Die Additions- und Multiplikationstabellen sehen also folgendermaßen aus:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Wir sehen, dass das etwas mehr als nur ein Ring ist: Jedes Element (außer dem Nullpolynom) hat ein multiplikatives Inverses! Somit ist $\mathbb{Z}_2/p(x)$ ein Körper mit $2^2 = 4$ Elementen. Dieser Körper $GF(4) = (\{0,1,a,b\}, +, \cdot)$ hat also vier Elemente und die Additions- wie auch Multiplikationstabellen sehen folgendermaßen aus (mit $x \mapsto a$ und $1+x \mapsto b$):

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

Aber nicht für jedes Polynom $p(x)$ ist $\mathbb{F}[x]/p(x)$ ein Körper: Betrachte dazu zum Beispiel die Multiplikationstabelle in $\mathbb{Z}_2[x]/(x^2+1)$:

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0

Was $\mathbb{Z}_2[x]/(x^2+x+1)$ zu einem Körper gemacht hat, ist dass das Polynom $p(x) = x^2+x+1$ ein *irreduzibles Polynom* über dem Körper $\mathbb{Z}_2$ ist, d. h. es gibt keine zwei Polynome $f(x)$ und $g(x)$ von kleinerem Grad mit $p(x) = f(x)g(x)$. Man kann zeigen (wir werden dies nicht tun), dass es für jede Primzahl p und für jede positive natürliche Zahl $n \geq 1$ ein irreduzibles Polynom $p(x)$ vom Grad n über dem Körper $\mathbb{Z}_p$ gibt. Ein solches Polynom kann man wie in dem obigen Beispiel benutzen, um den Galois Körper $GF(p^n)$ zu konstruieren.

5.5 Komplexe Zahlen: Rechnen in der Zahlenebene

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

- Leopold Kronecker

Die letzte Schöpfung des Menschen ist die Menge der sogenannten »komplexen Zahlen«. Diese Zahlen sind aus dem Wunsch entstanden, solche Gleichungen wie $x^2+1=0$ zu lösen. Im Laufe der Jahre hat dies zu der Menge $\mathbb{C}$, bekannt als die Menge der »komplexen Zahlen«, geführt. Diese Menge besteht aus allen geordneten Paaren $z = (a,b)$ der

reellen Zahlen, d. h. aus Punkten in der Ebene $\mathbb{R}^2$. Die reellen Zahlen $a \in \mathbb{R}$ sind dann Punkte von der Form $(a,0)$ mit $a \in \mathbb{R}$ – das sind die Punkte der x-Achse. Die Zahl b ist der *Imaginärteil* von $z = (a,b)$; dieser Teil entspricht der y-Koordinate. Man bezeichnet die Koordinaten von $z = (a,b)$ auch als $\operatorname{Re} z = a$ und $\operatorname{Im} z = b$. Die Summe und das Produkt solcher Paare sind definiert durch

$$(a,b) + (c,d) := (a+c, b+d) \quad \text{und} \quad (a,b) \cdot (c,d) := (ac - bd, ad + bc)\,.$$

Die Summe ist also als eine »ganz normale« komponentenweise Summe der Vektoren in $\mathbb{R}^2$ definiert. Nur das Produkt sieht etwas »magisch« aus. Diese »Magie« wird aber verschwinden, wenn wir das Paar $z = (a,b)$ als die Summe $z = a + bi$ schreiben, wobei $i = \sqrt{-1}$ als eine »neue Zahl« (oder eine Variable) mit der Eigenschaft $i^2 = -1$ verstanden wird. Diese neue »Zahl« entspricht dem Paar $i = (0,1)$ und man nennt sie *imaginäre Einheit*:

$$i^2 = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -1\,.$$

Die Schreibweise als Summe $a + bi$ ist praktisch, da man so die üblichen Rechenregeln für reelle Zahlen benutzen kann. So gilt zum Beispiel

$$(a + bi) \cdot (c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (ad + bc)i\,.$$

