Föreläsningsanteckningar
Algebra II - VT2022

Elin Persson Westin

elin.persson.westin@math.uu.se

Innehåll

1 Introduktion; heltal, delbarhet, primtal

1.1 Introduktion

Det här är en första kurs i *abstrakt algebra*, vilket jag tycker om att förklara som studier av "egenskaper" istället för konkreta objekt (så som heltal, reella eller komplexa tal etc.). Exempel på sådana egenskaper kan vara kommutativitet, existens av (multiplikativa) inverser osv. Det vi kommer fokusera på i den här kursen är något som kallas för *ringar*. Vi har helt enkelt listat ett antal egenskaper vi tycker verkar vara bra att ha, och allt som uppfyller detta kallar vi för en ring.

Första delen av kursen kommer handla om talteori, alltså om heltal och dess egenskaper. Målet kommer vara att kunna förstå hur RSA-kryptering fungerar. Den andra delen av kursen handlar om ringar, deras egenskaper och olika typer av ringar. Den tredje delen handlar fortfarande om ringar, men nu tittar vi på speciella avbildningar mellan ringar som bevarar vissa "strukturer". Vi ställer oss också frågan om när vi vill säga att två ringar är "i princip samma"? Den fjärde delen handlar om ett sätt att skapa nya ringar genom att "identifiera" vissa ringelement med varandra. Den femte och sista delen handlar om ett speciellt exempel av en ring. Det är de så kallade Gaussiska heltalen som vi ska titta extra noga på.

1.2 Delbarhet

Definition 1.1. Om a och b är heltal sägs b vara *delbart* med a om det finns ett heltal x så att $ax = b$. Vi kan också säga att "b är en multipel av a" eller att "a delar b". Vi skriver $a|b$.

Exempel 1.2. 18 har delarna $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$. ± 1 och ± 18 kallas för *triviala delare*, $\pm 2, \pm 3, \pm 6$ och ± 9 kallas för *äkta delare*.

Definition 1.3. Ett heltal > 1 kallas för *primtal* om det bara har triviala delare, och annars kallas det för *sammansatt*.

En speciell egenskap hos primtal är följande:

Sats 1.4. Låt p vara ett primtal. Om $p|ab$ så gäller $p|a$ eller $p|b$.

Nedan följer några användbara delbarhetsregler som gäller för godtyckliga heltal.

Sats 1.5 (Delbarhetsregler)**.** Låt a, b, c vara heltal.

1. Om $a|b$ och $b \neq 0$, så följer det att $|a| \leq |b|$.
2. Om $a|b$, så följer det att $a|bc$.
3. Om $a|b$ och $b|c$ så följer det att $a|c$.
4. Om $c|a$ och $c|b$ så följer det att $c|(ax + by)$ för godtyckliga heltal x och y.
5. Om $a|b$ och $b|a$ så följer det att $a = \pm b$.
6. Om $c \neq 0$ så gäller $a|b$ om och endast om $ac|bc$.

Kom ihåg denna viktiga sats från Algebra I:

Sats 1.6 (Divisionsalgoritmen)**.** Givet heltal a och b, med $a > 0$, så finns det två entydigt bestämda heltal q och r sådana att $b = aq + r$ och $0 \leq r < a$. Talen q och r kallas kvot respektive rest då b divideras med a.

Det betyder att $a|b$ om och endast om $r = 0$ i divisionsalgoritmen!

Definition 1.7. Låt $\text{mgm}(a, b)$ beteckna *minsta gemensamma multipeln* av två heltal a och b. I kompendiet av Hedén och Björklund betecknas detta med $[a, b]$.

Låt $\text{sgd}(a, b)$ beteckna *största gemensamma delaren* av två heltal a och b. I kompendiet av Hedén och Björklund betecknas detta med (a, b).

Vi säger att två nollskilda tal a, b är *relativt prima* om $\text{sgd}(a, b) = 1$.

Exempel 1.8. Vi vill hitta största gemensamma delaren av 18 och 12. Talet 18 har delarna $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$ och 12 har delarna $\{\pm 1, \pm 2, \pm 3, \pm 4 \pm 6, \pm 12\}$. Så den största gemensamma delaren är 6.

