Questa è una raccolta di approfondimenti scritti durante il corso di Algebra 2 tenuto dal prof. Andrea Lucchini nel primo semestre dell'anno accademico 2014-2015 all'università di Padova, dipartimento di Matematica. Si tratta di cose ben note e le ho scritte soprattutto per suscitare curiosità. Per commenti o domande mi si può scrivere all'indirizzo mgaronzi@math.unipd.it.

Martino Garonzi

1. Il gruppo dei quaternioni

Lo scopo di questa breve nota è fornire una dimostrazione del fatto che il gruppo degli automorfismi del gruppo dei quaternioni Q_8 è isomorfo a S_4. La dimostrazione è basata sullo studio del gruppo di matrici $GL(2,3)$ ed è tratta dal corso "Introduction to group theory" tenuto dal professor Andrea Lucchini all'università di Padova.

Sia $Q = Q_8$ il gruppo dei quaternioni. Ricordiamo che si tratta del sottogruppo di $GL(2,\mathbb{C})$ generato dalle matrici

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

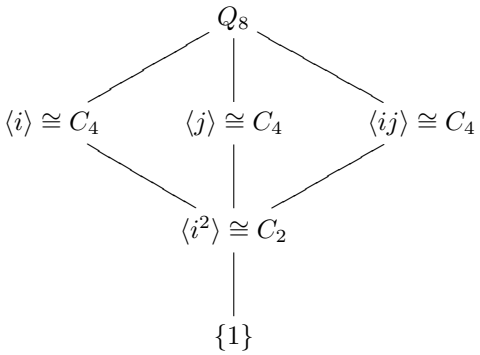
Qui i indica l'unità immaginaria.

D'ora in poi useremo le lettere minuscole per I, J, K indicandoli rispettivamente con i, j, k. Allora abbiamo $i^2 = j^2 = k^2 = -1$, $ij = k$ e $ji = -k$. Da qui possiamo ricavare tutti gli elementi di Q. Per esempio $ijkjk = kkjk = (-1)jij = -(-k)j = kj = ijj = -i$. Troviamo che

$$Q = Q_8 = \{1, i, j, k, -1, -i, -j, -k\}.$$

Inoltre come si verifica facilmente 1 ha ordine 1, -1 ha ordine 2 e tutti gli altri elementi hanno ordine 4. In particolare -1 è l'unico elemento di Q di ordine 2 quindi $N = \langle -1 \rangle$ è normale, ed è anzi il centro di Q (infatti -1 sta nel centro ed è facile vedere che nessun altro elemento non identico ci sta, per esempio i e j non ci stanno perché $ij = -ji \neq ji$). Ora Q/N ha ordine 4 e contiene almeno due elementi di ordine 2, iN e jN, quindi Q/N non è ciclico, in altre parole $Q/N \cong C_2 \times C_2$. Per il teorema di corrispondenza, tutti i sottogruppi normali di Q che contengono N sono normali. D'altra parte ogni sottogruppo normale non banale di Q contiene N: infatti sia L un sottogruppo normale non banale, con $L \neq N$. Allora L contiene un elemento fuori da N, cioè un elemento di $\{i, j, k, -i, -j, -k\}$. Se x sta in questo insieme allora $x^2 = -1$ e quindi L contiene -1, per cui contiene $\langle -1 \rangle = N$. Ne segue che tutti i sottogruppi di Q sono normali in Q. È facile dedurne il reticolo

dei sottogruppi di Q.



1.1. **Gli automorfismi del gruppo dei quaternioni.** Vogliamo capire come è fatto il gruppo degli automorfismi di Q_8, $A = \mathrm{Aut}(Q_8)$. Per risolvere questo tipo di problema, tipicamente si cerca di capire qualcosa sull'ordine $|A|$ e successivamente si trova un sottogruppo di A "abbastanza grande" (a confronto di $|A|$) da farci capire come è fatto A.

1.2. **Quanti automorfismi?** Cominciamo col capire qualcosa su $|A|$. Siccome l'azione di coniugio di Q su se stesso determina un omomorfismo $Q \to A$ con nucleo $N = \langle -1\rangle$ abbiamo che per il teorema di isomorfismo Q/N si immerge in A come sottogruppo di ordine 4. Inoltre siccome $Q = \langle i, j\rangle$ e $jij^{-1} = -jij = iij = -i$, $iji^{-1} = -iji = iij = -j$ abbiamo che ogni automorfismo interno (cioè ogni automorfismo dato dal coniugio per qualche elemento di Q) verifica $\varphi(x) = \pm x$ per ogni $x \in Q$. Ci sono esattamente quattro automorfismi siffatti, determinati da dove mandano i due generatori i, j :

- φ manda i in i e j in j. Si tratta dell'automorfismo identico.
- φ manda i in i e j in $-j$. Si tratta del coniugio con i.
- φ manda i in $-i$ e j in j. Si tratta del coniugio con j.
- φ manda i in $-i$ e j in $-j$. Si tratta del coniugio con k.

Sia I il sottogruppo di A che consiste degli automorfismi interni. Abbiamo appena dimostrato che $I \cong Q/N$, ma non solo: siccome se $x \in Q$ allora $xN = \{x, -x\}$, I coincide con l'insieme

$$\{\varphi \in A \ : \ \varphi(xN) = xN \ \forall x \in Q\}.$$

Ora siccome N è caratteristico in Q (è l'unico sottogruppo di Q di ordine 2), c'è un'azione indotta di A su Q/N, quella definita da $\varphi(xN) := \varphi(x)N$ per $\varphi \in A$, $x \in Q$ (osserviamo che tale azione è ben definita appunto perché $\varphi(N) = N$ per ogni $\varphi \in A$, cioè N è caratteristico). Siccome $Q/N \cong C_2 \times C_2$ ha esattamente tre elementi di ordine 2, che sono iN, jN e kN, ne deduciamo un'azione di A su $\{iN, jN, kN\}$. Il nucleo di tale azione è proprio I. Per il teorema di isomorfismo A/I è isomorfo a un sottogruppo di S_3, in particolare $|A/I| \leq |S_3|$ e quindi $|A| \leq |I| \cdot |S_3| = 4 \cdot 6 = 24$.

In altre parole Q_8 ha al più 24 automorfismi. Nella prossima sezione mostriamo che $A = \mathrm{Aut}(Q_8)$ contiene un sottogruppo isomorfo a S_4, per cui, siccome come abbiamo visto $|A| \leq 24 = |S_4|$, deduciamo che $A \cong S_4$.

1.3. **Un gruppo di matrici.** Per capire meglio come è fatto A studiamo il gruppo di matrici $G = GL(2,3)$, cioè il gruppo delle matrici 2×2 invertibili a coefficienti nel campo con tre elementi $\mathbb{F}_3$. La funzione che manda una matrice nel suo determinante è un omomorfismo $G \to \mathbb{F}_3^* = \{1, -1\}$ di nucleo $SL(2,3)$, il gruppo delle matrici 2×2 invertibili su $\mathbb{F}_3$ di determinante 1. Per il teorema di isomorfismo $GL(2,3)/SL(2,3) \cong \mathbb{F}_3^* \cong C_2$ e quindi $SL(2,3)$ ha indice 2 in $GL(2,3)$. Sia Q un 2-sottogruppo di Sylow di $S = SL(2,3)$.

(1) Q è normale in G.

Per dimostrarlo studiamo gli elementi di G di ordine una potenza di 2. Naturalmente c'è un unico elemento di ordine $2^0 = 1$, l'identità.

- Sia ora $g \in G$ un elemento di ordine 2. Allora $g^2 = 1$ quindi il polinomio minimo $f(X)$ di g divide $X^2 - 1 = (X-1)(X+1)$. Se $f(X) = X - 1$ allora $g = 1$, escluso essendo $o(g) = 2$, se $f(X) = X + 1$ allora $g = z = -1$ è una matrice scalare e sta in $S \cap Z(G) = Z(S)$. L'altra possibilità è che $f(X) = X^2 - 1$, ma in questo caso, siccome g è una matrice 2×2, $f(X)$ coincide col polinomio caratteristico di g e quindi il suo termine noto è il determinante di g, cioè $\det(g) = f(0) = -1$, in altre parole $g \notin S$. Ne segue che tutti gli elementi di G di ordine 2 diversi da -1 stanno fuori da S. Quindi $z = -1$ è l'unico elemento di S di ordine 2.
- Sia ora $g \in G$ un elemento di ordine 4. Allora $g^4 = 1$ quindi il polinomio minimo$f(X)$ di g divide $X^4 - 1 = (X^2-1)(X^2+1)$. Inoltre $f(X)$ non divide $X^2 - 1$ essendo $g^2 \neq 1$ (g ha ordine 4) quindi, siccome $X^2 + 1$ è irriducibile su $\mathbb{F}_3$ (ha grado 2 e non ha zeri in $\mathbb{F}_3$) si deve avere $f(X) = X^2 + 1$. Siccome g è una matrice 2×2, $f(X)$ coincide col polinomio caratteristico e quindi il suo termine noto è il determinante di g, cioè $\det(g) = f(0) = 1$, in altre parole $g \in S$. Ne segue che tutti gli elementi di G di ordine 4 stanno in S. Possiamo trovarli tutti: se g ha ordine 4 allora sta in S e g^2 sta in S e ha ordine 2, per cui $g^2 = z = -1$ (per quanto visto sopra z è l'unico elemento di S di ordine 2), e scrivendo $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ risolvendo l'equazione $g^2 = -1$ troviamo le seguenti possibilità per g:

$$\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}.$$

Ne segue che G ha esattamente sei elementi di ordine 4, tutti dentro S.

- Sia ora $g \in G$ un elemento di ordine 8. Allora $g^8 = 1$ quindi il polinomio minimo$f(X)$ di g divide $X^8 - 1 = (X^4 - 1)(X^2 + X - 1)(X^2 - X - 1)$. Inoltre $f(X)$ non divide $X^4 - 1$ essendo $g^4 \neq 1$ (g ha ordine 8) quindi, siccome $X^2 + X - 1$ e $X^2 - X - 1$ sono irriducibili su $\mathbb{F}_3$ (hanno grado 2 e non hanno zeri in $\mathbb{F}_3$) si deve avere $f(X) = X^2 + X - 1$ oppure $f(X) = X^2 - X - 1$. Siccome g è una matrice 2×2, $f(X)$ coincide col polinomio caratteristico e quindi il suo termine noto è il determinante di g, cioè $\det(g) = f(0) = -1$, in altre parole $g \notin S$. Ne segue che tutti gli elementi di G di ordine 8 stanno fuori da S. D'altra parte G ha elementi di ordine 8, per esempio $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Ne segue che gli elementi di ordine una potenza di 2 in S sono 1, $z = -1$ e i sei elementi di G di ordine 4, quindi otto elementi in totale. Siccome Q consiste di otto elementi, ne segue che Q contiene tutti e soli gli elementi di S di ordine una potenza di 2, per cui $Q \trianglelefteq S$. Non solo: siccome il quadrato di un elemento di ordine 4 è uguale a z, gli elementi di G di ordine 4 generano Q e quindi $Q \trianglelefteq G$ (un sottogruppo generato da un sottoinsieme stabile per coniugio è normale).

(2) $Q \cong Q_8$.

Siccome l'unico gruppo di ordine 8 con un elemento di ordine 2 e sei elementi di ordine 4 è Q_8, otteniamo $Q \cong Q_8$.

(3) Siano $z = -1$, $Z = \langle z \rangle$. Allora $G/Z \cong S_4$.