Man kann sich leicht überzeugen, dass die Menge $\mathbb{C}$ der komplexen Zahlen einen Körper bezüglich der so definierten Addition und Multiplikation bildet. Das neutrale Element bezüglich der Addition ist $0 = (0,0)$ und das additive Inverse von $z = a + bi$ ist $-z = (-a) + (-b)i$. Das neutrale Element bezüglich der Multiplikation ist $1 = (1,0)$ (wieder eine reelle Zahl!) und das multiplikative Inverse von $z = a + bi$ ist

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\,.$$

(Beachte, dass $a^2 + b^2 \neq 0$ für alle $z \neq 0$ gilt, denn aus $a + bi \neq 0$ folgt $a \neq 0$ oder $b \neq 0$.) Probe:

$$z \cdot z^{-1} = (a + bi) \cdot \Big(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \Big) = \frac{(a + bi) \cdot (a - bi)}{a^2 + b^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1\,.$$

Zur Veranschaulichung der Multiplikation benutzt man die sogenannte *Polarkoordinatendarstellung* der komplexen Zahlen. Eine komplexe Zahl $z = a + ib$, d. h. ein Punkt (a,b) in der Ebene $\mathbb{R}^2$, ist durch Angabe ihres Abstandes zum Nullpunkt

$$|z| = \sqrt{a^2 + b^2}$$

und des Winkels θ, den der Strahl von 0 durch z mit der reellen Achse bildet, eindeutig bestimmt (Bild 5.2). Man nennt $|z|, \theta$ die *Polarkoordinaten* von z. Der Winkel θ heißt das *Argument* von z, $\theta = \arg(z)$; es ist bis auf ganzzahlige Vielfache von 2π eindeutig bestimmt. Die (reelle!) Zahl $|z|$ heißt der *Betrag* von z. Durch geometrische Definition des Kosinus und Sinus ergibt sich $a = |z| \cos\theta$ sowie $b = |z| \sin\theta$ (Bild 5.2). Damit ergibt

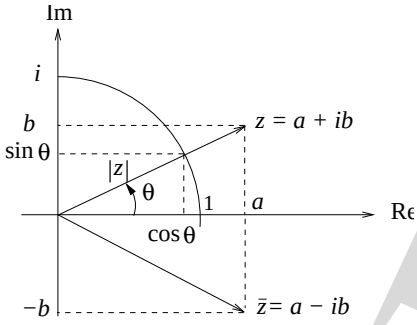

Bild 5.2: Polarkoordinatendarstellung von $z = a + bi$.

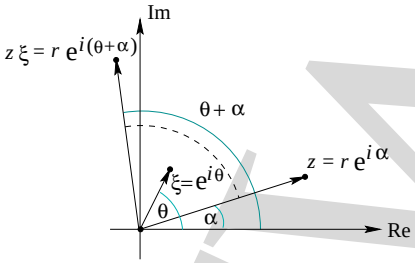

Bild 5.3: Eine Multiplikation mit $\xi = \mathrm{e}^{i\theta}$, $|\xi| = 1$, bewirkt eine Drehung um den Winkel θ. Eine Multiplikation mit einer komplexen Zahl ist also eine Drehstreckung.

sich für z die Darstellung

$$z = a + ib = |z|(\cos\theta + i\sin\theta)\,.$$

Wenn man i als eine »Zahl« mit der Eigenschaft $i^2 = -1$ betrachtet, dann kann man komplexe Zahlen auch in der *Euler'schen Form* darstellen (wir werden dies in Abschnitt 10.4 beweisen, siehe Beispiel 10.24):

$$\cos\theta + i\sin\theta = \mathrm{e}^{i\theta}\,.$$

Zusammen mit der sogenannten Formel von Moivre (siehe Aufgabe 5.17)

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

folgt daraus, dass für die komplexe Funktion e^z die gleichen Potenzrechenregeln wie im Reellen gelten. Um zwei komplexe Zahlen $z_1 = r_1 \cdot e^{i\theta_1}$ und $z_2 = r_2 \cdot e^{i\theta_2}$ in Polarkoordinatendarstellung zu multiplizieren, reicht es also, das Produkt der Längen zu bilden und die Winkel zu addieren (siehe Bild 5.3): $z_1 \cdot z_2 = r_1 r_2 \cdot e^{i(\theta_1+\theta_2)}$. Die Division ist auch einfach: $z_1/z_2 = (r_1/r_2)e^{i(\theta_1-\theta_2)}$.