Vi kan även använda oss av Euklides algoritm från Algebra I för att beräkna $\text{sgd}(18, 12)$:

$$18 = 1 \cdot 12 + 6$$
$$12 = 2 \cdot 6 + 0$$

Den största icke-försvinnande resten är 6, och därför är $\text{sgd}(18, 12) = 6$.

I Euklides algoritm använder vi oss av följande sats:

Sats 1.9. Låt $a, b \in \mathbb{Z}$. Då gäller $\text{sgd}(a, b) = \text{sgd}(a - nb, b)$ för $n \in \mathbb{Z}$.

Här kommer några väldigt användbara satser som handlar om delbarhet och tal som är relativt prima.

Sats 1.10. Om $\text{sgd}(a, b) = 1$, och $a|bc$, så följer det att $a|c$.

Sats 1.11. Om $\text{sgd}(a, b) = 1$ och $a|c$ samt $b|c$, så följer det att $ab|c$.

Sats 1.12. Om $\text{sgd}(a, b) = 1 = \text{sgd}(a, c)$, så följer det att $\text{sgd}(a, bc) = 1$.

Sats 1.13. Om a och b är icke-negativa heltal, så har vi

$$\text{sgd}(a, b)\,\text{mgm}(a, b) = ab.$$

1.3 Ideal av heltal

Nu ska vi prata om *ideal*, vilket är något vi kommer prata mer generellt om senare i kursen.

Definition 1.14. En mängd A av heltal kallas för ett *ideal* om följande gäller:

1. $A \neq \emptyset$ (Icke-tom),

2. $x, y \in A \Rightarrow x + y \in A$ (Sluten under addition),

3. $x \in A, n \in \mathbb{Z} \Rightarrow nx \in A$ (Sluten under multiplikation med heltal).

Exempel 1.15. 1. $\{0\}$ är ett ideal.

2. $\mathbb{Z}$ är ett ideal.

3. Alla jämna tal är ett ideal. Dessa kan skrivas som $\{2n \mid n \in \mathbb{Z}\}$. Vi säger att idealet *genereras* av talet 2 och skriver $2\mathbb{Z}$.

4. $g\mathbb{Z} = \{g \cdot n \mid n \in \mathbb{Z}\}$ är ett ideal för alla $g \in \mathbb{Z}$.

Proposition 1.16. För varje ideal A, finns ett entydigt icke-negativt heltal g så att $A = g\mathbb{Z}$. Generatorn g karakteriseras av att vara det minsta positiva heltalet som ingår i A, eller så är $g = 0$.

Bevis. Nollidealet $\{0\} = 0\mathbb{Z}$ är på rätt form, så vi kan nu anta att A inte är nollidealet. Det måste då finnas minst ett positivt tal i idealet. Vi vet nämligen att det finns ett $a \neq 0$ i A. Om detta tal inte är positivt så är $-a$ det, och $-1 \cdot a$ ligger också i A enligt egenskap 3. Alltså finns minst ett positivt tal i A.

Så låt nu g vara det minsta positiva talet i A. Eftersom att det för varje $n \in \mathbb{Z}$ gäller att $ng \in A$ så följer det att $g\mathbb{Z} \subseteq A$. Låt nu x vara ett godtyckligt tal i A. Då kan vi skriva $x = qg + r$ där q, r är heltal och $0 \leq r < g$ enligt Divisionsalgoritmen. Eftersom att $g \in A$ och $-q$ är ett heltal så måste $-qg \in A$. Detta betyder att $r = x + (-qg)$ också ligger i A. Men eftersom $0 \leq r < g$ och g är det minsta positiva talet i A måste $r = 0$. Alltså ligger $x = qg$ i $g\mathbb{Z}$. Detta visar att $A \subseteq g\mathbb{Z}$. De två inklusionerna implicerar att $A = g\mathbb{Z}$. □

Övning 1.17. Om vi har två ideal A och B, är då $A \cup B$ ett ideal? Är $A \cap B$ ett ideal?

Lösning. Vi börjar med att fundera på om $A \cap B$ är ett ideal. Antag att $x, y \in A \cap B$ och $r \in \mathbb{Z}$. Eftersom A är ett ideal så ligger $x + y$ och rx i A, och eftersom B är ett ideal så ligger $x + y$ och rx även i B. Alltså ligger både $x + y$ och rx i $A \cap B$. Talet 0 ligger i båda idealen, så deras snitt är icke-tomt. Alltså är $A \cap B$ ett ideal.