Siccome z è una matrice scalare, $Z \subseteq Z(G)$. Sia $g := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Allora $P := \langle g \rangle$ ha ordine 3 quindi è un 3-Sylow di G. Siccome $g \in S$ e tutti i 3-Sylow sono coniugati e S è normale in G, tutti i 3-Sylow di G sono contenuti in S e quindi $n_3(G) = n_3(S)$. Siccome $n_3(S)$ divide $|S|/3 = 8$ ed è congruo a 1 modulo 3, $n_3(S) \in \{1, 4\}$. D'altra parte $n_3(S) \neq 1$ perché $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ è un elemento di ordine 3 che non appartiene a P, e quindi genera un 3-Sylow diverso da P. Ne segue che $n_3(S) = 4$. Si ha allora $4 = n_3(S) = |S : N_S(P)|$ per cui $N_S(P) = |S|/4 = 6$. Siccome Z è contenuto nel centro di G certamente il normalizzante $N_S(P)$ contiene P e Z, quindi contiene PZ, e siccome $P \cap Z = \{1\}$ (hanno ordine coprimo) si ha $|PZ| = |P||Z| = 3 \cdot 2 = 6$. Siccome $|N_S(P)| = 6$ ne segue che $N_S(P) = PZ \cong P \times Z \cong C_3 \times C_2 \cong C_6$. Ma allora $N_S(P)$ centralizza P quindi, siccome $C_S(P) \subseteq N_S(P)$, si deve avere $C_S(P) = N_S(P)$. Sia $K := N_G(P)$. Allora $4 = n_3(S) = n_3(G) = |G : K|$ da cui $|K| = |G|/4 = 12$. Consideriamo il cuore normale K_G. Mostriamo che $P \not\subseteq K_G$. Se fosse $P \subseteq K_G$ allora essendo $K_G \subseteq K = N_G(P)$ si avrebbe $P \trianglelefteq K_G$ e quindi P è caratteristico in K_G (se un sottogruppo di Sylow è normale allora è caratteristico, per il teorema di Sylow: applicare un automorfismo preserva l'ordine di un sottogruppo), per cui P è normale in G (infatti l'azione di coniugio di G induce automorfismi di K_G) ma questo è falso perché $n_3(G) = 4$. Ne segue che $P \not\subseteq K_G$, e siccome $|P| = 3$ segue $K_G \cap P = \{1\}$. Ora siano $x \in K_G$, $y \in P$. L'elemento $xyx^{-1}y^{-1}$ sta in P perché $xyx^{-1} \in P$, essendo $y \in P$ e $x \in K_G \subseteq K = N_G(P)$, e sta in K_G perché $yx^{-1}y^{-1} \in K_G$ essendo $x^{-1} \in K_G$ e $K_G \trianglelefteq G$. Siccome $K_G \cap P = \{1\}$ segue $xyx^{-1}y^{-1} = 1$, cioè $xy = yx$. Per cui $K_G \leq C_G(P)$.

Ora, siccome $n_3(G) = n_3(S) = 4$, e i 3-Sylow hanno ordine 3, G ha $2 \cdot 4 = 8$ elementi di ordine 3 e siccome g ha $|S : C_S(P)| = |S : PZ| = 4$ coniugati in S il numero di coniugati di g in G è uguale a

$$|G : C_G(P)| = |G : S||S : C_S(P)|/|C_G(P) : C_S(P)| = 8/|C_G(P) : C_S(P)|$$

quindi è 4 oppure 8 (è almeno 4 e divide 8). Un elemento che coniuga g in un elemento di $P = \langle g \rangle$ deve stare nel normalizzante di P, in particolare se sta in $SL(2, 3)$ allora fissa g, essendo $N_S(P) = C_S(P)$. Ne segue che g e g^{-1} non sono coniugati in $SL(2, 3)$. D'altra parte lo sono in $GL(2, 3)$,

infatti

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Ne segue che g ha più coniugati in $GL(2,3)$ di quanti ne ha in $SL(2,3)$, quindi per quanto detto sopra g ha 8 coniugati in $GL(2,3)$. Ma allora $8 = |G : C_G(P)| = 8/|C_G(P) : C_S(P)|$ da cui $C_G(P) = C_S(P) = PZ$. Ne deduciamo che $K_G \leq C_G(P) = PZ$. Siccome P non è contenuto in K_G e $|P| = 3$, $|Z| = 2$ ne segue $K_G = Z$. Ma $K = N_G(P)$ ha indice $n_3(G) = 4$ in G, quindi G/K_G si immerge in S_4. Siccome $|G/K_G| = |G/Z| = 24$ otteniamo che $G/Z = G/K_G \cong S_4$.

(4) I sottogruppi normali di G sono tutti e soli i seguenti:

$$\{1\} < Z < Q < S < G.$$

Per il teorema di corrispondenza, siccome $G/Z \cong S_4$ e sappiamo quali sono i sottogruppi normali di S_4, i sottogruppi normali di G che contengono Z sono Q, S e G; inoltre $Q/Z \cong C_2 \times C_2$, $S/Z \cong A_4$, $G/Q \cong S_3$. Per concludere basta mostrare che ogni sottogruppo normale non banale di G contiene Z. Per assurdo sia $M \trianglelefteq G$ con $M \neq \{1\}$ e $Z \not\subseteq M$. Allora $MZ \trianglelefteq G$ è uno dei sottogruppi normali contenenti Z, cioè $MZ \in \{Q, S, G\}$ (non può essere $MZ = Z$ perché $M \not\subseteq Z$). In particolare MZ contiene Q. Siccome ogni sottogruppo non banale di Q contiene Z (come si evince dal reticolo dei sottogruppi di Q_8), e M non contiene Z, si ha $M \cap Q = \{1\}$. Sia $x \in Q$ di ordine 4. Siccome $MZ \supseteq Q$ possiamo scrivere $x = my$ con $m \in M$, $y \in Z$ per cui $m = xy^{-1} \in M \cap Q$ essendo $y \in Z \subseteq Q$. Siccome $M \cap Q = \{1\}$ abbiamo $x = y$ assurdo perché x ha ordine 4 e $y \in Z$ ha ordine 1 o 2.

(5) $C_G(Q) = Z = Z(G)$.

Siccome $Q \trianglelefteq G$, anche $C_G(Q) \trianglelefteq G$ e siccome Q non è abeliano, $C_G(Q)$ non contiene Q. Siccome gli unici sottogruppi normali di G sono $\{1\} < Z < Q < S < G$ e $Z \subseteq C_G(Q)$ si deve avere $C_G(Q) = Z$. Inoltre siccome Z è contenuto nel centro (consiste di matrici scalari) ed è l'unico sottogruppo normale non banale abeliano, si deve avere $Z(G) = Z$.

(6) $S_4 \cong G/Z$ si immerge in $A = \mathrm{Aut}(Q)$.

Per quanto visto $G/Z \cong S_4$ e $Z = C_G(Q)$. Ora l'azione di coniugio di G su Q determina un omomorfismo $G \to A$ di nucleo $C_G(Q) = Z$, quindi per il teorema di isomorfismo G/Z si immerge in A.

Aggiungiamo una curiosità sui 2-sottogruppi di Sylow di $G = GL(2,3)$. Sia X uno di essi. Allora siccome Q è un 2-sottogruppo normale di G, per il teorema di Sylow $Q \subseteq X$, e siccome $|X| = 16$ e $|Q| = 8$, si ha $|X : Q| = 2$. Inoltre X/Z è un 2-sottogruppo di Sylow di $G/Z \cong S_4$ quindi $X/Z \cong D_4$, il gruppo diedrale di ordine 8. Ne segue che X è un gruppo di ordine 16 che ha Q_8 come sottogruppo e D_4 come quoziente.

2. Un gruppo commutativo di matrici

Sia p un numero primo dispari. Si consideri il seguente insieme:

$$R := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_p\}.$$

Nel seguito mostriamo che R è un anello commutativo unitario. Inoltre detto G il gruppo delle unità di R (il gruppo dei suoi elementi invertibili), cioè

$$G = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_p, \ a^2 + b^2 \neq 0\},$$

si ha:

- Se $p \equiv 3 \mod 4$ allora R è un campo di p^2 elementi e $G \cong C_{p^2-1}$;
- Se $p \equiv 1 \mod 4$ allora $G \cong C_{p-1} \times C_{p-1}$.

2.1. **Svolgimento.** Che R sia un anello commutativo unitario segue dalle seguenti relazioni.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \in R.$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Ricordiamo che per un primo dispari p le seguenti affermazioni sono equivalenti:

- $p \equiv 1 \mod 4$.
- $\mathbb{F}_p$ contiene una radice quadrata di -1.

Questo segue dal fatto che $\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ è un gruppo moltiplicativo ciclico. Infatti se $p \equiv 1 \mod 4$ allora 4 divide $p-1$ quindi $\mathbb{F}_p^*$ contiene un elemento i di ordine 4 (detto x un generatore del gruppo ciclico $\mathbb{F}_p^*$, $o(x) = p-1$ quindi $x^{(p-1)/4}$ ha ordine 4), per cui $i^2 \neq 1$ e $(i^2)^2 = 1$ da cui $i^2 = -1$ (essendo i^2 una radice di $X^2 - 1$ diversa da 1). Viceversa se $\mathbb{F}_p$ contiene una radice quadrata di -1, sia essa i, allora $i^2 = -1$ da cui $i \neq 1$ (osserviamo che $1 \neq -1$ essendo $p \neq 2$) e $i^3 = -i \neq 1$, e $i^4 = (-1)^2 = 1$, da cui i ha ordine 4 in $\mathbb{F}_p^*$, un gruppo di ordine $p-1$, quindi 4 divide $p-1$, cioè $p \equiv 1 \mod 4$.

Ora la condizione $a^2 + b^2 = 0$ per $a, b \in \mathbb{F}_p$ è equivalente, se $b \neq 0$, alla condizione $(a/b)^2 = -1$, in particolare in $\mathbb{F}_p$ c'è una radice quadrata di -1, quindi se $p \equiv 3 \mod 4$ da $a^2 + b^2 = 0$ segue $a = b = 0$, in altre parole la matrice nulla è l'unico elemento non invertibile di R. Quindi in questo caso R è un anello commutativo unitario ogni cui elemento non nullo è invertibile, cioè R è un campo di ordine p^2. Siccome il gruppo moltiplicativo di un campo finito è ciclico, otteniamo allora $G \cong C_{p^2-1}$.

Supponiamo ora che sia $p \equiv 1 \mod 4$. Sia i una radice quadrata di -1 in $\mathbb{F}_p$.

(1) $|G| = (p-1)^2$.

Contiamo le coppie (a, b) in $\mathbb{F}_p^2$ tali che $a^2 + b^2 = 0$. Se $b = 0$ allora $a = 0$ e troviamo la coppia $(0, 0)$. Supponiamo ora $b \neq 0$. Allora $(a/b)^2 = -1$ cioè a/b è radice del polinomio $X^2 + 1$. Le radici di questo polinomio sono i e $-i$ (infatti $X^2 + 1 = (X + i)(X - i)$ e in un campo un prodotto è zero se e solo se è zero uno dei fattori) quindi ci sono due possibili valori per $u = a/b$. Quindi per ognuno dei $p-1$ possibili valori di $b \neq 0$ ci sono 2 valori possibili per $a = ub$, ne segue che $|\{(a, b) \in \mathbb{F}_p^2 \ : \ a^2 + b^2 = 0\}| = 1 + 2(p-1)$. Ma allora $|G| = |R| - (1 + 2(p-1)) = p^2 - 1 - 2(p-1) = (p-1)^2$.

(2) Sia $S = \{a^2 \ : \ a \in \mathbb{F}_p\}$. Allora $|S| = (p+1)/2 > p/2$.

Consideriamo l'applicazione $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$ che manda a in a^2. Siccome $\mathbb{F}_p^*$ è un gruppo moltiplicativo abeliano, φ è un omomorfismo di gruppi. Il suo nucleo consiste degli $a \in \mathbb{F}_p$ tali che $a^2 = 1$. L'equazione polinomiale $X^2 = 1$ sul campo $\mathbb{F}_p$ ha come uniche soluzioni 1 e -1 (infatti da $X^2 = 1$ segue $(X-1)(X+1) = 0$ e in un campo un prodotto è zero se e solo se è zero uno dei fattori). Inoltre l'immagine di φ, per definizione, è uguale a $S - \{0\}$. Segue dal teorema di isomorfismo che $S - \{0\}$ è un sottogruppo di $\mathbb{F}_p^*$ isomorfo a $\mathbb{F}_p^*/\{1, -1\}$ per cui $|S - \{0\}| = (p-1)/2$. Siccome $|S - \{0\}| = |S| - 1$ segue che $|S| = 1 + (p-1)/2 = (p+1)/2$.

(3) $\{a^2 + b^2 \ : \ a, b \in \mathbb{F}_p\} = \mathbb{F}_p$.

Sia $S := \{a^2 \ : \ a \in \mathbb{F}_p\}$. Sia $x \in \mathbb{F}_p$. Come visto sopra $|S| > p/2 = |\mathbb{F}_p|/2$, e siccome $x - S = \{x - s \ : \ s \in S\}$ ha cardinalità $|x - S| = |S| > p/2$, certamente $S \cap (x - S) \neq \emptyset$, cioè esistono $s, r \in S$ con $x - s = r$, da cui $x = s + r$.

(4) L'applicazione $\det : G \to \mathbb{F}_p^*$ che manda una matrice nel suo determinante è suriettiva e detto N il suo nucleo, $N = G \cap SL(2,p)$ e $|N| = p - 1$, $G/N \cong C_{p-1}$.

Per il punto precedente $\det : G \to \mathbb{F}_p^*$ è suriettiva. Il suo nucleo N consiste delle matrici in G di determinante 1, cioè $N = G \cap SL(2,p)$. Per il teorema di isomorfismo $G/N \cong \mathbb{F}_p^* \cong C_{p-1}$ quindi, siccome $|G| = (p-1)^2$, segue $|N| = |G|/(p-1) = p - 1$.

