Il gruppo moltiplicativo di un campo finito a.a. 2014-2015

Valentina Barucci

Sia K un campo finito, ad esempio $K = \mathbb{Z}_p$ e sia $K^* = K \setminus \{0\}$ il gruppo moltiplicativo degli elementi non nulli di K. Vogliamo dimostrare che K^* è un gruppo ciclico. Premettiamo il

Lemma 1. *Sia G un gruppo abeliano finito con un solo sottogruppo per ogni divisore dell'ordine di G. Allora G è un gruppo ciclico.*

Dimostrazione. Sia n l'ordine massimo degli elementi di G e sia $g \in G$ un elemento di ordine n. Mostriamo innanzi tutto che ogni altro elemento h di G ha un ordine che divide n. Sia d l'ordine di h e supponiamo per assurdo che d non divida n. Allora esiste un primo p che compare nella fattorizzazione di d con un esponente, diciamo e, maggiore dell'esponente f con cui compare nella fattorizzazione di n. Consideriamo i due elementi

$$h^{d/p^e} \text{ che ha ordine } p^e$$

$$g^{p^f} \text{ che ha ordine } n/p^f$$

poiché gli ordini di questi due elementi sono coprimi, ovvero $(p^e, n/p^f) = 1$, e il gruppo è abeliano, l'elemento prodotto $h^{d/p^e} g^{p^f}$ avrà ordine $np^{e-f} > n$, assurdo.

Dimostriamo adesso che l'elemento g di ordine massimo genera tutto il gruppo G, ovvero che ogni altro elemento h di G è una potenza di g. Se h ha ordine d, per le ipotesi del lemma, i due sottogruppi di ordine d, $\langle h \rangle$ e $\langle g^{n/d} \rangle$ coincidono, quindi

$$h \in \langle g^{n/d} \rangle \subset \langle g \rangle$$

□

Proposizione 2. *Se K è un campo finito, allora K^* è un gruppo ciclico.*

Dimostrazione. Possiamo applicare il lemma a K^*, infatti se per assurdo ci fossero in K^* due sottogruppi distinti H_1 e H_2 dello stesso ordine, diciamo d, allora avremmo che tutti gli elementi x di $H_1 \cup H_2$, in numero maggiore di

d, verificherebbero $x^d = 1$ ovvero sarebbero radici del polinomio (di grado d) $x^d - 1$, il che è assurdo per il teorema di Ruffini.

□