Wir fassen nun die verschiedenen Darstellungen der komplexen Zahlen zusammen. Ist z eine komplexe Zahl mit dem Realteil a, dem Imaginärteil b, sowie Argument $\arg(z) = \theta$

und Betrag $|z| = \sqrt{a^2 + b^2}$, so gilt

$$\begin{aligned} z &= (a, b) && \text{Cartesische Form} \\ &= a + bi && \text{mit } i^2 = -1 \\ &= |z|(\cos\theta + i\sin\theta) && \text{Polardarstellung} \\ &= |z|\mathrm{e}^{i\theta} && \text{Euler'sche Form}\,. \end{aligned}$$

Zwei komplexe Zahlen $z = a + bi$ und $\overline{z} = a - bi$, die sich nur im Vorzeichen des Imaginärteils unterscheiden, werden als *konjugiert* komplex bezeichnet. Die konjugierte Zahl entspricht einer Spiegelung ihres Gegenstücks an der reellen Achse (siehe Bild 5.2).

Für die Konjugation gelten die folgenden Regeln.

Lemma 5.29:

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
2. $\overline{-z} = -\overline{z}$.
3. $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$.
4. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
5. $\overline{(1/z)} = 1/\overline{z}$.
6. $\overline{(z_1/z_2)} = \overline{z_1}/\overline{z_2}$.
7. z ist eine reelle Zahl genau dann, wenn $\overline{z} = z$ gilt.
8. Ist $z = a + bi$, so gilt
$$a = \frac{z + \overline{z}}{2}, \quad b = \frac{z - \overline{z}}{2i}\,.$$
9. Ist $z = a + bi$, so gilt $z \cdot \overline{z} = |z|^2$.
10. Division: Für $x, z \in \mathbb{C}$ mit $z \neq 0$ gilt
$$\frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{\overline{z}}{|z|^2} \quad \text{und} \quad \frac{x}{z} = \frac{x \cdot \overline{z}}{z \cdot \overline{z}} = \frac{x \cdot \overline{z}}{|z|^2}\,.$$

Alle diese Regeln kann man durch einfaches Nachrechnen verifizieren. Zum Beispiel (4): Sind $z_1 = a_1 + b_1 i$ und $z_2 = a_2 + b_2 i$, so gilt (unter Beachtung von $i^2 = -1$)

$$\begin{aligned} \overline{z_1} \cdot \overline{z_2} &= (a_1 - b_1 i) \cdot (a_2 - b_2 i) = a_1 a_2 - a_1 b_2 i - a_2 b_1 i + b_1 b_2 i^2 \\ &= (a_1 a_2 - b_1 b_2) - (a_1 b_2 + a_2 b_1) i = \overline{z_1 \cdot z_2}\,. \end{aligned}$$

Die Haupteigenschaft der komplexen Zahlen ist, dass nun nicht nur die Gleichung $z^2 - 1 = 0$, sondern auch jede Gleichung $f(z) = 0$ für ein *beliebiges* Polynom $f(z)$ stets lösbar ist. Ein Beweis dieses Fundamentalsatzes war schon Gauß bekannt. Der Beweis ist aber nicht einfach und wir verzichten auf ihn.

Satz 5.30: Fundamentalsatz der Algebra

Für jedes nicht konstante Polynom $f(z) = c_0 + c_1 z + \cdots + c_n z^n$ über $\mathbb{C}$ mit $n \geq 1$ und $c_n \neq 0$ gibt es ein $z \in \mathbb{C}$ mit $f(z) = 0$.

Genauer gilt sogar, dass die Anzahl der Nullstellen, wenn sie mit der richtigen Vielfachheit gezählt werden, insgesamt gleich dem Grad des Polynoms ist.