(5) Se $g \in G$ allora $g^{p-1} = 1$.

Osserviamo che una matrice A diagonale invertibile a coefficienti in $\mathbb{F}_p$ certamente verifica $A^{p-1} = 1$ (gli elementi diagonali appartengono al gruppo moltiplicativo $\mathbb{F}_p^*$ di ordine $p-1$), quindi siccome l'ordine di un elemento è uguale all'ordine dei suoi coniugati, se un elemento $g \in G$ è diagonalizzabile allora $g^{p-1} = 1$. Quindi per concludere basta mostrare che gli elementi di G sono matrici diagonalizzabili (in $GL(2,p)$, non necessariamente in G). Il polinomio caratteristico di $g = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ è $(X-a)^2 + b^2 = X^2 - 2aX + (a^2 + b^2)$, il suo discriminante è $-b^2 = (ib)^2$ per cui i due autovalori di g sono $a \pm ib$. Ora se $b \neq 0$ questi due autovalori sono distinti quindi g è diagonalizzabile. Se invece $b = 0$ allora $g = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ è addirittura diagonale, in particolare è diagonalizzabile.

(6) N è ciclico: $N \cong C_{p-1}$.

Sappiamo che $|N| = p - 1$. Ci resta da trovare un elemento $g \in N$ di ordine $p - 1$. Scriviamo $g = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Come visto sopra, siccome in questo caso $a^2 + b^2 = \det(g) = 1$, il polinomio caratteristico di g è $X^2 - 2aX + 1$, e i due autovalori sono $a \pm ib$. Abbiamo visto che g è diagonalizzabile ed è anzi coniugata (in $GL(2,p)$, non necessariamente in G) alla matrice $\begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix}$. Inoltre essendo $a^2+b^2 = 1$, $(a+ib)^{-1} = a - ib$. Quindi siamo ricondotti a trovare un elemento di $\mathbb{F}_p^*$ della forma $a+ib$, con $a^2 + b^2 = 1$, che abbia ordine $p-1$. Dato $x \in \mathbb{F}_p^*$ di ordine $p-1$ (esiste perché $\mathbb{F}_p^*$ è ciclico), cerchiamo $a, b \in \mathbb{F}_p$ tali che $a^2 + b^2 = 1$ e $a + ib = x$.

Siccome $a = x - ib$ dobbiamo avere $1 = a^2 + b^2 = (x - ib)^2 + b^2 = x^2 - 2ibx$ da cui $b = \frac{x^2-1}{2ix}$, e deduciamo che $a = x - ib = \frac{x^2+1}{2x}$. Abbiamo finito.

(7) Esistono interi $n, m > 1$ con $nm = (p-1)^2$, $G \cong C_n \times C_m$.

Si ha $N = G \cap SL(2,p) \cong C_{p-1}$ e $G/N \cong C_{p-1}$. Siano $x \in N$ un generatore di N e $g \in G$ un elemento tale che gN è un generatore del gruppo ciclico G/N. Allora $\langle x, g\rangle = G$, infatti siccome ogni laterale di N in G è del tipo $g^k N$ (perché G/N è ciclico), e $N = \langle x\rangle$, $\langle x, g\rangle$ contiene tutti i laterali di N quindi è uguale a G. Quindi G è un gruppo abeliano 2-generato. Per il teorema fondamentale di struttura dei gruppi abeliani finiti segue che esistono interi positivi n, m con $G \cong C_n \times C_m$. Osserviamo che G è un gruppo di ordine $(p-1)^2$ ogni cui elemento g verifica $g^{p-1} = 1$ (come visto) quindi G non è ciclico (per essere ciclico dovrebbe avere un elemento di ordine $(p-1)^2$). Ne segue che $n, m > 1$. Inoltre $nm = |G| = (p-1)^2$.

(8) $G \cong C_{p-1} \times C_{p-1}$.

Ci rimane da mostrare che $n = m = p - 1$. Osserviamo che siccome $g^{p-1} = 1$ per ogni $g \in G$ e g ha elementi di ordine $p-1$ (perché $N \cong C_{p-1}$), l'esponente di G (cioè il minimo intero positivo k tale che $g^k = 1$ per ogni $g \in G$, cioè il minimo comune multiplo degli ordini degli elementi di G) è proprio $p-1$. D'altra parte $G \cong C_n \times C_m$ ha esponente $\mathrm{mcm}(n, m)$ quindi $\mathrm{mcm}(n, m) = p - 1$. Ne segue che n, m sono due interi positivi tali che $\mathrm{mcm}(n, m) = p - 1$ e $nm = (p-1)^2$, quindi $n = m = p - 1$.

3. Il teorema di Schur-Zassenhaus, caso abeliano

Un importante risultato in teoria dei gruppi è il teorema di Schur-Zassenhaus:

Teorema 1 (Schur-Zassenhaus)**.** *Sia G un gruppo finito con un sottogruppo normale N tale che $|N|$ e $|G : N|$ sono coprimi. Allora G ha un sottogruppo di ordine $|G : N|$. Inoltre tutti i sottogruppi di G di ordine $|G : N|$ sono coniugati.*

Qui dimostriamo questo teorema nel caso in cui N è abeliano.

3.1. Il caso abeliano.

Teorema 2 (Schur-Zassenhaus, caso abeliano)**.**
Sia G un gruppo finito con un sottogruppo normale abeliano N tale che $|N|$ e $|G : N|$ sono coprimi. Allora G ha un sottogruppo di ordine $|G : N|$. Inoltre tutti i sottogruppi di G di ordine $|G : N|$ sono coniugati.

Dimostrazione. Dati due elementi $x, y \in G$ indicheremo con x^y il coniugato $y^{-1}xy$, e con x^{-y} l'elemento $(x^{-1})^y$. Un "1-cociclo" o "derivazione" è una mappa $\varphi : G \to N$ tale che $\varphi(xy) = \varphi(x)^y \varphi(y)$ per ogni $x, y \in G$.

Sia $\varphi : G \to N$ un 1-cociclo. Allora si hanno i seguenti fatti.

(1) $\varphi(1) = 1$.

Infatti $1 = 1 \cdot 1$ quindi $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)^1 \varphi(1) = \varphi(1)\varphi(1)$, da cui moltiplicando per $\varphi(1)^{-1}$ entrambi i membri troviamo $\varphi(1) = 1$.

(2) $\varphi(x^{-1}) = \varphi(x)^{-x^{-1}}$. In particolare se $x \in N$ allora $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Infatti $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)^{x^{-1}} \varphi(x^{-1})$. La seconda asserzione segue dal fatto che N è abeliano.

(3) $K := \{g \in G \mid \varphi(g) = 1\} \leq G$.

Infatti $1 \in K$ dal punto (1), e se $x, y \in K$ allora $\varphi(xy) = \varphi(x)^y \varphi(y) = 1^y \cdot 1 = 1$ quindi $xy \in K$. Inoltre se $x \in K$ allora dal punto (2) $\varphi(x^{-1}) = \varphi(x)^{-x^{-1}} = 1^{-x^{-1}} = 1$ quindi $x^{-1} \in K$.

(4) $\varphi(x) = \varphi(y)$ se e solo se $Kx = Ky$.

Supponiamo $\varphi(x) = \varphi(y)$. Allora

$$\begin{aligned} \varphi(xy^{-1}) &= \varphi(x)^{y^{-1}} \varphi(y^{-1}) = \varphi(y)^{y^{-1}} \varphi(y^{-1}) \\ &= \varphi(yy^{-1}) = \varphi(1) = 1, \end{aligned}$$

per cui $xy^{-1} \in K$, cioè $x \in Ky$, cioè $Kx = Ky$. Viceversa se $Kx = Ky$ allora $xy^{-1} \in K$ da cui $1 = \varphi(xy^{-1}) = \varphi(x)^{y^{-1}} \varphi(y^{-1}) = \varphi(x)^{y^{-1}} \varphi(y)^{-y^{-1}}$ per cui coniugando con y troviamo $1 = \varphi(x)\varphi(y)^{-1}$, cioè $\varphi(x) = \varphi(y)$.

(5) $|\varphi(G)| = |G : K|$.

Mostriamo che se $g \in G$ allora $\varphi^{-1}(\varphi(g)) = Kg$. Dire che $h \in \varphi^{-1}(\varphi(g))$ è come dire che $\varphi(h) = \varphi(g)$, cioè $Kh = Kg$ (dal punto (4)), cioè $h \in Kg$. Quindi $\varphi^{-1}(\varphi(g)) = Kg$. In particolare $|\varphi^{-1}(\varphi(g))| = |Kg| = |K|$. Ora $G = \bigcup_{n \in \varphi(G)} \varphi^{-1}(n)$ è un'unione disgiunta quindi

$$|G| = \sum_{n \in \varphi(G)} |\varphi^{-1}(n)| = \sum_{n \in \varphi(G)} |K| = |\varphi(G)| \cdot |K|$$

da cui $|\varphi(G)| = |G|/|K| = |G : K|$.

Un "trasversale" di N in G è un insieme di elementi $\{g_1, \ldots, g_k\}$, dove $k = |G : N|$, tali che $g_1 N, \ldots, g_k N$ sono tutti e soli i laterali di N (osserviamo che siccome N è normale non serve distinguere tra "laterali destri" e "laterali sinistri" dato che $gN = Ng$ per ogni $g \in G$). Sia $\mathfrak{T}$ l'insieme di tutti i trasversali di N in G, e siano $S, T \in \mathfrak{T}$. Definiamo

$$d(S, T) := \prod_{s \in S, t \in T, s^{-1}t \in N} s^{-1}t \in N.$$

Osserviamo che questo prodotto è ben definito perché non importa l'ordine in cui moltiplichiamo elementi di N, essendo N abeliano! Inoltre tale prodotto consiste di esattamente $|G : N|$ fattori, infatti se $s \in S$ c'è un unico $t \in T$ tale che $Ns = Nt$ (per definizione di trasversale). Alcune osservazioni: se $S, T, U \in \mathfrak{T}$ allora

(1) $d(S, T) \cdot d(T, U) = d(S, U)$.

Scriviamo $S = \{s_1, \ldots, s_k\}$, $T = \{t_1, \ldots, t_k\}$, $U = \{u_1, \ldots, u_k\}$, in modo che $Ns_i = Nt_i = Nu_i$ per $i = 1, \ldots, k = |G : N|$. Allora siccome N è abeliano e $s_i^{-1}t_i, t_i^{-1}u_i \in N$ per ogni $i \in \{1, \ldots, k\}$,

$$d(S, T) \cdot d(T, U) = \prod_{i=1}^{k} s_i^{-1}t_i \cdot \prod_{i=1}^{k} t_i^{-1}u_i = \prod_{i=1}^{k} s_i^{-1}u_i = d(S, U).$$

(2) $d(S, T)^g = d(Sg, Tg)$.

Qui $Sg = \{sg \ : \ g \in G\}$, $Tg = \{tg \ : \ g \in G\}$ sono anch'essi trasversali di N in G. Scriviamo come sopra $S = \{s_1, \ldots, s_k\}$, $T = \{t_1, \ldots, t_k\}$ in modo che $Ns_i = Nt_i$ per $i = 1, \ldots, k = |G : N|$. Si ha allora

$$d(S, T)^g = g^{-1} \cdot \prod_{i=1}^{k} s_i^{-1}t_i \cdot g = \prod_{i=1}^{k} g^{-1}s_i^{-1}t_i g = \prod_{i=1}^{k} (s_i g)^{-1}(t_i g) = d(Sg, Tg).$$

(3) $d(S, Sn) = n^{|G:N|}$ per ogni $n \in N$.
Scriviamo $S = \{s_1, \ldots, s_k\}$ dove $k = |G : N|$. Allora

$$d(S, Sn) = \prod_{i=1}^{k} s_i^{-1} \cdot s_i n = \prod_{i=1}^{k} n = n^k.$$

Ora fissiamo $T \in \mathfrak{T}$, e definiamo $\vartheta : G \to N$ tramite la posizione $\vartheta(g) := d(T, Tg)$. Le proprietà elencate implicano che ϑ è un 1-cociclo suriettivo. Infatti:

$$\begin{aligned} \vartheta(g_1 g_2) &= d(T, Tg_1g_2) = d(T, Tg_2) \cdot d(Tg_2, Tg_1g_2) = \\ &= d(T, Tg_1)^{g_2} \cdot d(T, Tg_2) = \vartheta(g_1)^{g_2}\vartheta(g_2). \end{aligned}$$

ϑ è suriettivo perché se $n \in N$ allora poiché $(|N|, |G : N|) = 1$, una opportuna potenza di $\vartheta(n) = n^{|G:N|}$ è uguale a n. Come visto $K := \{g \in G \mid \vartheta(g) = 1\}$ è un sottogruppo di G. Siccome ϑ è suriettivo, $|N| = |\vartheta(G)| = |G : K|$, per cui $|K| = |G : N|$, cioè K è un sottogruppo di G di ordine $|G : N|$, quello che vogliamo.