Vi tittar på ett exempel: Låt $A = 4\mathbb{Z}$ och $B = 6\mathbb{Z}$. Vi ser att alla tal som ligger i $A \cap B$ måste vara en multipel av både 4 och 6. Generatorn av idealet är alltså $\text{mgm}(4, 6) = 12$. Allmänt gäller:

$$a\mathbb{Z} \cap b\mathbb{Z} = \text{mgm}(a, b)\mathbb{Z}.$$

Hur är det då med $A \cup B$? Låt $A = 4\mathbb{Z}$ och $B = 6\mathbb{Z}$. Uppenbarligen ligger 4 och 6 i $A \cup B$, men $4 + 6 = 10$ ligger inte i något av idealen, och därför inte heller i deras union. Så $A \cup B$ är inte (nödvändigtvis) ett ideal!

Men! Kan vi lägga till fler tal till $A \cup B$ så att vi får ett ideal? Vi ser att vi måste lägga till alla element på formen $4x + 6y$ eftersom element i A är på formen $4x$ och element i B är på formen $6y$. Är detta tillräckligt? Låt $J = \{4x + 6y \mid x, y \in \mathbb{Z}\}$. Genom att sätta x resp. y lika med 0 ser vi att $A \cup B$ ligger i J, och framförallt så är J icke-tomt (eftersom A och B är icke-tomma). Låt x, x', y, y' och m vara heltal.

$$(4x + 6y) + (4x' + 6y') = 4(x + x') + 6(y + y') \in J$$

$$m(4x + 6y) = 4(mx) + 6(my) \in J$$

Detta visar att J faktiskt är ett ideal!

Proposition 1.18. Givet två heltal a och b så genereras idealet

$$\{ax + by \mid x, y \in \mathbb{Z}\}$$

av $g = \text{sgd}(a, b)$.

För att bevisa detta kan vi tänka tillbaka på Algebra I: $ax + by = n$ har en lösning om och endast om $\text{sgd}(a, b)|n$.

2 Kongruenser och Eulers φ-funktion

2.1 Kongruenser

I det här avsnittet ska vi titta mer på kongruenser, vilket ni känner igen från Algebra I. Vi kommer gå igenom knep för att beräkna kongruenser och även titta närmare på primtal och kongruenser.

Definition 2.1. Låt m vara ett positivt heltal. Om $m|(a-b)$ så säger vi att a *är kongruent med* b *modulo* m, och skriver $a \equiv b \pmod{m}$. I annat fall säger vi att a och b *inte* är kongruenta modulo m, och skriver då istället $a \not\equiv b \pmod{m}$.

Anmärkning 2.2. Eftersom 1 delar alla heltal så är alla tal kongruenta modulo 1. Detta är alltså inte ett särskilt intressant fall.

Sats 2.3. Låt a, b vara heltal och m ett positivt heltal. Då gäller $a \equiv b \pmod{m}$ om och endast om a och b ger samma rest vid division med m.

Bevis. Antag först att a och b ger samma rest vid division med m. Enligt Divisionsalgoritmen kan vi skriva a och b på följande sätt:

$$a = mx + r$$

$$b = my + r$$

Vi kan använda detta för att visa att $m|(a-b)$:

$$a - b = (mx + r) - (my + r) = m(x - y),$$

vilket är ekvivalent med att $a \equiv b \pmod{m}$.

Om vi istället antar att $a \equiv b \pmod{m}$ och skriver upp Divisionsalgoritmen för a och b med m som kvot så får vi:

$$a = mx + r$$

$$b = my + s$$

där $0 \leq r, s < m$. Detta ger oss följande ekvivalenser:

$$m|(a-b) \Leftrightarrow m|(m(x-y) + (r-s)) \Leftrightarrow m|(r-s).$$

Om $(r-s) \neq 0$ så måste $|m| \leq |r-s|$, annars kan m omöjligen dela $r-s$ enligt Sats 1.5. Men eftersom $0 \leq r, s < m$ så får vi att $-m < r - s < m$, d.v.s. $|r-s| < |m|$ vilket är en motsägelse. Alltså måste $r - s = 0 \Leftrightarrow r = s$. Det vi alltså har kommit fram till är att om $a \equiv b \pmod{m}$ så ger a och b samma rest vid division med m. □

Proposition 2.4. Kongruens modulo m är en ekvivalensrelation, d.v.s.:

1. $a \equiv a \pmod{m}$ för alla $a \in \mathbb{Z}$.

