOS Y FACTORIZACIÓN

PRIMER CUATRIMESTRE 2007

Segunda hoja de ejercicios: a ser entregada resuelta el Lunes 18 de Junio.

(**1**) Ejercicio sobre Látices en general:
- Probar que $L \subset \mathbb{R}^n$ es un látice si y solo si L es un subgrupo discreto de $\mathbb{R}^n$.
- Sea T el paralelepípedo fundamental del látice completo L. Probar que Vol(T)=det(L).
- Probar el lema de Minkowski para conjuntos convexos.

(**2**) Dar un algoritmo para encontrar eficientemente uno de los vectores más cortos de un látice en $\mathbb{R}^2$.

(**3**) Lema de Hensel para más de dos factores: generalizarlo para $f \equiv f_1 \cdots f_s \pmod p$ donde $f, f_1, \ldots, f_s \in \mathbb{Z}[x]$ son polinomios mónicos y f libre de cuadrados en $\mathbb{Z}[x]$ y módulo p.

(**4**) Generalizar el ejercicio **4** de la primer hoja de ejercicios a más de dos polinomios.

(**5**) Sea K un cuerpo de números.
- Probar que el conjunto de los elementos de K cuyo minimal (mónico) sobre $\mathbb{Q}$ tiene todos sus coeficientes enteros es un anillo, que se llama el anillo $\mathcal{O}_K$ de enteros de K.
- Probar que si $\alpha \in \mathcal{O}_K$ es tal que $K = Q[\alpha]$, con $g \in \mathbb{Z}[x]$ el minimal de α sobre $\mathbb{Q}$, entonces
$$\big[\mathcal{O}_K : \mathbb{Z}[\alpha]\big]^2 \,|\, \mathrm{Disc}(g)$$
(donde Disc nota el discriminante) y deducir que entonces, existe algún d con $d^2 \,|\, \mathrm{Disc}(g)$ tal que
$$\mathcal{O}_K \subseteq \frac{1}{d}\,\mathbb{Z}[\alpha].$$