Sia ora H un altro sottogruppo di G di ordine $|G : N|$. In particolare siccome $|G : N| = |H|$ e $|G : H| = |N|$ sono coprimi, $|NH| = |N| \cdot |H| = |N| \cdot |G : N| = |G|$ da cui $NH = G$ quindi $H \in \mathfrak{T}$. Detto $m := d(H, T)$ siccome ϑ è suriettivo esiste $n \in N$ con $\vartheta(n) = m$. Dato $x \in H$, mostriamo che $\vartheta(x^n) = 1$. Osserviamo che $m^x = d(H, T)^x = d(Hx, Tx) = d(H, Tx) = d(H, T) \cdot d(T, Tx) = m \cdot \vartheta(x)$. Quindi

$$\begin{aligned} \vartheta(x^n) &= \vartheta(n^{-1}xn) = \vartheta(n^{-1}x)^n\vartheta(n) = \vartheta(n^{-1}x)m = \\ &= \vartheta(n^{-1})^x\vartheta(x)m = (\vartheta(n)^{-1})^x m\vartheta(x) = (m^x)^{-1}m\vartheta(x) = 1. \end{aligned}$$

Quindi $\vartheta(x^n) = 1$ per ogni $x \in H$. Questo implica che $H^n = K$, infatti $|H^n| = |H| = |G : N| = |K|$ e $H^n \subseteq \{g \in G \ : \ \vartheta(g) = 1\} = K$. □

4. Contenimenti di campi ciclotomici

Nel seguito indichiamo con ζ_n una radice primitiva n-esima dell'unità, e indichiamo con E_n il campo ciclotomico n-esimo, cioè $E_n = \mathbb{Q}(\zeta_n)$. Vogliamo capire quando succede che un campo ciclotomico ne contiene un altro.

Lemma 1. *Siano x, y due elementi di un gruppo con $xy = yx$ e siano $o(x) = n$, $o(y) = p^k$ con p un primo, e p^k non divida n. Allora $o(xy) = mcm(n, p^k)$.*

Dimostrazione. Supponiamo dapprima che $n = p^a$ sia una potenza di un primo. Siccome p^k non divide n, $a < k$. Sia $z := xy$. Allora $z^{p^a} = y^{p^a}$ ha ordine p^{k-a} quindi $p^{k-a} = o(z^{p^a}) = o(z)/(p^a, o(z))$ da cui

$$o(z) = p^{k-a}(p^a, o(z)) = p^{k-a}(p^a, p^{k-a}(p^a, o(z))) = \ldots = p^k.$$

Scriviamo ora $n = mp^{k-h}$ con p che non divide m. Per ipotesi $h \geq 1$. Si ha $\mathrm{mcm}(n, p^k) = np^h$. Mostriamo che xy ha ordine np^h. Siccome p non divide m, x^m ha ordine p^{k-h} e y^m ha ordine p^k. Per il caso appena discusso segue che $(xy)^m = x^m y^m$ ha ordine p^k, quindi p^k divide l'ordine di xy. Certamente $(xy)^{np^h} = x^{np^h}y^{np^h} = 1$. Ora supponiamo che $(xy)^t = 1$ e mostriamo che np^h divide t. Da $(xy)^t = 1$ deduciamo che $x^t = y^{-t}$ per cui $o(x^t) = o(x)/(t, o(x)) = n/(t, n)$ è uguale a $o(y^{-t}) = o(y^t) = o(y)/(t, o(y)) = p^k/(t, p^k)$ quindi m divide t. D'altra parte p^k divide $o(xy)$ che divide t (perché $(xy)^t = 1$) quindi p^k divide t e deduciamo che $mp^k = np^h$ divide t. □

Teorema 3. *Siano d, n interi positivi. Allora $E_d \subseteq E_n$ se e solo se d divide n oppure n è dispari e $d/2$ è un intero dispari che divide n.*

Dimostrazione. Mostriamo l'implicazione ($\Leftarrow$). Se d divide n allora ${\zeta_n}^{n/d}$ ha ordine d nel gruppo moltiplicativo $\mathbb{C}^*$ quindi una sua opportuna potenza (e quindi anche una opportuna potenza di ζ_n) è uguale a ζ_d, per cui $\zeta_d \in \mathbb{Q}(\zeta_n) = E_n$ cioè $E_d \subseteq E_n$. Se $d/2$ è dispari e $d/2$ divide n allora $-\zeta_{d/2}$ è una radice primitiva d-esima di 1 quindi $E_{d/2} = E_d$, ora siccome $d/2$ divide n si ha per il caso già discusso che $E_d = E_{d/2} \subseteq E_n$.

Mostriamo l'implicazione ($\Rightarrow$). Supponiamo che sia $E_d \subseteq E_n$, in altre parole $\zeta_d \in E_n = \mathbb{Q}(\zeta_n)$. Supponiamo dapprima che sia $d = p^k$ con p primo. Supponiamo che d non divida n. Per il lemma 1 abbiamo che $\zeta_d\zeta_n$ ha ordine np^h, dove p^{k-h} è la massima potenza di p che divide n (qui $h \geq 1$ per ipotesi), quindi $|\mathbb{Q}(\zeta_d\zeta_n) : \mathbb{Q}| = \varphi(np^h)$. Siccome $\zeta_d \in \mathbb{Q}(\zeta_n)$, $\mathbb{Q}(\zeta_d\zeta_n) \subseteq \mathbb{Q}(\zeta_n)$ e quindi per la formula dei gradi $\varphi(np^h)$ divide $\varphi(n)$. Scriviamo $n = mp^{k-h}$ cosicché dal fatto che $\varphi(np^h) = \varphi(mp^k) = \varphi(m)\varphi(p^k)$ divide $\varphi(n) = \varphi(mp^{k-h}) = \varphi(m)\varphi(p^{k-h})$ segue che $\varphi(p^k) = p^{k-1}(p-1)$ divide $\varphi(p^{k-h})$. Ora se $k > h$ allora $p^{k-1}(p-1)$ divide $\varphi(p^{k-h}) = p^{k-h-1}(p-1)$, assurdo perché $h \geq 1$. Se $k = h$ allora $\varphi(mp^k)$ divide $\varphi(m)$ da cui $\varphi(p^k) = 1$ cioè $p^k \in \{1, 2\}$. Siccome $k = h \geq 1$ otteniamo $p^k = 2$ quindi n è dispari e $d/2 = 1$ divide n.

Mettiamoci ora nel caso generale, cioè d non necessariamente una potenza di primo. Supponiamo che d non divida n. Allora esiste una potenza di primo p^k che divide d ma non n, e possiamo assumere che p^{k+1} non divida d. Inoltre scegliamo $p \neq 2$ se è possibile. Per quanto discusso sopra si deve allora avere $p^k = 2$ e n è dispari. Per la scelta di p e k segue che $d/2$ è dispari e tutte le potenze di primi dispari che dividono d dividono anche n, in altre parole $d/2$ divide n. □

4.1. **Grado di** $\cos(2\pi/n)$**,** $\sin(2\pi/n)$ **su** $\mathbb{Q}$**.**

Teorema 4. *Siano $n \geq 2$ un intero, $u := \cos(2\pi/n)$, $\omega := \sin(2\pi/n)$. Siano $D(u)$, $D(\omega)$ rispettivamente il grado di u e di ω su $\mathbb{Q}$.*

(1) $D(u) = \varphi(n)/2$ se $n \neq 2$, e $D(u) = 1$ se $n = 2$.
(2) Se 4 non divide n allora $D(\omega) = \varphi(n)$.
(3) Se $n = 4$ allora $D(\omega) = 1$.
(4) Se 4 divide n, 8 non divide n e $n > 4$ allora $D(\omega) = \varphi(n)/4$.
(5) Se 8 divide n allora $D(\omega) = \varphi(n)/2$.

Se $n \neq 4$, $D(\omega)$ risulta uguale a $\varphi(r)/2$ dove r è l'ordine moltiplicativo di $i\varepsilon$ dove $\varepsilon = u + i\omega$.

Dimostrazione. Se $n \leq 2$ allora u, ω sono numeri razionali quindi hanno grado 1 su $\mathbb{Q}$. Supponiamo ora $n \geq 3$. In particolare u, ω sono diversi da zero. Sia $\varepsilon := e^{i2\pi/n} = u + i\omega$. Allora $\varepsilon^{-1} = u - i\omega$ quindi $u = \frac{1}{2}(\varepsilon + \varepsilon^{-1})$ e $\omega = \frac{1}{2}(-i\varepsilon - (i\varepsilon)^{-1})$. Ne segue che $u \in \mathbb{Q}(\varepsilon)$ e $\omega \in \mathbb{Q}(i\varepsilon)$. Per il lemma 1, siccome i ha ordine 4, se 4 non divide n allora $i\varepsilon$ ha ordine $\mathrm{mcm}(4, n)$. Se invece 4 divide n allora scrivendo $n = 4m$ abbiamo $\varepsilon^m = e^{i2\pi/4} = i$ quindi $\omega \in \mathbb{Q}(\varepsilon)$.

Da $u = \frac{1}{2}(\varepsilon + \varepsilon^{-1})$ segue, moltiplicando per 2ε, che $2u\varepsilon = \varepsilon^2 + 1$ quindi ε è zero del polinomio $X^2 - 2uX + 1 \in \mathbb{Q}(u)[X]$ che ha grado 2, quindi ε ha grado al più 2 su $\mathbb{Q}(u)$. D'altra parte non ha grado 1 perché $\varepsilon \notin \mathbb{Q}(u)$, infatti $\varepsilon \notin \mathbb{R}$ (la sua parte immaginaria è $\sin(2\pi/n) \neq 0$ essendo $n \geq 3$) e $\mathbb{Q}(u) \subseteq \mathbb{R}$ essendo $u \in \mathbb{R}$. Ne segue

che $|\mathbb{Q}(\varepsilon):\mathbb{Q}(u)|=2$ quindi

$$\varphi(n)=|\mathbb{Q}(\varepsilon):\mathbb{Q}|=|\mathbb{Q}(\varepsilon):\mathbb{Q}(u)|\cdot|\mathbb{Q}(u):\mathbb{Q}|=2|\mathbb{Q}(u):\mathbb{Q}|$$

per cui u ha grado $\varphi(n)/2$ su $\mathbb{Q}$.

Da $\omega=\frac{1}{2}(-i\varepsilon-(i\varepsilon)^{-1})$ segue, moltiplicando per $2i\varepsilon$, che $2\omega(i\varepsilon)=-(i\varepsilon)^2-1$ da cui $i\varepsilon$ è zero del polinomio $-X^2-2\omega X-1\in\mathbb{Q}(\omega)[X]$ che ha grado 2, quindi $i\varepsilon$ ha grado al più 2 su $\mathbb{Q}(\omega)$. D'altra parte se $n\neq 4$ allora ω non ha grado 1 su $\mathbb{Q}(\omega)$ perché $i\varepsilon\notin\mathbb{Q}(\omega)$, infatti $i\varepsilon\notin\mathbb{R}$ (la sua parte immaginaria è $\cos(2\pi/n)$ quindi è diversa da zero quando $n\geq 3$ e $n\neq 4$) e $\mathbb{Q}(\omega)\subseteq\mathbb{R}$ essendo $\omega\in\mathbb{R}$. Ne segue che $|\mathbb{Q}(i\varepsilon):\mathbb{Q}(\omega)|=2$ quindi, detto r l'ordine di $i\varepsilon$, si ha

$$\varphi(r)=|\mathbb{Q}(i\varepsilon):\mathbb{Q}|=|\mathbb{Q}(i\varepsilon):\mathbb{Q}(\omega)|\cdot|\mathbb{Q}(\omega):\mathbb{Q}|=2|\mathbb{Q}(\omega):\mathbb{Q}|$$

per cui ω ha grado $\varphi(r)/2$ su $\mathbb{Q}$. Ci rimane da calcolare r.

Se 4 non divide n allora per il lemma 1, $r=\mathrm{mcm}(4,n)$. Se n è dispari allora $r=4n$ quindi $\varphi(r)=2\varphi(n)$. Se $n=2m$ con m dispari allora $r=4m$ quindi $\varphi(r)=2\varphi(m)=2\varphi(n)$.

