**Sottogruppi finiti del gruppo moltiplicativo di un campo**

Maurizio Cornalba

25/3/2013

**Lemma 1.** *Sia $G$ un gruppo finito. Supponiamo che per ogni intero $n > 0$ ci siano al più $n$ elementi di $G$ tali che $g^n = 1$. Allora $G$ è ciclico.*

*Dimostrazione.* Per ogni $g \in G$ il sottogruppo $\langle g \rangle$ generato da $g$ è normale. Sia infatti $n$ l'ordine di $g$. Se $\gamma \in \langle g \rangle$ e $h \in G$ allora $(h\gamma h^{-1})^n = 1$. Dato che $\langle g \rangle$ contiene già $n$ elementi la cui $n$-esima potenza è 1 ne segue che $h\gamma h^{-1} \in \langle g \rangle$. Sia ora $g$ un elemento di $G$ di ordine massimo. Mostreremo che $G = \langle g \rangle$. Indichiamo con $n$ l'ordine di $g$. Sia $\gamma$ un altro elemento di $G$. Dato che $\langle g \rangle$ contiene $n$ elementi la cui $n$-esima potenza è 1, per mostrare che $\gamma \in \langle g \rangle$ basta mostrare che l'ordine di $\gamma$ divide $n$. Sia $p$ un primo. Scriviamo $n = kp^h$, $o(\gamma) = mp^\ell$, dove $k$ e $m$ sono primi con $p$. Poniamo $a = g^{p^h}$, $b = \gamma^m$. I sottogruppi $\langle a \rangle$ e $\langle b \rangle$ sono normali e hanno intersezione $\{1\}$ perché hanno ordini primi fra loro. Ne segue che $a$ e $b$ commutano e che l'ordine di $ab$ è $o(a)o(b) = kp^\ell$. Dunque, per la scelta di $g$, deve essere $kp^\ell \leq n = kp^h$, cioè $\ell \leq h$. Data l'arbitrarietà del primo $p$ se ne deduce che l'ordine di $\gamma$ divide $n$. □

**Corollario 1.** *Sia $A$ un dominio di integrità e sia $G$ un sottogruppo finito del gruppo $A^\times$ delle unità di $A$. Allora $G$ è ciclico.*

*Dimostrazione.* Basta osservare che in un dominio il polinomio $X^n - 1$ ha al più $n$ radici. □

**Corollario 2** (Teorema di Wilson)**.** *Un intero positivo $n$ è primo se e solo se*

$$(n-1)! \equiv -1 \mod n.$$

*Dimostrazione.* Supponiamo che $n$ non sia primo, cioè che ci siano interi $h, k$ tali che $1 < h \leq k$, $n = hk$. Se $h < k$ allora $k < n - 1$ e $(n-1)! = 1 \cdots h \cdots k \cdots (n-1)$, quindi $(n-1)! \equiv 0 \mod n$. Se $h = k > 2$ allora $2h < n - 1$ e $(n-1)! = 1 \cdots h \cdots 2h \cdots (n-1)$, quindi anche in questo caso $(n-1)! \equiv 0 \mod n$. Se infine $h = k = 2$, cioè se $n = 4$, allora $(n-1)! = 6 \equiv 2 \not\equiv -1 \mod n$.

Supponiamo ora che $n$ sia primo. La riduzione di $(n-1)!$ modulo $n$ è il prodotto di tutti gli elementi di $\mathbb{F}_n^\times$. Dobbiamo mostrare che vale $-1$. Sappiamo che $\mathbb{F}_n^\times$ è un gruppo ciclico per il lemma (1). Indicandone con $\gamma$ un generatore la riduzione di $(n-1)!$ modulo $n$ vale

$$\gamma \cdot \gamma^2 \cdot \gamma^3 \cdots \gamma^{n-1} = \gamma^{\frac{(n-1)(n-2)}{2}}$$

Se $n = 2$ allora $(n-1)! = 1 \equiv -1 \mod 2$. Se $n$ è un primo dispari $\gamma^{\frac{(n-1)}{2}}$ è diverso da 1 perché $\gamma$ ha ordine $n - 1$; per lo stesso motivo ha quadrato uguale a 1. Dunque $\gamma^{\frac{(n-1)}{2}} = -1$ e di conseguenza, dato che $n - 2$ è dispari,

$$\gamma^{\frac{(n-1)(n-2)}{2}} = -1$$

□