2. Om $a \equiv b \pmod{m}$, så gäller även $b \equiv a \pmod{m}$.

3. Om $a \equiv b \pmod{m}$ och $b \equiv c \pmod{m}$, så gäller även $a \equiv c \pmod{m}$.

Bevis. 1. $a \equiv a \pmod{m} \Leftrightarrow m|(a-a)$, vilket alltid är sant ty $m \cdot 0 = 0 = a - a$.

2.

$$\begin{aligned} a \equiv b \pmod{m} &\Leftrightarrow \exists x \in \mathbb{Z} : (a-b) = mx \\ &\Leftrightarrow \exists y = -x \in \mathbb{Z} : (b-a) = m(-x) = my \\ &\Leftrightarrow b \equiv a \pmod{m}. \end{aligned}$$

3.

$$\begin{aligned} \begin{cases} a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{cases} &\Leftrightarrow \begin{cases} \exists x \in \mathbb{Z} : a = b + mx \\ \exists y \in \mathbb{Z} : b = c + my \end{cases} \\ &\Rightarrow \exists z = x + y \in \mathbb{Z} : a = c + m(x+y) = c + mz \\ &\Leftrightarrow a \equiv c \pmod{m}. \end{aligned}$$

□

Från Algebra I vet vi att detta betyder att vi kan dela upp heltalen i ekvivalensklasser med avseende på relationen "kongruens modulo m". Men eftersom dessa ekvivalensklasser kommer vara mycket viktiga för oss ger vi dem ett speciellt namn, nämligen *restklasser*.

Definition 2.5. Låt a vara ett heltal och m ett positivt heltal. Mängden

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

av heltal kongruenta med a modulo m, kallas för a:s *restklass* modulo m.

Proposition 2.6. Det finns exakt m stycken restklasser modulo m, nämligen

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}.$$

Bevis. Använd Divisionsalgoritmen: Givet m, för varje heltal a så finns det ett *unikt* $0 \leq r \leq m-1$ (och q) så att $a = qm + r$. Vi ser nu att $\overline{a} = \overline{r}$. □

Definition 2.7. Varje mängd $\{x_1, x_2, \ldots, x_m \mid x_i \in \mathbb{Z}\}$ som innehåller exakt en representant för varje restklass modulo m kallas för ett *fullständigt restklassystem*.

Exempel 2.8. • Mängden $\{0, 1, 2, 3, 4\}$ är ett fullständigt restklassystem modulo 5.

• Mängden $\{15, -4, 2, 23, 9\}$ är ett fullständigt restklassystem modulo 5.

Vi har följande räkneregler för kongruenser:

Proposition 2.9. Låt a, b, c och d vara heltal.

1. Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $a + c \equiv b + d \pmod{m}$.

2. Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$, så är $ac \equiv bd \pmod{m}$.

3. Om $a \equiv b \pmod{m}$, så är $a^k \equiv b^k \pmod{m}$ för alla icke-negativa heltal k.

4. Låt $f(x)$ vara ett polynom med heltalskoefficienter. Om $a \equiv b \pmod{m}$, så är $f(a) \equiv f(b) \pmod{m}$.

Vi vill nu hitta en metod för att beräkna $a^N \pmod{m}$ där N är ett STORT positivt heltal. Det som är bra med metoden är att vi endast behöver multiplicera med a samt kvadrera tal, och detta är oftast relativt enkelt! Metoden använder sig upprepade gånger av det faktum att om $a \equiv b \pmod{m}$, så är $a^k \equiv b^k \pmod{m}$ för alla icke-negativa heltal k och att

$$a^k = \begin{cases} (a^{k/2})^2 & \text{om } k \text{ jämn} \\ a \cdot (a^{(k-1)/2})^2 & \text{om } k \text{ udda} \end{cases}$$