Se 4 divide n allora scrivendo $n=4m$ abbiamo $\varepsilon^m=e^{i2\pi/4}=i$ quindi $i\varepsilon=\varepsilon^{m+1}$ per cui

$$r=o(i\varepsilon)=o(\varepsilon^{m+1})=o(\varepsilon)/(m+1,o(\varepsilon))=n/(m+1,n).$$

Ne segue che se m è pari allora $r=n$. Supponiamo ora che m sia dispari. Se 4 non divide $m+1$ allora $(m+1,n)=2$ quindi $r=n/2=2m$ e abbiamo $\varphi(r)=\varphi(2m)=\varphi(m)=\varphi(n)/2$. Se 4 divide $m+1$ allora $(m+1,n)=4$ quindi $r=n/4=m$ e abbiamo $\varphi(r)=\varphi(m)=\varphi(n)/2$. □

5. Numeri primi e polinomi irriducibili

Ho tratto questo materiale da [1]. Per fattorizzare i numeri ho usato [2].

Se un polinomio $f(X)\in\mathbb{Z}[X]$ è riducibile, $f(X)=g(X)h(X)$, allora per un $n\in\mathbb{Z}$ ci verrebbe da dire che $f(n)=g(n)h(n)$ non è un numero primo dato che è il prodotto di $g(n)$ e $h(n)$. Naturalmente dobbiamo però trattare i casi $g(n),h(n)=\pm 1$. Nel seguito viene formalizzata questa idea.

Teorema 5. *Sia $f(X)=a_mX^m+a_{m-1}X^{m-1}+\ldots+a_1X+a_0\in\mathbb{Z}[X]$ un polinomio di grado m e sia*

$$H:=\max_{0\leq i\leq m-1}|a_i/a_m|.$$

Se $f(n)$ è un numero primo per un intero $n\geq H+2$ allora $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

Quindi per esempio il polinomio X^8+1 è irriducibile perché $4^8+1=65537$ è un numero primo.

Teorema 6. *Sia $b>2$ un intero e sia p un numero primo con espansione in base b seguente:*

$$p=a_nb^n+a_{n-1}b^{n-1}+\ldots+a_1b+a_0.$$

Allora il polinomio $f(X)=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ è irriducibile in $\mathbb{Q}[X]$.

Quindi per esempio $X^3 + 2X^2 + 9X + 1$ e $X^4 + 2X^3 + 6X^2 + 4X + 1$ sono irriducibili perché 1291 e 12641 sono numeri primi.

La conclusione del Teorema 6 vale anche per $b = 2$ ma in questo caso la dimostrazione è più tecnica quindi la omettiamo. Una conseguenza per esempio è che se c'è un primo della forma $2^k + 1$ allora il polinomio $X^k + 1$ è irriducibile. È il caso di $k = 8$ e $k = 16$. Invece $X^{32} + 1$ è irriducibile mentre $2^{32} + 1 = 641 \cdot 6700417$. Inoltre l'espansione di 37 in base 2 è 100101 quindi $X^5 + X^2 + 1$ è irriducibile.

5.1. **Dimostrazione del Teorema 5.** Ci serve il lemma seguente.

Manteniamo le notazioni dell'enunciato del Teorema 5.

Lemma 2. *Sia α una radice complessa di $f(X)$. Allora $|\alpha| < H + 1$.*

Dimostrazione. Riscriviamo l'uguaglianza $f(\alpha) = 0$ nel modo seguente:

$$-a_m\alpha^m = a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0.$$

Segue che

$$|\alpha|^m \leq H(|\alpha|^{m-1} + \ldots + |\alpha| + 1) = H\left(\frac{|\alpha|^m - 1}{|\alpha| - 1}\right).$$

Quindi se $|\alpha| \leq 1$ allora $|\alpha| < H + 1$ banalmente, essendo $H > 0$, e se $|\alpha| > 1$ allora moltiplicando la relazione ottenuta per $|\alpha| - 1$ abbiamo $|\alpha|^{m+1} - |\alpha|^m < H|\alpha|^m$ da cui $|\alpha| < H + 1$. □

Procediamo con la dimostrazione del Teorema 5. Per il lemma di Gauss basta mostrare che $f(X)$ è irriducibile in $\mathbb{Z}[X]$. Supponiamo per assurdo che $f(X)$ sia riducibile in $\mathbb{Z}[X]$ e scriviamo $f(X) = g(X)h(X)$ con $g(X), h(X) \in \mathbb{Z}[X]$ non costanti. Siccome $g(n)h(n) = f(n)$ è un numero primo, si deve avere $g(n) = \pm 1$ oppure $h(n) = \pm 1$. Senza perdita in generalità supponiamo $g(n) = \pm 1$. Scriviamo $g(X) = c\prod_i (X - \alpha_i)$ dove gli α_i sono gli zeri di $g(X)$ e c è il coefficiente del termine di grado massimo di $g(X)$. Siccome $n = |n - \alpha_i + \alpha_i| \leq |n - \alpha_i| + |\alpha_i|$, per il Lemma 2 si ha

$$|g(n)| = |c| \prod_i |n - \alpha_i| \geq \prod_i (n - |\alpha_i|) > \prod_i (n - (H + 1)) \geq 1,$$

da cui $|g(n)| > 1$, e questo contraddice il fatto che $g(n) = \pm 1$.

5.2. **Dimostrazione del Teorema 6.** Ci serve il lemma seguente.

Lemma 3. *Sia $f(X) \in \mathbb{Z}[X]$ e scriviamo*

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$$

con $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Supponiamo $a_n \geq 1$ e $a_{n-1} \geq 0$. Sia H un numero reale positivo tale che $|a_i| \leq H$ per $i = 0, 1, \ldots, n - 2$. Allora per ogni zero complesso α di $f(X)$ con parte reale positiva si ha

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2}.$$

Dimostrazione. Sia $T := \frac{1+\sqrt{1+4H}}{2}$. Indichiamo con $\Re(x)$ la parte reale di $x \in \mathbb{C}$. Sia $z \in \mathbb{C}$ con $\Re(z) > 0$ e $|z| > 1$. Ricordando la disuguaglianza triangolare $|a+b| \leq |a| + |b|$ si ha $|a| \geq |a+b| - |b|$ e usando $a_n \geq 1$, $a_{n-1} \geq 0$ abbiamo

$$\begin{aligned}
\left|\frac{f(z)}{z^n}\right| &\geq \left|a_n + \frac{a_{n-1}}{z}\right| - H\left(\frac{1}{|z|^2} + \ldots + \frac{1}{|z|^n}\right) \\
&= \left|a_n + \frac{a_{n-1}}{z}\right| - H\left(\frac{1-(1/|z|)^{n+1}}{1-1/|z|} - 1 - 1/|z|\right) \\
&> \Re\left(a_n + \frac{a_{n-1}}{z}\right) - H\left(\frac{1}{1-1/|z|} - 1 - 1/|z|\right) \\
&\geq 1 - \frac{H}{|z|^2 - |z|} = \frac{|z|^2 - |z| - H}{|z|^2 - |z|}.
\end{aligned}$$

Ne segue che se la quantità $\frac{|z|^2-|z|-H}{|z|^2-|z|}$ è non negativa, cioè se $|z| \geq T$ (ricordiamo infatti che $|z| > 1$), allora $|f(z)/z^n| > 0$, in particolare $f(z) \neq 0$.

Sia ora α uno zero complesso di $f(X)$ con parte reale positiva. Siccome $H > 0$ si ha $T > 1$ quindi se $|\alpha| \leq 1$ la conclusione è immediata. Supponiamo ora che sia $|\alpha| > 1$. Allora applicando quanto visto nel caso $z = \alpha$, siccome $f(\alpha) = 0$ otteniamo $|\alpha| < T$. □

Procediamo con la dimostrazione del Teorema 6. Per il lemma di Gauss basta mostrare che $f(X)$ è irriducibile in $\mathbb{Z}[X]$. Scriviamo $f(X) = g(X)h(X)$ con $g(X), h(X) \in \mathbb{Z}[X]$, non costanti per assurdo. Da $g(b)h(b) = f(b) = a_n b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = p$ segue, siccome p è un primo, che $g(b) = \pm 1$ oppure $h(b) = \pm 1$. Senza perdita di generalità supponiamo che sia $g(b) = \pm 1$. Scriviamo $g(X) = c\prod_i (X - \alpha_i)$ dove gli α_i sono gli zeri di $g(X)$ e c è il coefficiente del termine di grado massimo di $g(X)$. Sia α uno zero di $f(X)$. Se α ha parte reale non positiva allora $|b - \alpha| \geq b > 1$. Se invece α ha parte reale positiva allora per il Lemma 3 e per il fatto che $b \geq 3$ si ha

$$|\alpha| < \frac{1 + \sqrt{1 + 4(b-1)}}{2} \leq b - 1,$$

da cui $b = |(b-\alpha) + \alpha| \leq |b-\alpha| + |\alpha| < |b-\alpha| + b - 1$ e deduciamo che $|b - \alpha| > 1$. Segue che per ogni zero α di $f(X)$ si ha $|b - \alpha| > 1$, in particolare $|b - \alpha_i| > 1$ per ogni i. Ma allora $|g(b)| = |c\prod_i (b - \alpha_i)| = |c| \prod_i |b - \alpha_i| > |c| \geq 1$ da cui $|g(b)| > 1$, e questo contraddice il fatto che $g(b) = \pm 1$.

6. Indovinello con infiniti cappelli

Il seguente indovinello è dovuto a Yuval Gabay e Michael O'Connor.

Tu e altre infinite persone indossate un cappello. Ogni cappello è rosso oppure verde. Ogni persona vede il colore del cappello di ogni altra persona, ma non vede il colore del proprio; a parte questo, non ci si può scambiare informazioni (ma si può fissare una strategia prima della comparsa dei cappelli). Simultaneamente, ognuno prova a indovinare il colore del proprio cappello. Si vince se solo un numero finito di persone si sbaglia. Trovare una strategia vincente.

La soluzione è nella prossima pagina.

Le seguenti due risoluzioni sono due formulazioni equivalenti della stessa idea in due diversi linguaggi.

Risoluzione 1. Sia X l'insieme delle persone e sia I l'insieme $\{rosso, verde\}$. Un'assegnazione di cappelli è una funzione $f : X \to I$, cioè un elemento di I^X. Diciamo che $f, g \in I^X$ sono equivalenti se l'insieme $\{x \in X \ : \ f(x) \neq g(x)\}$ è finito, cioè se f e g coincidono al di fuori di un insieme finito. Denotiamo con $[f]$ la classe di $f \in I^X$. Quando è data un'assegnazione f, la persona x conosce $f(y)$ per ogni $y \neq x$ ma non conosce $f(x)$. Siccome $\{x\}$ è un insieme finito, la persona x certamente conosce $[f]$. L'idea è che x sceglierà una $g \in [f]$ e proverà a indovinare che il colore del suo cappello è $g(x)$. La cosa funziona solo se ogni altra persona sceglie la stessa g. Quindi la strategia è la seguente: usando l'assioma della scelta, prima della comparsa dei cappelli le persone scelgono un rappresentante g_C di ogni classe di equivalenza C. Alla comparsa dei cappelli, associata all'assegnazione $f \in I^X$, ogni persona x calcola $[f]$ e dichiara che il colore del suo cappello è $g_{[f]}(x)$. Questo è tutto perché per definizione $g_{[f]}$ e f differiscono solo su un numero finito di persone.

Risoluzione 2. Sia $\mathbb{F}_2 = \{0, 1\}$ il campo con due elementi, e sia $A := \mathbb{F}_2^X$ l'insieme delle funzioni $X \to \mathbb{F}_2$, dove X è l'insieme delle persone. Allora A è un anello con le operazioni per componenti: se $f, g \in A$ definiamo $(f + g)(x) := f(x) + g(x)$ e $(fg)(x) := f(x)g(x)$ per ogni $x \in X$. Consideriamo

$$\mathfrak{J} := \{a \in A \ : \ \{x \in X \ : \ a(x) \neq 0\} \text{ è finito}\}.$$

Allora si vede facilmente che $\mathfrak{J}$ è un ideale di A. Sia

$$\pi : A \to A/\mathfrak{J}$$

la proiezione canonica. Essendo π una funzione suriettiva, essa ammette un'inversa destra π^* (per questo occorre l'assioma della scelta) - occhio: in generale π^* non è un omomorfismo di anelli. Abbiamo $\pi\pi^*(t) = t$ per ogni $t \in A/\mathfrak{J}$ (l'esistenza di π^* equivale alla possibilità di "scegliere" un rappresentante in A di $t \in A/\mathfrak{J}$ per ogni tale t). La strategia prima della comparsa dei cappelli è di fissare tale inversa destra π^*. Un'assegnazione di cappelli corrisponde a un elemento $a \in A$, dove per esempio $0 = rosso$ e $1 = verde$. Alla comparsa dei cappelli, cioè dell'assegnazione $a \in A$, la persona $x \in X$ conosce $a(y)$ per ogni $y \in X$ diverso da x. Siccome $a(x) \in \{0, 1\}$ ci sono esattamente due possibilità per a, date dai due possibili valori di $a(x)$. Siano a_0, a_1 queste due possibilità. Allora certamente $\pi(a_0) = \pi(a) = \pi(a_1)$, infatti $a - a_0$ e $a - a_1$ assumono solo un numero finito di valori diversi da zero (sono zero solo in un insieme contenuto in $\{x\}$) e quindi $a - a_0$, $a - a_1 \in \mathfrak{J} = \ker \pi$, in altre parole $0 = \pi(a - a_0) = \pi(a) - \pi(a_0)$ e $0 = \pi(a - a_1) = \pi(a) - \pi(a_1)$. Quindi x conosce $\pi(a)$ e sosterrà che il colore del suo cappello è

$$\pi^*\pi(a)(x).$$

Perché questa strategia funzioni è necessario che $\{x \in X \ : \ (\pi^*\pi(a) - a)(x) \neq 0\}$ sia finito, in altre parole $\pi^*\pi(a) - a \in \mathfrak{J} = \ker \pi$, e questo è vero perché

$$\pi(\pi^*\pi(a) - a) = \pi\pi^*\pi(a) - \pi(a) = \pi(a) - \pi(a) = 0.$$

7. Spettro di un anello: cenni di geometria algebrica

Obiettivo di questa nota è dare dei cenni di geometria algebrica moderna per suscitare curiosità. Per chi fosse interessato ad approfondire consiglio la lettura di [3], [4], [5], [6], [7] (nell'ordine).

