Algebra Conmutativa 1 marzo

Ayer: Módulos libres y no libres

Hoy: Repaso (& RC)

Teorema (Gauss) ℓ, p primos impares

$\ell^* = (-1)^{(\ell-1)/2} \ell$ entonces

$$\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right) \quad \dots (1)$$

Argumento: $\left(\frac{-1}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)}$

entonces $$\left(\frac{\ell^*}{p}\right) = \left(\frac{(-1)^{\frac{\ell-1}{2}}\ell}{p}\right) = \left(\frac{\ell}{p}\right)(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{\ell-1}{2}\right)}$$

Por tanto demostrar (1) es suficiente.

$\left(\frac{\ell^*}{p}\right)=1$ sii p escinde en $\mathcal{O}(\sqrt{\ell^*})$

sii p escinde en $\mathcal{O}(J_\ell) \subseteq \mathbb{Q}[J_\ell]$

Recordar: si $p = P_1 \cdot \ldots \cdot P_r$ en $\mathcal{O}_{J_\ell}$ entonces r es par.

Afirmación: $\boxed{rf = \ell - 1}$ donde $p = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$

$$\sum_{i}^{r} e_i f_i = [\mathbb{Q}(J) : \mathbb{Q}]$$

Como r es par $(2s = r)$ tenemos

$2sf = \ell - 1$ i.e. $f \mid \frac{\ell-1}{2}$

lo cual es equivalente a

$$p^{\left(\frac{q-1}{2}\right)} \equiv 1 \pmod{q}$$

$$p^{\frac{q-1}{2}} \equiv 1 \pmod{q}.$$

Observar: $\mathbb{F}_q^*$ es cíclico. Un elemento aquí tiene orden un divisor de $\frac{q-1}{2}$ sii está en $\mathbb{F}_q^{*2}$.

Por lo tanto $p^{\left(\frac{q-1}{2}\right)} \equiv 1 \pmod{q}$

sii $\left(\frac{p}{q}\right) = 1$ y entonces

$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$ como se deseaba mostrar ∎.