Vi visar detta med två exempel:

$$\begin{aligned} \pmod{15}\ 5^{12} &= (5^6)^2 \\ &= ((5^3)^2)^2 \\ &= ((5 \cdot (5)^2)^2)^2 \\ [\text{Här vänder vi och börjar förenkla kongruensen!}] &= ((5 \cdot 25)^2)^2 \\ [25 \equiv 10] &\equiv ((5 \cdot 10)^2)^2 \\ &= ((50)^2)^2 \\ [50 \equiv 5] &\equiv ((5)^2)^2 \\ &= (25)^2 \\ [25 \equiv 10] &\equiv (10)^2 \\ &= 100 \\ [100 = 6 \cdot 15 + 10] &\equiv 10 \end{aligned}$$

Det här sättet att bokföra beräkningarna kan vara lite krångligt när man arbetar med stora potenser. Istället så skriver vi bara ner exponenterna k och beräknar a^k för varje k (börja från den lägsta potensen och jobba dig uppåt):

k	12	6	3	2	1
$5^k \pmod{15}$	10	10	5	10	5

Nu till ett mycket mer komplicerat exempel: $3^{1332} \pmod{122}$:

k	1332	666	333	332	166	83	82	41	40	20	10	5	4	2	1
$3^k \pmod{122}$	9	-3	27	9	-3	27	9	3	1	1	1	-1	81	9	3

För att utföra beräkningarna behöver vi endast följande beräkningar (förutom beräkningar av enklare kvadrater och multiplikationer):

$$81 \cdot 3 = 243 \equiv -1 \pmod{122}$$
$$27^2 = 729 = 122 \cdot 6 - 3 \equiv -3 \pmod{122}.$$

I t.ex. Python finns en inbyggd funktion för att beräkna $a^k \pmod{m}$, nämligen $\text{pow}(a, k, m)$. Denna funktion använder i princip samma algoritm som ovan.

2.2 Kinesiska restsatsen

Detta avsnitt är en repetition från Algebra I, men det är något vi kommer använda oss av senare i kursen.

Lemma 2.10. Låt a, b vara heltal som är relativt prima, och antag att den så kallade diofantiska ekvationen $ax + by = c$ har en heltalslösning $(x, y) = (x_0, y_0)$. Då ges samtliga lösningar av

$$\begin{cases} x = x_0 + nb \\ y = y_0 - na \end{cases} \qquad \text{där } n \in \mathbb{Z}.$$

Kom ihåg att $ax + by = c$ har en lösning om och endast om $\text{sgd}(a, b)|c$.

Korollarium 2.11. Kongruensen $ax \equiv 1 (\text{mod}\, m)$ är lösbar om och endast om $\text{sgd}(a, m) = 1$, och i så fall är dess lösningar parvis kongruenta med varandra modulo m.

Bevis. $ax \equiv 1 \pmod{m}$ har en lösning om och endast om det finns heltal x och n så att $ax + mn = 1$. Denna ekvation har heltalslösningar om och endast om $\text{sgd}(a, m) = 1$. Från föregående lemma vet vi också att om (x_0, n_0) är en lösning så ges samtliga lösningar av

$$\begin{cases} x = x_0 + km \\ n = n_0 - ka \end{cases} \qquad k \in \mathbb{Z}.$$

Att $x = x_0 + km$ för alla lösningar x visar att de är kongruenta med x_0. Transitivitet ger att alla lösningar är parvis kongruenta. □

Sats 2.12 (Kinesiska restsatsen)**.** Systemet av kongruenser

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

där $m_1, m_2, \ldots, m_r$ är parvis relativt prima, har en unik lösning modulo $m_1 m_2 \cdot \ldots \cdot m_r$. Detta betyder att det finns en lösning, och om x_0 och x_1 är två lösningar så är $x_0 \equiv x_1 \pmod{m_1 m_2 \cdot \ldots \cdot m_r}$.

Tänk på den här satsen som att vi vill hitta ett tal x som har resten a_i när vi delar med m_i.

Bevis. Vi börjar med att visa att det finns minst en lösning. Efter det så visar vi att det är en unik lösning modulo $m_1 m_2 \cdot \ldots \cdot m_r$.

Vårt mål är att skriva en lösning x på ett sådant sätt att varje ekvation i systemet kan lösas oberoende! Alltså att den okända variabeln är olika i varje ekvation (just nu har vi samma x i alla ekvationer).

