חוגים

- תחום נורמלי: כל איבר בשדה השברים שמאפס פולינום מתוקן מעל A שייך ל-A
- תחום פריקות יחידה: כל איבר ניתן לכתוב כמכפלה סופית של אי-פריקים, וכל אי-פריק הוא ראשוני
- תחום ראשי: כל אידיאל נוצר על-ידי איבר אחד
- פונקציה אוקלידית: פונקציה מהתחום A ל-$\mathbb{N}$ כך שעבור $a,b\in A$, אם b לא מחלק את a אז יש d עבורו $\alpha(a-db)<\alpha(b)$.
- משפט השאריות הסיני: אם $n_1,\ldots,n_k$ שלמים זרים בזוגות, אז ההעתקה הטבעית מ-$\mathbb{Z}/_{n_1\ldots n_k}$ ל-$\mathbb{Z}/_{n_1}\times\ldots\times\mathbb{Z}/_{n_k}$ היא איזומורפיזם.

חבורות

- משפט לגרנז': אם $H\leqslant G$ חבורות סופיות, אז הסדר של H מחלק את הסדר של G
- אם $f:G\to H$ העתקה של חבורות ו-G סופית, אז $|G|=|Im(f)||Ker(f)|$.
- התמרת פורייה: אם G חילופית וסופית מסדר n, ו-$\Bbbk$ שדה סגור אלגברית ממציין זר ל-n (או 0), אז יש איזומורפיזם $\mathcal{F}:\Bbbk[G]\to\Bbbk^{\check{G}}$ של חוגים שנקבע על-ידי התנאים $\mathcal{F}(g)(\phi)=\chi(g^{-1})$ ו-$\mathcal{F}(a)(\chi)=a$ לכל $g\in G$, $\phi\in\check{G}$ ו-$a\in\Bbbk$ (כאשר $\check{G}=\mathrm{Hom}(G,\Bbbk^\times)$ החבורה הדואלית). ההעתקה ההפוכה נתונה על-ידי $\tilde{\mathcal{F}}(t)=\frac{1}{n}\sum_{g\in G}(\sum_{\chi\in\check{G}}\chi(g)t(\chi))g$

שאריות ריבועיות

- סימן לז'נדר: $\left(\frac{n}{p}\right)=r-1$, כאשר r מספר השורשים הריבועיים של n ב-$\mathbb{F}_p$ (לשלם n וראשוני אי-זוגי p)
- נוסחת אוילר: $\left(\frac{n}{p}\right)=n^{\frac{p-1}{2}}$ ב-$\mathbb{F}_p$ לכל ראשוני אי-זוגי p ומספר שלם n.
- הדדיות ריבועית: $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ אם ורק אם לפחות אחד מהראשוניים p,q הוא מהצורה $4k+1$ (כאשר p,q אי-זוגיים שונים)
- ל-2 יש שורש ב-$\mathbb{F}_p$ אם ורק אם $p=8k\pm1$

צפיפות

- צפיפות דיריכלה: קיימת פונקציה חלקית d על תתי-הקבוצות של קבוצת הראשוניים $\mathbb{P}$, כך ש-$d(\mathbb{P})=1$, אם Q סופית אז $d(Q)=0$ ו-$d(Q_1\cup Q_2)=d(Q_1)+d(Q_2)$ אם Q_1 ו-Q_2 זרות.
- משפט דיריכלה: לקבוצת הראשוניים מהצורה $an+b$, כאשר $a>0$ ו-b זר ל-a, יש צפיפות דיריכלה $\frac{1}{\phi(a)}$.

תבניות ריבועיות

- תבנית $p(x,y)=ax^2+bxy+cy^2$ היא פרימיטיבית אם a,b,c זרים ו-$a>0$
- תבנית p שקולה לתבנית q אם $p=q\circ A$ עבור $A\in\mathrm{SL}_2(\mathbb{Z})$.
- התבנית p היא מצומצמת אם ורק אם $|b|\leqslant a\leqslant c$, ואם אחד מהם שוויון, אז $b\geqslant 0$.
- אם $\tau\in\mathbb{H}$ ו-$A=\left[\begin{smallmatrix} r & s\\ u & v\end{smallmatrix}\right]\in\mathrm{GL}_2(\mathbb{R})$ אז $\Im(A(\tau))=\frac{\det(A)\Im(\tau)}{|u\tau+v|^2}$, כאשר $A(\tau)=\frac{r\tau+s}{u\tau+v}$.
- התחום היסודי: $\{\tau\in\mathbb{H}\mid|\tau|\geqslant1\wedge|\Re(\tau)|\leqslant 1/2\}$