7.1. **Topologia.** Dato un insieme X denotiamo con $\mathscr{P}(X)$ l'insieme delle parti di X, cioè l'insieme dei sottoinsiemi di X.

Definition 1 (Spazio topologico)**.** *Uno spazio topologico è una coppia $(X, \mathscr{T})$ dove X è un insieme, e $\mathscr{T}$ è un sottoinsieme di $\mathscr{P}(X)$, detto "topologia (su X)", i cui elementi si dicono "**aperti** (di X)" tale che:*

- *$\emptyset, X \in \mathscr{T}$;*
- *se $U, V \in \mathscr{T}$ allora $U \cap V \in \mathscr{T}$;*
- *se $(U_i)_{i\in I}$ è una qualsiasi famiglia di elementi di $\mathscr{T}$ allora $\bigcup_{i\in I} U_i \in \mathscr{T}$.*

*Un sottoinsieme di X si dice **chiuso** (in X) se il suo complementare in X è aperto.*

Se la topologia è sottintesa lo spazio topologico $(X, \mathscr{T})$ si può indicare semplicemente con X.

Dare una topologia ad un insieme X significa dire chi sono gli aperti di X. Ciò è equivalente a dire chi sono i chiusi di X. In altre parole:

Proposizione 1. *Sia X un insieme, e sia $\mathscr{T}$ un sottoinsieme di $\mathscr{P}(X)$. Le seguenti affermazioni sono equivalenti:*

(1) $\mathscr{T}$ è una topologia su X;
(2) $\mathscr{F} := \{X - U \mid U \in \mathscr{T}\}$ verifica le seguenti tre condizioni:
- *$\emptyset, X \in \mathscr{F}$;*
- *se $F, G \in \mathscr{F}$ allora $F \cup G \in \mathscr{F}$;*
- *se $(F_j)_{j\in J}$ è una qualsiasi famiglia di elementi di $\mathscr{F}$ allora $\bigcap_{j\in J} F_j \in \mathscr{F}$.*

Esempio: se X è un qualsiasi insieme, i seguenti sottoinsiemi di $\mathscr{P}(X)$:

$$\mathscr{P}(X), \qquad\qquad \{\emptyset, X\}$$

sono topologie su X. La prima di esse si dice "topologia discreta", la seconda "topologia banale". Un spazio topologico la cui topologia è quella discreta si dirà "spazio (topologico) discreto".

Esercizio: uno spazio topologico $(X, \mathscr{T})$ è discreto se e solo se tutti i "punti" (cioè gli insiemi della forma $\{x\}$ con $x \in X$) sono aperti.

Esercizio: se X è un punto (cioè $X = \{x\}$) c'è un'unica possibile topologia su X, quella banale.

Definition 2 (Topologia indotta sui sottoinsiemi: sottospazi topologici)**.** *Sia $(X, \mathscr{T})$ uno spazio topologico, e sia Y un sottoinsieme di X. La topologia indotta di X su Y è per definizione la topologia su Y $\mathscr{T}|_Y := \{U \cap Y \mid U \in \mathscr{T}\}$. In questo caso si dice che Y è un "sottospazio (topologico)" di X.*

Esempio: La topologia "usuale" su $\mathbb{R}$ è definita dicendo che gli aperti sono il vuoto più tutte le unioni di intervalli della forma (a, b) con $a < b$ elementi di $\mathbb{R}$. Allora la topologia indotta su $\mathbb{Z} \subset \mathbb{R}$ è quella discreta, infatti se $n \in \mathbb{Z}$ allora $(n - 1/2, n + 1/2) \cap \mathbb{Z} = \{n\}$ (quindi i punti sono aperti). Tutto ciò normalmente si sintetizza dicendo che "$\mathbb{Z}$ è discreto".

Esercizio: $\mathbb{Q}$ non è discreto (ogni suo aperto contiene infiniti punti).

Definition 3 (Spazi compatti)**.** *Sia X uno spazio topologico. Diciamo che X è compatto se una tra le seguenti condizioni equivalenti è soddisfatta:*

(1) Ogni ricoprimento aperto di X ammette un sottoricoprimento finito. Ovvero se $(U_i)_{i\in I}$ è una qualsiasi famiglia di aperti di X tale che $X = \bigcup_{i\in I} U_i$ allora esiste $J \subseteq I$ finito tale che $X = \bigcup_{j\in J} U_j$.
(2) Ogni famiglia di chiusi ad intersezione vuota ammette una sottofamiglia finita ad intersezione vuota. Ovvero se $(F_i)_{i\in I}$ è una famiglia di chiusi di X tale che $\bigcap_{i\in I} F_i = \emptyset$ allora esiste $J \subseteq I$ finito tale che $\bigcap_{j\in J} F_j = \emptyset$.

La seconda condizione in tale definizione si può esprimere anche nel seguente modo: diciamo che una famiglia di chiusi di X ha la f.i.p. (dall'inglese, *finite intersection property*) se ogni sua sottofamiglia finita ha intersezione non vuota. Allora X è compatto se e solo se ogni famiglia di chiusi di X con la f.i.p. ha intersezione non vuota.

Nello spazio topologico $\mathbb{R}$ con la topologia usuale (gli aperti sono il vuoto e le unioni di intervalli (a, b) con $a < b$ in $\mathbb{R}$) un sottospazio è compatto se e solo se è chiuso e limitato. Per esempio l'intervallo chiuso $[0, 1]$ è un sottospazio compatto di $\mathbb{R}$.

Definition 4 (Funzioni continue)**.** *Siano $(X, \mathscr{T})$, $(Y, \mathscr{T}')$ due spazi topologici. Una funzione $f : X \to Y$ si dice continua se per ogni $V \in \mathscr{T}'$, la controimmagine $f^{-1}(V)$ di V tramite f sta in $\mathscr{T}$. In altre parole, una funzione è continua se l'antiimmagine di ogni aperto è un aperto, o equivalentemente, l'antiimmagine di ogni chiuso è un chiuso.*

Nel caso di funzioni $\mathbb{R} \to \mathbb{R}$ la continuità è equivalente a commutare coi limiti, cioè quella ben nota.

Uno spazio topologico X si dice "di Hausdorff" se per ogni due punti distinti x, y di X esistono aperti disgiunti U, V di X tali che $x \in U$ e $y \in V$. Per esempio $\mathbb{R}$ con la topologia usuale è di Hausdorff.

Proposizione 2. *Siano X, Y spazi topologici e sia F un sottospazio topologico di X.*

(1) Se X è compatto e F è chiuso in X allora F è compatto.
(2) Se X è di Hausdorff e F è compatto allora F è chiuso.
(3) Se $f : X \to Y$ è una funzione continua e F è compatto allora $f(F)$ è compatto.

Dimostrazione. 1. Fissato un ricoprimento aperto di F se ci aggiungiamo $X - F$ otteniamo un ricoprimento aperto di X. Per la compattezza di X esiste un sottoricoprimento finito di X che ne contiene uno di F.

2. Per mostrare che F è chiuso (cioè che $X - F$ è aperto) fissiamo $x \in X - F$ e mostriamo che x è contenuto in un aperto di X contenuto in $X - F$ (la loro unione sarà $X - F$ che risulterà quindi un aperto, in quanto unione di aperti). Siccome X è di Hausdorff per ogni $y \in F$ esistono aperti U_y, V_y di X con $U_y \cap V_y = \emptyset$ e $x \in U_y$, $y \in V_y$. Allora ovviamente $F \subseteq \bigcup_{y\in F} V_y$ e siccome F è compatto esistono $y_1, \ldots, y_n \in F$ con $F \subseteq \bigcup_{i=1}^n V_{y_i}$. Ne segue che $x \in \bigcap_{i=1}^n U_{y_i} \subseteq X - F$ e $\bigcap_{i=1}^n U_{y_i}$ è un aperto essendo intersezione finita di aperti.

3. La controimmagine tramite f di un ricoprimento aperto di $f(F)$ è un ricoprimento aperto di F e ora basta usare la compattezza di F per dedurne un sottoricoprimento finito di $f(F)$. □

7.2. **Assiomi di separazione.** Un sottoinsieme A di uno spazio topologico X si dice "denso" se interseca tutti gli aperti non vuoti di X. Un "punto" in uno spazio topologico X è un insieme della forma $\{x\}$ con $x \in X$. Quindi un punto denso non è altro che un elemento che appartiene a tutti gli aperti non vuoti.

Definition 5 (Assiomi di separazione)**.** *Sia $(X, \mathscr{T})$ uno spazio topologico. Esso si dice:*

1. *T0 se in X c'è al più un punto denso;*
2. *T1 se i punti di X sono chiusi;*
3. *T2 se presi comunque due punti distinti x, y di X; esistono aperti U_x, U_y di X tali che:*
   - *$x \in U_x$;*
   - *$y \in U_y$;*
   - *$U_x \cap U_y = \emptyset$.*

   Per esprimere il fatto che X ha la proprietà T2 si dice spesso "X è (uno spazio) di Hausdorff".
4. *T3 o "regolare" se è T1 e per ogni $x \in X$ e ogni chiuso F di X che non contiene x, esistono due aperti disgiunti U e V di X tali che $x \in U$ e $F \subseteq V$.*
5. *$T3\frac{1}{2}$ ("ti tre e mezzo") o spazio di Tychonoff se X è T1 e per ogni $x \in X$ e per ogni chiuso F di X non contenente x esiste una funzione continua $f : X \to [0, 1]$ (dove su $[0, 1]$ c'è la topologia indotta da quella usuale su $\mathbb{R}$) che vale 0 in x e 1 in ogni punto di F.*
6. *T4 o normale se è T1 e per ogni due chiusi disgiunti A, B di X esistono due aperti disgiunti U e V di X tali che $A \subseteq U$ e $B \subseteq V$.*

Uno spazio compatto e di Hausdorff è T4 (ed è un po' l'*archetipo* degli spazi T4).

Si ha la catena di implicazioni $T4 \Rightarrow T3\frac{1}{2} \Rightarrow T3 \Rightarrow T2 \Rightarrow T1 \Rightarrow T0$. La prima di queste implicazioni non è per niente banale ed è una conseguenza del seguente risultato, che non dimostreremo.

Teorema 7 (Lemma di Urysohn)**.** *Sia X uno spazio normale, e siano A e B due chiusi disgiunti di X. Allora esiste una funzione continua $f : X \to [0, 1]$ che vale 0 in ogni punto di A e 1 in ogni punto di B. In particolare ogni spazio T4 è $T3\frac{1}{2}$.*

7.3. **Spettro di un anello.** Sia A un anello commutativo unitario. Un ideale proprio $\mathfrak{p}$ di A si dice "primo" se la seguente condizione è soddisfatta: ogni volta che $a, b \in A$ e $ab \in P$ si ha $a \in \mathfrak{p}$ oppure $b \in \mathfrak{p}$. Un altro modo di dirlo è il seguente: il complementare $S = A - \mathfrak{p}$ contiene 1 ed è chiuso per moltiplicazione. Dire che un ideale $\mathfrak{p}$ di A è primo è equivalente a dire che $A/\mathfrak{p}$ è un dominio di integrità (infatti un dominio di integrità non è altro che un anello commutativo unitario A tale che l'ideale (0) è primo). Osserviamo che se M è un ideale massimale di A allora A/M è un campo, in particolare un dominio di integrità. Quindi ogni ideale massimale è primo. Ma il viceversa non vale: per esempio l'ideale nullo (0) di $\mathbb{Z}$ è primo (perché $\mathbb{Z}$ è un dominio di integrità) ma non è massimale (perché $\mathbb{Z}$ non è un campo).