Vi skriver

$$x = b_1 m_2 \cdot \ldots \cdot m_r + m_1 b_2 \cdot \ldots \cdot m_r + \ldots + m_1 m_2 \cdot \ldots \cdot m_{r-1} b_r,$$

alltså en summa där vi i varje term byter ut m_i mot en okänd variabel b_i. Om vi nu sätter in detta istället för x i vårt system av kongruenser ser vi att termer utom den första innehåller en faktor m_1, så dessa är kongruenta med 0 modulo m_1. Liknande händer i resterande kongruenser. Efter förenkling får vi följande:

$$\begin{cases} b_1 m_2 \cdot \ldots \cdot m_r \equiv a_1 \pmod{m_1} \\ m_1 b_2 \cdot \ldots \cdot m_r \equiv a_2 \pmod{m_2} \\ \vdots \\ m_1 m_2 \cdot \ldots \cdot m_{r-1} b_r \equiv a_r \pmod{m_r} \end{cases}$$

När vi gjort detta kan vi visa att vi kan hitta $b_i, i = 1, \ldots, r$, som löser det nya systemet av kongruenser.

Nu har vi r stycken kongruenser som vi kan lösa separat! Om vi kollar på den $i : te$ kongruensen:

$$m_1 \cdot \ldots \cdot b_i \cdot \ldots \cdot m_r \equiv a_i \pmod{m_i}$$

ser vi att denna har en lösning b_i eftersom att $\text{sgd}(m_i, m_j) = 1$ för alla $j \neq i$. När vi löst alla kongruenser och hittat alla b_i så vet vi att vi har en lösning x enligt ovan.

Det sista vi ska göra är att visa att om vi har två lösningar x_0 och x_1 så är dessa kongruenta modulo $m_1 m_2 \cdot \ldots \cdot m_r$. Om både x_0 och x_1 är lösningar så gäller det att för varje i så är de båda kongruenta med a_i modulo m_i. Det betyder att $x_0 \equiv x_1 \pmod{m_i}$, vilket är ekvivalent med att $m_i | (x_0 - x_1)$. Eftersom att alla m_i är parvis relativt prima så får vi enligt Sats 1.11 att $m_1 m_2 \cdot \ldots \cdot m_r | (x_0 - x_1)$, d.v.s. $x_0 \equiv x_1 \pmod{m_1 m_2 \cdot \ldots \cdot m_r}$. □

Exempel 2.13. Vi vill lösa följande system av kongruenser:

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{6} \\ x \equiv 5 \pmod{7} \end{cases}$$

Vi börjar med att kontrollera att $5, 6, 7$ är parvis relativt prima och ansätter sedan en lösning

$$x = b_1 \cdot 6 \cdot 7 + b_2 \cdot 5 \cdot 7 + b_3 \cdot 5 \cdot 6.$$

Beviset till Kinesiska restsatsen säger oss att vi faktiskt kan hitta en lösning på den här formen! Utan den hade vi inte kunnat vara säkra på att x kan skrivas på just det här sättet.

Nu sätter vi in vårt x på den här formen i systemet:

$$\begin{cases} b_1 \cdot 6 \cdot 7 + b_2 \cdot 5 \cdot 7 + b_3 \cdot 5 \cdot 6 \equiv 2 \pmod{5} \\ b_1 \cdot 6 \cdot 7 + b_2 \cdot 5 \cdot 7 + b_3 \cdot 5 \cdot 6 \equiv 4 \pmod{6} \\ b_1 \cdot 6 \cdot 7 + b_2 \cdot 5 \cdot 7 + b_3 \cdot 5 \cdot 6 \equiv 5 \pmod{7} \end{cases} \Leftrightarrow \begin{cases} b_1 \cdot 6 \cdot 7 \equiv 2 \pmod{5} \\ b_2 \cdot 5 \cdot 7 \equiv 4 \pmod{6} \\ b_3 \cdot 5 \cdot 6 \equiv 5 \pmod{7} \end{cases}$$