Nach Lemma 5.25 kann man jedes Polynom $f(z)$ in lineare Faktoren $f(z) = c_n(z - w_1)(z - w_2)\cdots(z - w_n)$ zerlegen, wobei alle $w_1, w_2, \ldots, w_n$ Nullstellen von $f(z)$ sind. Sind die Koeffizienten c_i des Polynoms $f(z)$ *reelle* Zahlen, dann kann man das Polynom sogar in lineare $z - a$ und quadratische $z^2 - az + b$ Faktoren zerlegen, wobei nun a, b *reelle* Zahlen sind; solche Faktoren nennt man *reelle Faktoren.*

Satz 5.31: Polynome mit reellen Koeffizienten

Sei $f(z)$ ein nicht-konstantes Polynom mit reellen Koeffizienten.

1. Gilt $f(z) = 0$ für ein $z \in \mathbb{C}$, so gilt auch $f(\overline{z}) = 0$.
2. Man kann $f(z)$ in reelle lineare und reelle quadratische Faktoren zerlegen.

Die erste Behauptung bedeutet, dass nicht-reelle Nullstellen bei Polynomen mit reellen Koeffizienten immer paarweise auftreten, das heißt, die Anzahl der komplexen Nullstellen ist gerade. Daraus kann man auch folgern, dass jedes Polynom mit reellen Koeffizienten und ungeradem Grad eine reelle Nullstelle hat.

Beweis:

(1) Sei $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$ ein Polynom mit reellen Koeffizienten. Dann gilt

$$\begin{aligned} 0 = \overline{0} = \overline{f(z)} &= \overline{a_0} + \overline{a_1 z} + \overline{a_2 z^2} + \cdots + \overline{a_n z^n} \\ &= \overline{a_0} + \overline{a_1}\,\overline{z} + \overline{a_2}\,\overline{z}^2 + \cdots + \overline{a_n}\,\overline{z}^n && \text{Lemma 5.29(4)} \\ &= a_0 + a_1\overline{z} + a_2\overline{z^2} + \cdots + a_n\overline{z^n} && \text{Lemma 5.29(7)} \\ &= f(\overline{z})\,. \end{aligned}$$

(2) Nach Satz 5.30 kann man $f(z)$ in komplexe lineare Faktoren zerlegen. Sei $z - w$ einer dieser Faktoren mit $w \in \mathbb{C} \setminus \mathbb{R}$. Nach Teil (1) muss dann auch $z - \overline{w}$ ein Faktor von $f(z)$ sein. Dann ist aber $(z - w)(z - \overline{w})$ bereits ein *reeller* quadratischer Faktor von $f(z)$:

$$(z - w)(z - \overline{w}) = z^2 - (w + \overline{w})z + w\overline{w} = z^2 - (2\,\mathrm{Re}\,w)z + |w|^2\,. \qquad \square$$

Beispiel 5.32:

Das Polynom $f(z) = z^4 + 1$ besitzt keine reellen Nullstellen, wohl aber komplexe: Die Zerlegung $f(z) = (z^2 - i)(z^2 + i)$ ergibt vier Nullstellen $\pm(1+i)/\sqrt{2}$ und $\pm(1-i)/\sqrt{2}$. D. h. $f(z)$ hat vier komplexe Nullstellen $w, \overline{w}, -w, -\overline{w}$ mit $w = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$. Unter Beachtung von $2 \cdot \mathrm{Re}\,w = 2 \cdot (1/\sqrt{2}) = \sqrt{2}$ und $w \cdot \overline{w} = |w|^2 = \frac{1}{2} + \frac{1}{2} = 1$, ergibt dies eine Zerlegung des Polynoms in reelle quadratische Faktoren:

$$\begin{aligned} z^4 + 1 &= (z - w)(z - \overline{w})(z + w)(z + \overline{w}) \\ &= (z^2 - 2z\,\mathrm{Re}\,w + w\overline{w})(z^2 + 2z\,\mathrm{Re}\,w + w\overline{w}) \\ &= (z^2 - \sqrt{2}z + 1)(z^2 + \sqrt{2}z + 1)\,. \end{aligned}$$

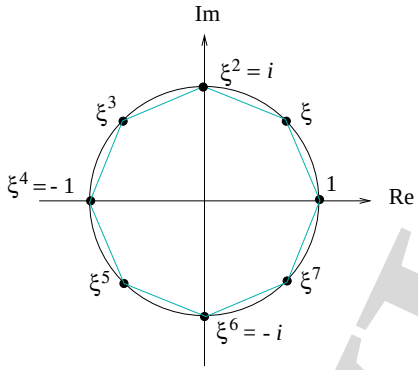

Bild 5.4: Die primitive 8-te Einheitswurzel $\xi = e^{\frac{2\pi i}{8}}$ und ihre Potenzen; $\xi^2 = i$ ist eine 4-te Einheitswurzel.