Indichiamo con $\mathrm{Spec}(A)$ l'insieme degli ideali primi di A. Per esempio $\mathrm{Spec}(\mathbb{Z})$ consiste dell'ideale nullo (0), che è primo e non massimale, e degli ideali generati dai numeri primi, (p) con p primo, che sono tutti massimali. Un altro esempio è $\mathrm{Spec}(\mathbb{R}[X])$, che consiste dell'ideale nullo (0), che è primo e non massimale, e degli ideali generati dai polinomi irriducibili, $(P(X))$ con $P(X)$ irriducibile, che sono tutti massimali. Un esempio rilevante è $\mathrm{Spec}(\mathbb{C}[X])$, che consiste dell'ideale nullo (0) e degli ideali generati dai polinomi irriducibili, cioè di grado 1 ($\mathbb{C}$ è algebricamente chiuso), che sono massimali. In altre parole gli ideali massimali di $\mathbb{C}[X]$ sono tutti e soli quelli del tipo $(X-a)$ con $a \in \mathbb{C}$, quindi c'è una corrispondenza biunivoca tra $\mathbb{C}$ e l'insieme degli ideali massimali di $\mathbb{C}[X]$ definita da $a \mapsto (X-a)$.

Dato un ideale I di A, definiamo

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid I \subseteq \mathfrak{p}\}.$$

In particolare $V(A) = \emptyset$ e $V(\{0\}) = \mathrm{Spec}(A)$.

Deduciamo facilmente le seguenti proprietà (qui I, J e gli I_k sono ideali di A, e $\sum_k I_k$ indica l'ideale generato dagli ideali I_k):

$$\bigcap_k V(I_k) = V(\sum_k I_k), \qquad V(I) \cup V(J) = V(I \cap J).$$

La prima di tali proprietà è facile. Quanto alla seconda, è chiaro che se un ideale primo contiene I oppure J allora contiene $I \cap J$. Viceversa, se $\mathfrak{p} \in \mathrm{Spec}(A)$ contiene $I \cap J$ senza contenere né I né J allora se $i \in I - \mathfrak{p}$ e $j \in J - \mathfrak{p}$, da $ij \in I \cap J \subseteq \mathfrak{p}$ segue che $i \in \mathfrak{p}$ oppure $j \in \mathfrak{p}$ ($\mathfrak{p}$ è un ideale primo), assurdo.

Quanto appena esposto dimostra, grazie alla proposizione 1, che la definizione seguente ha senso:

Definition 6 (Topologia di Zariski)**.** *Sia A un anello. La topologia di Zariski su* $\mathrm{Spec}(A)$ *è quella topologia i cui chiusi sono i sottoinsiemi di* $\mathrm{Spec}(A)$ *della forma $V(I)$ dove I è un ideale di A.*

Osserviamo che in questa topologia gli ideali massimali corrispondono ai punti chiusi. Infatti se $\mathfrak{m}$ è un ideale massimale di A allora $V(\mathfrak{m}) = \{\mathfrak{m}\}$ (per definizione).

Per esempio in $\mathrm{Spec}(\mathbb{Z})$ i punti sono tutti chiusi tranne (0), che è l'unico punto denso. In particolare $\mathrm{Spec}(\mathbb{Z})$ è T0.

La topologia di Zariski sarà considerata la topologia "usuale" per lo spettro di un anello. Segue un primo risultato di "buon comportamento".

Teorema 8. *Sia $\varphi : A \to B$ un omomorfismo di anelli commutativi unitari. Sia $f_\varphi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ la funzione definita da $f_\varphi(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p})$. Allora f_φ è una funzione ben definita ed è continua.*

Dimostrazione. Mostriamo che f_φ è ben definita. In altre parole, mostriamo che se $\mathfrak{p}$ è un ideale primo di B allora $I = \varphi^{-1}(\mathfrak{p})$ è un ideale primo di A. Certamente I è un ideale, essendo la controimmagine di un ideale tramite un omomorfismo di anelli. Prendiamo ora $a, b \in A$ con $ab \in I$. In altre parole $\varphi(ab) \in \mathfrak{p}$, cioè $\varphi(a)\varphi(b) \in \mathfrak{p}$ (φ è un omomorfismo). Siccome $\mathfrak{p}$ è un ideale primo $\varphi(a) \in \mathfrak{p}$ oppure $\varphi(b) \in \mathfrak{p}$, in altre parole $a \in \varphi^{-1}(\mathfrak{p})$ oppure $b \in \varphi^{-1}(\mathfrak{p})$.

Scriviamo $X = \mathrm{Spec}(B)$ e $Y = \mathrm{Spec}(A)$. Sia U un aperto di Y, cioè $U = Y - V(I)$ con I ideale di A. Allora $f_\varphi^{-1}(U) = X - f_{\varphi^{-1}}(V(I))$ è un aperto se e solo se $C := f_\varphi^{-1}(V(I))$ è un chiuso. Mostriamo quindi che C è un chiuso. Dobbiamo trovare un ideale J di B tale che $C = V(J)$. Scegliamo come J l'ideale di B generato da $\varphi(I)$ (osserviamo che in generale $\varphi(I)$ non è un ideale di B, per esempio se φ è un'inclusione di A in B come sottoanello allora $\varphi(A) = A$ non è un ideale in generale). Ricordiamo che $C = f_\varphi^{-1}(V(I))$. Mostriamo che $C = V(J)$.

- $C \subseteq V(J)$. Sia $\mathfrak{p} \in C$. Allora $\varphi^{-1}(\mathfrak{p}) = f_\varphi(\mathfrak{p}) \in V(I)$, cioè $\varphi^{-1}(\mathfrak{p})$ contiene I, in altre parole $\varphi(I) \subseteq \mathfrak{p}$. Siccome $\mathfrak{p}$ è un ideale anche l'ideale generato da $\varphi(I)$ è contenuto in $\mathfrak{p}$, cioè $J \subseteq \mathfrak{p}$, cioè $\mathfrak{p} \in V(J)$.
- $V(J) \subseteq C$. Sia $\mathfrak{p} \in V(J)$. Allora $\mathfrak{p}$ contiene J, l'ideale generato da $\varphi(I)$, in particolare $\mathfrak{p}$ contiene $\varphi(I)$, cioè $f_\varphi(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ contiene I, cioè $f_\varphi(\mathfrak{p}) \in V(I)$. Questo dimostra che $\mathfrak{p} \in C$.

Questo dimostra che $C = V(J)$ e conclude la dimostrazione. □

7.4. **Nullstellensatz.** Sia k un anello commutativo unitario, e sia $A = k[X_1, \ldots, X_n]$ l'anello dei polinomi in n indeterminate su k. Definiamo $k^n := \{(a_1, \ldots, a_n) \ : \ a_1, \ldots, a_n \in k\}$. Se $S \subseteq k^n$ definiamo $I(S) := \{f \in A \ : \ f(s) = 0 \ \forall s \in S\}$, l'insieme dei polinomi i cui zeri comprendono tutti gli elementi di S, e se J è un ideale di A definiamo $V(J) := \{z \in k^n \ : \ f(z) = 0 \ \forall f \in J\}$, l'insieme degli zeri comuni a tutti gli elementi di J. Il *Nullstellensatz di Hilbert*, o teorema degli zeri di Hilbert (considerato il punto di contatto tra l'algebra e la geometria) afferma che se k è un campo algebricamente chiuso e J è un qualsiasi ideale di $A = k[X_1, \ldots, X_n]$ allora

$$I(V(J)) = \sqrt{J}$$

dove $\sqrt{J} := \{a \in A \ : \ a^n \in J \ \exists n \in \mathbb{N}\}$. Siccome $\sqrt{J} \supseteq J$, se J è un ideale massimale allora $\sqrt{J} = J$ e otteniamo che $I(V(J)) = J$. In particolare $V(J) \neq \emptyset$ (infatti $I(\emptyset) = A \neq J$) e quindi esiste $P = (a_1, \ldots, a_n) \in V(J)$. In particolare $I(V(J)) = J$ contiene gli elementi $X_1 - a_1, \ldots, X_n - a_n$, quindi contiene l'ideale $(X_1 - a_1, \ldots, X_n - a_n)$, che è massimale e quindi coincide con J. Riassumendo, se k è un campo algebricamente chiuso allora ogni ideale massimale di $k[X_1, \ldots, X_n]$ è del tipo $(X_1 - a_1, \ldots, X_n - a_n)$ con $a_1, \ldots, a_n \in k$ (!). Quindi gli ideali massimali di $k[X_1, \ldots, X_n]$ sono in biiezione con k^n. In geometria algebrica moderna (Grothendieck, 1928 - 2014) i "punti" (oggetto di accese discussioni nel corso dei secoli) e gli ideali massimali sono moralmente la stessa cosa.

Vediamo ora come il Nullstellensatz si traduce nel linguaggio degli spettri. Sia A un anello commutativo unitario e sia $X := \mathrm{Spec}(A)$. Se $S \subseteq A$ definiamo $V(S) := \{\mathfrak{p} \in \mathrm{Spec}(A) \ : \ \mathfrak{p} \supseteq S\}$ e se $Y \subseteq X = \mathrm{Spec}(A)$ definiamo $I(Y) := \bigcap_{\mathfrak{p} \in Y} \mathfrak{p}$. Come sopra, se I è un ideale di A definiamo $\sqrt{I} := \{a \in A \ : \ a^n \in I \ \exists n \in \mathbb{N}\}$.

Teorema 9. $\bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathfrak{p} = \sqrt{(0)}$.

Dimostrazione. $\sqrt{(0)}$ consiste degli elementi nilpotenti di A, cioè degli elementi $a \in A$ tali che $a^n = 0$ per qualche numero naturale $n > 0$.

Sia $S = \{x^n \ : \ n \in \mathbb{N}_{>0}\}$ dove x è un elemento non nilpotente di A, cioè $x^n \neq 0$ per ogni $n \in \mathbb{N}_{>0}$.

Sia $\mathfrak{X}$ la famiglia degli ideali di A disgiunti da S, ordinata per inclusione. Allora $\mathfrak{X} \neq \emptyset$ dato che $(0) \in \mathfrak{X}$. Mostriamo che $\mathfrak{X}$ ha elementi massimali, cioè elementi $M \in \mathfrak{X}$ tali che se $I \in \mathfrak{X}$ e $I \supseteq M$ allora $I = M$. Per farlo usiamo il lemma di Zorn. Dobbiamo quindi mostrare che ogni catena (sottoinsieme totalmente ordinato) di $\mathfrak{X}$ ammette maggioranti in $\mathfrak{X}$. Sia $C = \{I_\lambda\}_{\lambda\in\Lambda}$ una catena in $\mathfrak{X}$, e sia $I := \bigcup_{\lambda\in\Lambda} I_\lambda$. Certamente I è un maggiorante per C, essendo $I_\lambda \subseteq I$ per ogni $\lambda \in \Lambda$ (per definizione di unione). Rimane da dimostrare che $I \in \mathfrak{X}$, e per questo è necessario che I sia un ideale di A.

- 0 appartiene ad I essendo $0 \in I_\lambda$ per ogni $\lambda \in \Lambda$ e quindi anche $0 \in I$.
- Sia $x \in I$ e sia $a \in A$, mostriamo che $ax \in I$. Per definizione di unione siccome $I = \bigcup_\lambda I_\lambda$ esiste $\lambda \in \Lambda$ tale che $x \in I_\lambda$ per cui $ax \in I_\lambda$ essendo I_λ un ideale, quindi anche $ax \in I$ per definizione di unione. In particolare quando $a = -1$ otteniamo che $-x \in I$, cioè I contiene gli inversi additivi dei suoi elementi.
- Siano $x, y \in I$, mostriamo che $x + y \in I$. Siccome $I = \bigcup_{\lambda\in\Lambda} I_\lambda$ per definizione di unione esistono $\lambda, \mu \in \Lambda$ tali che $x \in I_\lambda$ e $y \in I_\mu$. Siccome l'inclusione induce in C un ordine totale (perché C è una catena) si ha $I_\lambda \subseteq I_\mu$ oppure $I_\mu \subseteq I_\lambda$. Nel primo caso $x \in I_\lambda \subseteq I_\mu \ni y$ quindi siccome I_μ è un ideale di A, $x + y \in I_\mu \subseteq I$ e quindi $x + y \in I$. Nel secondo caso $y \in I_\mu \subseteq I_\lambda \ni x$ quindi siccome I_λ è un ideale di A, $x + y \in I_\lambda \subseteq I$ quindi $x + y \in I$.

Per mostrare che $I \in \mathfrak{X}$ ci rimane da verificare che $S \cap I = \emptyset$. Se fosse $S \cap I \neq \emptyset$ allora esisterebbe $a \in S$ con $a \in I = \bigcup_{\lambda\in\Lambda} I_\lambda$, quindi per definizione di unione esiste $\lambda \in \Lambda$ tale che $a \in I_\lambda$ e siccome $a \in S$ questo contraddice il fatto che $I_\lambda \in \mathfrak{X}$.

Sia P un elemento massimale di $\mathfrak{X}$ (abbiamo appena dimostrato che esiste). Mostriamo che è un ideale primo. Dobbiamo cioè mostrare che se $\alpha, \beta \in A$ con $\alpha\beta \in P$ allora almeno uno tra α e β appartiene a P. Supponiamo quindi per assurdo che sia $\alpha\beta \in P$ con $\alpha \notin P$ e $\beta \notin P$. Allora gli ideali $P + (\alpha)$ e $P + (\beta)$ contengono P propriamente, infatti α e β non appartengono a P. Siccome P è un elemento massimale di $\mathfrak{X}$ segue che $P + (\alpha), P + (\beta) \notin \mathfrak{X}$. In altre parole esistono n, m interi positivi con $x^n \in P + (\alpha)$ e $x^m \in P + (\beta)$, cioè esistono $a, c \in P$ e $b, d \in A$ con $x^n = a + \alpha b$, $x^m = c + \beta d$. Allora abbiamo

$$x^{n+m} = x^n x^m = (a + \alpha b)(c + \beta d) = ac + a\beta d + \alpha bc + \alpha\beta bd$$

e questo elemento appartiene a P, infatti $a, c \in P$, $\alpha\beta \in P$ e P è un ideale. Deduciamo che $x^{n+m} \in P$ e questo contraddice il fatto che $P \in \mathfrak{X}$. In conclusione, P è un ideale primo di A.

Sia ora $\mathcal{N} = \sqrt{(0)}$ l'insieme degli elementi nilpotenti di A. Mostriamo che $\mathcal{N}$ è uguale all'intersezione degli ideali primi di A.

- ($\subseteq$). Se $x \in \mathcal{N}$ e I è un ideale primo di A allora esiste un intero positivo n con $x^n = 0 \in I$ e quindi, siccome I è un ideale primo, da $x \cdot x^{n-1} = x^n \in I$ segue $x \in I$ oppure $x^{n-1} \in I$, e per induzione concludiamo che $x \in I$. Quindi x appartiene a tutti gli ideali primi di A, quindi appartiene alla loro intersezione.
- ($\supseteq$). Sia x un elemento di A che appartiene a tutti gli ideali primi di A, e mostriamo che $x \in \mathcal{N}$. Se fosse $x \notin \mathcal{N}$ allora per quanto dimostrato sopra la famiglia $\mathfrak{X} = \{J \trianglelefteq A \ : \ x^n \notin J \ \forall n \in \mathbb{N}_{>0}\}$ ha un elemento massimale P,

che come visto è un ideale primo di A. Siccome $P \in \mathfrak{X}$ si ha $x = x^1 \notin P$ e questo contraddice il fatto che x appartiene a tutti gli ideali primi di A.

□

Teorema 10 (Nullstellensatz di Hilbert)**.** *Sia I un ideale di A. Allora $I(V(I)) = \sqrt{I}$.*

Dimostrazione. $I(V(I))$ consiste degli elementi $a \in A$ che appartengono a tutti gli ideali primi che contengono I, cioè $I(V(I)) = \bigcap_{\mathrm{Spec}(A) \ni \mathfrak{p} \supseteq I} \mathfrak{p}$. Per il teorema di corrispondenza, $I(V(I))$ corrisponde all'intersezione degli ideali primi di A/I, cioè a $\sqrt{(0)}$ dove (0) è l'ideale nullo di A/I, cioè $(0) = I/I$. Di conseguenza $I(V(I)) = \sqrt{I}$. □

7.5. **Spettro massimale.** Facciamo un esempio in cui si vede un po' il senso delle nozioni introdotte. La fonte del materiale che segue è la seguente: [3], pagina 14 (esercizio 26 del capitolo 1, "Rings and Ideals").

Dato un anello commutativo unitario A denoteremo con $\mathrm{Specmax}(A)$ (lo spettro massimale di A) il sottoinsieme di $\mathrm{Spec}(A)$ che consiste degli ideali massimali di A.

Sia X uno spazio topologico compatto e di Hausdorff (per esempio l'intervallo chiuso $[0, 1]$ in $\mathbb{R}$). Sia $C(X)$ l'insieme delle funzioni continue $X \to \mathbb{R}$. Allora $C(X)$ ha le operazioni di somma e prodotto per componenti: se $f, g \in C(X)$ definiamo $f + g$ e $f \cdot g$ tramite le posizioni $(f + g)(x) := f(x) + g(x)$ e $(f \cdot g)(x) := f(x)g(x)$. Con queste operazioni $C(X)$ è un anello commutativo unitario.

Il seguente risultato dimostra che gli spazi compatti e di Hausdorff si possono vedere come spettri massimali con la topologia di Zariski.

Teorema 11. *Sia X uno spazio topologico compatto e di Hausdorff. Per ogni $x \in X$ sia $v_x : C(X) \to \mathbb{R}$ la funzione che manda f in $f(x)$: si tratta di un omomorfismo di anelli. Con le notazioni dette, la funzione*

$$\varphi : X \to \mathrm{Specmax}(C(X))$$
$$x \mapsto \mathfrak{m}_x := \ker(v_x)$$

è ben definita e biiettiva. Inoltre se mettiamo su $\mathrm{Specmax}(C(X))$ *la topologia indotta da quella di Zariski su* $\mathrm{Spec}(C(X))$ *allora φ è un omeomorfismo (cioè è continua, biiettiva e la sua inversa è continua).*

Dimostrazione. φ è ben definita perché per ogni $x \in X$, l'omomorfismo v_x è suriettivo (perché le costanti sono continue) e quindi $C(X)/\mathfrak{m}_x \cong \mathbb{R}$ è un campo (ovvero $\mathfrak{m}_x$ è un ideale massimale di $C(X)$).

L'iniettività segue dal lemma di Urysohn: se $x \neq y$ sono elementi di X allora $\{x\}$ e $\{y\}$ sono chiusi, quindi esiste una funzione continua $f : X \to \mathbb{R}$ tale che $f(x) = 0$ e $f(y) = 1$. Ne segue che $f \in \mathfrak{m}_x - \mathfrak{m}_y$, e quindi $\mathfrak{m}_x \neq \mathfrak{m}_y$.

Proviamo la suriettività. Sia $\mathfrak{m} \in \mathrm{Specmax}(C(X))$, e sia $\Sigma := \bigcap_{f \in \mathfrak{m}} f^{-1}(\{0\})$. Se $x \in \Sigma$ allora $\mathfrak{m} \subseteq \mathfrak{m}_x$, da cui $\mathfrak{m} = \mathfrak{m}_x$ per massimalità di $\mathfrak{m}$. Ne segue che ci basta mostrare che $\Sigma \neq \emptyset$. Poiché X è compatto e Σ è un'intersezione di una famiglia di chiusi (controimmagini del punto chiuso $\{0\}$ tramite funzioni continue), per mostrare che Σ è non vuoto basta mostrare che ogni sottofamiglia finita ha intersezione non vuota. Siano allora $f_1, ..., f_n \in \mathfrak{m}$. Dobbiamo mostrare che esiste

$x \in X$ tale che $f_1(x) = ... = f_n(x) = 0$. Supponiamo che ciò non sia vero, e consideriamo $f := \sum_{i=1}^{n} f_i^2 \in \mathfrak{m}$. Allora dato $x \in X$, si ha $f(x) = 0$ se e solo se $f_1(x) = ... = f_n(x) = 0$, e questo non succede per ipotesi. Ma allora $f \in \mathfrak{m}$ non si annulla mai in X, e di conseguenza è un elemento invertibile di $C(X)$ (il cui inverso è $g(x) := 1/f(x)$, composizione della funzione continua $\alpha \mapsto 1/\alpha$ con f). Ciò significa che $\mathfrak{m}$ è un ideale massimale che contiene un elemento invertibile: assurdo.

Per mostrare che φ è un omeomorfismo basta mostrare che è una funzione continua, in virtù del seguente:

Lemma 4. *Una funzione continua e biiettiva a dominio compatto e codominio di Hausdorff è un omeomorfismo.*

Dimostrazione. Sia allora $f : X \to Y$ una funzione continua e biiettiva, con X compatto. Per mostrare che è un omeomorfismo basta mostrare che la f manda chiusi in chiusi, perché ciò è equivalente a dire che la controimmagine di un chiuso tramite l'inversa è un chiuso. Sia quindi F un chiuso di X. Nel seguito usiamo la proposizione 2. Siccome X è compatto e F è chiuso, F è compatto, e quindi $f(F)$ è compatto essendo la f continua. Un sottospazio compatto di uno spazio di Hausdorff è chiuso e quindi abbiamo finito. □

In effetti, $\mathrm{Specmax}(C(X))$ è di Hausdorff. Per vedere questo mettiamoci nello spazio topologico $S = \mathrm{Spec}(C(X))$ con la topologia di Zariski, dove se $f \in C(X)$ il seguente insieme è un aperto: $D(f) := \{\mathfrak{p} \in S \mid f \notin \mathfrak{p}\} = S - V((f))$. Siano $\mathfrak{m}_x$ e $\mathfrak{m}_y$ due elementi distinti di $\mathrm{Specmax}(C(X))$. Per "separare" $\mathfrak{m}_x$ e $\mathfrak{m}_y$ con degli aperti disgiunti di $\mathrm{Specmax}(C(X))$ troviamo due funzioni continue $f, g : X \to \mathbb{R}$ tali che $x \in D(f)$, $y \in D(g)$ e $D(f) \cap D(g) \cap \mathrm{Specmax}(C(X)) = \emptyset$. In altre parole $f(x) \neq 0$, $g(x) \neq 0$ e non ci sono $z \in X$ tali che $f(z) \neq 0 \neq g(z)$, ovvero $fg = 0$. Per trovare f e g utilizziamo il lemma di Urysohn: separiamo innanzitutto x e y con degli aperti nello spazio di Hausdorff X: siano U e V due aperti disgiunti contenenti rispettivamente x e y. Nel seguito dato $A \subseteq X$ indichiamo con $\overline{A}$ la "chiusura" di A in X, cioè l'intersezione dei chiusi che contengono A; si tratta del "più piccolo" chiuso che contiene A. Poiché X è T4 esistono intorni aperti U', V' di x, y rispettivamente tali che

$$x \in U' \subseteq \overline{U'} \subseteq U, \qquad y \in V' \subseteq \overline{V'} \subseteq V.$$

Scegliamo allora (grazie al lemma di Urysohn) una funzione continua $f : X \to \mathbb{R}$ che vale 1 in $\overline{U'}$ e 0 in $X - U$, e una funzione continua $g : X \to \mathbb{R}$ che vale 1 in $\overline{V'}$ e 0 in $X - V$. Per costruzione $f(x) \neq 0$, $g(y) \neq 0$ e $fg = 0$.

Basta allora mostrare che la φ è continua. Prendiamo un chiuso $V(I) \cap \mathrm{Specmax}(C(X))$ dove $I \trianglelefteq C(X)$. La sua controimmagine tramite φ è

$$\begin{aligned} \{x \in X \mid \mathfrak{m}_x \in V(I)\} &= \{x \in X \mid \mathfrak{m}_x \supseteq I\} \\ &= \{x \in X \ : \ f(x) = 0 \ \forall f \in I\} \\ &= \bigcap_{f \in I} f^{-1}(\{0\}), \end{aligned}$$

che è un chiuso perché le $f \in I$ sono continue, in $\mathbb{R}$ i punti sono chiusi e intersezione arbitraria di chiusi è un chiuso. □

Riferimenti bibliografici

[1] Ram Murty, M. Prime numbers and irreducible polynomials. Amer. Math. Monthly 109 (2002), no. 5, 452-458.
[2] http://www.alpertron.com.ar/ECM.HTM
[3] Atiyah, M. F.; Macdonald, I. G. Introduction to Commutative Algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
[4] Mumford David, Algebraic geometry. I. Complex projective varieties. Reprint of the 1976 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1995.
[5] Hartshorne Robin, Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
[6] Grothendieck, Alexandre; Dieudonné, Jean (1960). Éléments de géométrie algébrique. (EGA)
[7] Grothendieck, Alexandre (1971). Séminaire de Géométrie Algébrique. (SGA)