Beispiel 5.33: Einheitswurzeln

Eine n-te *Einheitswurzel* ist eine Zahl ξ mit $\xi^n = 1$. Die n-ten Einheitswurzel sind also die Nullstellen des Polynoms $x^n - 1$, daher gibt es höchstens n verschiedene. Der Körper $\mathbb{R}$ der reellen Zahlen hat nur ± 1 als Einheitswurzeln, weil aus $x^n = 1$ auch $|x| = 1$ folgt. Anders sieht es für den Körper $\mathbb{C}$ der komplexen Zahlen aus: Hier hat man für jedes $n = 1,2,\ldots$ sogar n verschiedene n-te Einheitswurzeln. Diese kann man mit Hilfe des Euler'schen Satzes leicht bestimmen.

Dazu betrachten wir komplexe Zahlen der Form $z = \mathrm{e}^{2\pi i x}$. Wir suchen zunächst die Lösungen $x \in \mathbb{R}$ der Gleichung $\left(\mathrm{e}^{2\pi i x}\right)^n = 1$. Wir schreiben diese Gleichung als $\mathrm{e}^{i\theta} = 1$ mit $\theta = 2\pi n x$ um. Wegen $\mathrm{e}^{i\theta} = \cos\theta + i\sin\theta$, ist $\mathrm{e}^{i\theta} = 1$ genau dann, wenn $\cos\theta = 1$ und $\sin\theta = 0$ gilt, was genau dann der Fall ist, wenn $\theta \in \{0,2\pi,4\pi,\ldots\}$ gilt. Somit erhalten wir $\left(e^{2\pi i x}\right)^n = 1$ genau dann, wenn x eine der Zahlen $0, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots$ ist. Beschränkt man sich auf $x \in [0,1)$, so bekommt man eine Umrundung des Einheitskreises (siehe Bild 5.4) mit den Werten $x = 0, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}$. Damit sind die Zahlen $1, \xi, \xi^2, \ldots, \xi^{n-1}$ mit

$$\xi := \mathrm{e}^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

n-te Einheitswurzeln; man nennt sie *primitive n-te Einheitswurzeln.* Die n-ten Einheitswurzeln bilden in der Zahlenebene die Ecken eines gleichmäßigen n-Ecks mit Radius 1 (siehe Bild 5.4). Die Einheitswurzeln benutzt man zum Beispiel, um zwei Polynome vom Grad n mit $n\log_2 n$ (statt n^2) arithmetischen Operationen zu multiplizieren (die sogenannte »schnelle Fourier Transformation«). Dabei spielt die folgende Eigenschaft eine entscheidende Rolle: Ist ξ eine primitive n-te Einheitswurzel (n gerade), so ist ξ^2 eine primitive $(n/2)$-te Einheitswurzel: $(\xi^2)^{n/2} = \xi^n = 1$. D. h. das Quadrieren halbiert die Anzahl der Einheitswurzeln (Bild 5.4).

5.5.1 Anwendung: Schnelle Fourier Transformation*

Gegeben ist eine unbekannte Funktion $f : \mathbb{C} \to \mathbb{C}$. Wir wissen nur, dass es sich um ein Polynom vom Grad $n-1$ handelt, also $f(z) = \sum_{i=0}^{n-1} c_i z^i$, wobei uns die Koeffizienten

c_i unbekannt sind. Unser Ziel ist, die Funktion $f(z)$ möglichst schnell zu rekonstruieren. Dabei können wir o. B. d. A. annehmen, dass n gerade ist: Wir dürfen ja Glieder $c_i x^i$ mit $c_i = 0$ zu der Summe beliebig hinzufügen.

Da der Grad des Polynoms $f(z)$ kleiner als n ist, kann es höchstens $n-1$ *verschiedene* Nullstellen haben. Somit ist das Polynom $f(z)$ durch seine Werte $f(a_1), \ldots, f(a_n)$ an n beliebigen *verschiedenen* Punkten $a_1, \ldots, a_n \in \mathbb{C}$ *eindeutig* bestimmt. Würde nämlich ein anderes Polynom $g(z)$ vom Grad $n-1$ mit $g(a_i) = f(a_i)$ für alle $i = 1, \ldots, n$ geben, so hätte das Polynom $h(z) = f(z) - g(z)$ mindestens n verschiedene Nullstellen $a_1, \ldots, a_n$. Da aber der Grad des Polynoms $h(z)$ kleiner als n ist, hätten wir somit einen Widerspruch mit Korollar 5.26.

Es ist klar, dass ungefähr n^2 Operationen für die Auswertung des Polynoms $f(z)$ an n Punkten ausreichen. Die sogenannte *schnelle Fourier-Transformation* kommt aber mit ungefähr $n \log_2 n$ Operationen vollkom aus! Diese (in vielen Algorithmen implementierte) Transformation beruht auf zwei Ideen.

Die erste Idee ist, den Wert eines Polynoms $f(z) = \sum_{i=0}^{m} c_i z^i$ vom Grad m (m sei gerade) in einem Punkt a durch die Werte zweier Polynome vom Grad höchstens $m/2$ im Punkt a^2 auszudrücken:

$$f(z) = f_{\text{even}}(z^2) + z \cdot f_{\text{odd}}(z^2)$$

mit

$$\begin{aligned} f_{\text{even}}(z) &= c_0 + c_2 z + c_4 z^2 + c_6 z^3 + \cdots + c_{2k} z^k + \cdots + c_m z^{m/2}\,, \\ f_{\text{odd}}(z) &= c_1 + c_3 z + c_5 z^2 + c_7 z^3 + \cdots + c_{2k+1} z^k + \cdots + c_{m-1} z^{\lfloor (m-1)/2 \rfloor}\,. \end{aligned}$$

Beispiel 5.34:
Sei $f(z) = a_0 + c_1 z + c_2 z^2 + c_3 z^3 + c_4 z^4 + c_5 z^5 + c_6 z^6$. Dann gilt

$$\begin{aligned} f_{\text{even}}(z) &= c_0 + c_2 z + c_4 z^2 + c_6 z^3\,, \\ f_{\text{odd}}(z) &= c_1 + c_3 z + c_5 z^2\,, \\ f_{\text{even}}(z^2) + z \cdot f_{\text{odd}}(z^2) &= c_0 + c_2 z^2 + c_4 z^4 + c_6 z^6 \\ &\quad + z(c_1 + c_3 z^2 + c_5 z^4) = f(z)\,. \end{aligned}$$

Die zweite Idee ist, die Auswertungspunkte $a_1, \ldots, a_n$ sehr spezifisch auszuwählen. Man betrachtet nämlich als Auswertungspunkte die Potenzen $1, \xi, \xi^2, \ldots, \xi^{n-1}$ der n-ten Einheitswurzel $\xi = \mathrm{e}^{\frac{2\pi i}{n}}$; wir nehmen hier an, dass n eine gerade Zahl ist. Der große Vorteil dieser Auswahl ist, dass das Quadrat ξ^2 eine $(n/2)$-te Einheitwurzel ist:

$$\xi^2 = (\mathrm{e}^{\frac{2\pi i}{n}})^2 = \mathrm{e}^{\frac{2\pi i}{(n/2)}}\,.$$

Will man nun das Polynom $f(z)$ an n Potenzen der n-ten Einheitswurzel ξ auswerten, so reicht es, die Polynome $f_{\text{even}}(z)$ und $f_{\text{odd}}(z)$ auf $n/2$ Potenzen der $(n/2)$-ten Einheitswurzel $\zeta = \xi^2$ auszuwerten:

$$f(\xi^i) = f_{\text{even}}(\zeta^i) + \xi^i \cdot f_{\text{odd}}(\zeta^i), \qquad i = 0{,}1, \ldots, n/2 - 1\,. \tag{5.1}$$

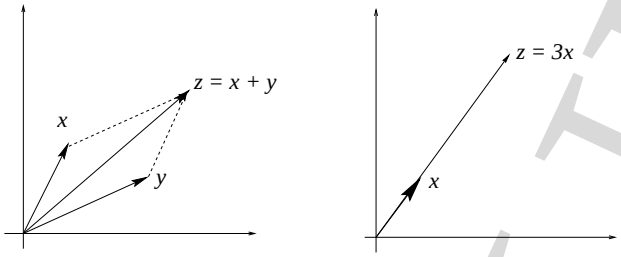

Bild 5.5: Zwei lineare Operationen mit Vektoren.

D. h. anstatt ein Polynom des Grades $n-1$ auf n Punkten $1, \xi, \xi^2, \ldots, \xi^{n-1}$ auszuwerten, reicht es zwei Polynome des Grades $n/2-1$ auf $n/2$ Punkten $1, \zeta, \zeta^2, \ldots, \zeta^{n/2-1}$ auszuwerten. Somit halbiert sich in jedem Schritt der Grad der Polynome sowie die Anzahl der Auswertungspunkte. Dabei braucht man zusätzlich in jedem Schritt nur eine lineare Anzahl cn der Operationen, um die Ausdrücke (5.1) auszurechnen.

Sei nun $T(n)$ die Anzahl der arithmetischen Operationen, die man für die Berechnung der schnellen Fourier-Transformation für ein Polynom vom Grad n benötigt. Da sich der Grad der Polynome in jedem Schritt halbiert, gilt $T(n) \leq 2 \cdot T(n/2) + cn$. Durch Einsetzen $n \to n/2 \to n/2^2 \to \cdots \to n/2^k$ bis $k = \log_2 n$ erhalten wir wegen $T(n/2^k) = T(1) \leq c$

$$T(n) \leq 2T(n/2) + cn \leq 2^2 T(n/2^2) + 2cn/2 + cn \leq \ldots \leq (2^k + kn)c = cn \log_2(2n)\,.$$

5.6 Lineare Räume

Sei $\mathbb{F}$ ein endlicher oder unendlicher Körper. Ein Vektor $\boldsymbol{u} \in \mathbb{F}^n$ ist eine endliche Folge $\boldsymbol{u} = (u_1, \ldots, u_n)$ von nicht unbedingt verschiedenen Zahlen $u_i \in \mathbb{F}$. Vektoren kann man komponentenweise addieren

$$\boldsymbol{u} + \boldsymbol{v} = (u_1 + v_1, \ldots, u_n + v_n)$$

und mit einer Zahl (oder Skalar) $\lambda \in \mathbb{F}$ multiplizieren

$$\lambda \boldsymbol{u} = (\lambda u_1, \ldots, \lambda u_n)\,.$$

Betrachtet man Vektoren in $\mathbb{R}^2$ als aus dem Punkt (0,0) ausgehende Pfeile, so kann man diese beiden Operationen wie im Bild 5.5 veranschaulichen.

Nicht jede Teilmenge von Vektoren in $\mathbb{F}^n$ ist unter diesen zwei Operationen abgeschlossen. Abgeschlossene Teilmengen heißen *Vektorräume*.

Definition: Vektorraum

Eine Teilmenge $V \subseteq \mathbb{F}^n$ ist ein *Vektorraum* über dem Körper $\mathbb{F}$, falls Folgendes gilt:

1. Aus $\boldsymbol{u} \in V$ und $\lambda \in \mathbb{F}$ folgt $\lambda \boldsymbol{u} \in V$.
2. Aus $\boldsymbol{u}, \boldsymbol{v} \in V$ folgt $\boldsymbol{u} + \boldsymbol{v} \in V$.

Da V nach (2) unter der Addition abgeschlossen ist, bildet $(V, +, \mathbf{0})$ eine (additive) abelsche Gruppe, wobei der Nullvektor $\mathbf{0} = (0, \ldots, 0)$ das neutrale Element ist. Man kann