Vi löser nu en kongruens i taget:

$$\begin{aligned} & 2 \equiv b_1 \cdot 6 \cdot 7 \equiv b_1 \cdot 1 \cdot 2 \pmod{5} \\ \Rightarrow\ & b_1 \equiv 1 \pmod{5} \\ \Rightarrow\ & \text{Vi kan välja } b_1 = 1. \end{aligned}$$

$$
\begin{aligned}
&4 \equiv b_2 \cdot 5 \cdot 7 \equiv b_2 \cdot (-1) \cdot 1 \pmod 6 \\
\Rightarrow\ &b_2 \equiv -4 \equiv 2 \pmod 6 \\
\Rightarrow\ &\text{Vi kan välja } b_2 = 2 \\
&\quad \text{(Vi hade även kunnat välja } b_2 = -4).
\end{aligned}
$$

$$
\begin{aligned}
&5 \equiv b_3 \cdot 5 \cdot 6 \equiv b_3 \cdot 5 \cdot -1 \pmod 7 \\
\Rightarrow\ &b_3 \equiv -1 \pmod 7 \\
\Rightarrow\ &\text{Vi kan välja } b_3 = -1 \\
&\quad \text{(Vi hade även kunnat välja } b_3 = 6).
\end{aligned}
$$

Vi har nu hittat värdet på b_1, b_2, b_3 som löser kongruenserna. Vi sätter in detta i ekvationen för x och får:

$$
\begin{aligned}
x &= b_1 \cdot 6 \cdot 7 + b_2 \cdot 5 \cdot 7 + b_3 \cdot 5 \cdot 6 \\
&= 1 \cdot 6 \cdot 7 + 2 \cdot 5 \cdot 7 + (-1) \cdot 5 \cdot 6 \\
&= 82
\end{aligned}
$$

För att vara på den säkra sidan sätter vi in $x = 82$ i systemet av kongruenser:

$$
\begin{cases}
82 = 80 + 2 \equiv 2 \pmod 5 \\
82 = 60 + 22 = 60 + 18 + 4 \equiv 4 \pmod 6 \\
82 = 77 + 5 \equiv 5 \pmod 7
\end{cases}
$$

Det stämde! Vi vet nu att samtliga lösningar till systemet är $x = 82 + 210n$. (Obs: $5 \cdot 6 \cdot 7 = 210$)

2.3 Eulers φ-funktion

Lemma 2.14. Om a och b tillhör samma restklass modulo m, så gäller $\text{sgd}(a, m) = \text{sgd}(b, m)$.

Bevis. Detta följer direkt från Sats 1.9 eftersom att $a = b + qm$ för något heltal q, och då gäller $\text{sgd}(a, m) = \text{sgd}(b + qm, m) = \text{sgd}(b, m)$. □

Nu när vi vet detta så kan vi definiera följande:

Definition 2.15. En restklass $\overline{a}$ modulo m kallas *relativt prim* med m om $\text{sgd}(a, m) = 1$.

Anmärkning 2.16. När vi skriver en sån här definition är det viktigt att vi vet att egenskapen vi pratar om gäller för ALLA representanter samtidigt.

Exempel 2.17. Tänk er att vi vill definiera jämna tal modulo m genom att säga att $\overline{a}$ är jämnt om a är jämnt. Men om vi kollar på restklassen $\overline{1}$ modulo 5 så är 1 udda, men samtidigt så har vi $\overline{1} = \overline{6}$ och 6 är ett jämnt tal! Så vår definition fungerar inte...

Definitionen av relativt prima restklasser ger oss följande väldigt viktiga funktion, Eulers φ-funktion.

Definition 2.18. Låt $\varphi(m)$ beteckna antalet restklasser modulo m som är relativt prima med m. Denna funktion φ kallas för *Eulers φ-funktion.*

Exempel 2.19. Låt $m = 6$. Vi har 6 stycken restklasser: $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$. Restklasserna $\overline{0}, \overline{2}, \overline{3}, \overline{4}$ är inte relativt prima med m, medan restklasserna $\overline{1}$ och $\overline{5}$ är relativt prima. Så $\varphi(6) = 2$.

Definition 2.20. En mängd $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ kallas för ett *reducerat restklassystem* om de $\varphi(m)$ heltalen som den innehåller är parvis icke-kongruenta och relativt prima med m.

Proposition 2.21. Låt p vara ett primtal och k ett positivt heltal. Då gäller $\varphi(p^k) = p^k - p^{k-1}$.

Bevis. Först måste vi tänka på vilka delare till p^k vi har. Det är talen $\{1, p, p^2, \ldots, p^{k-1}, p^k\}$. Så ett heltal är relativt primt med p^k om det inte innehåller en faktor p, alltså alla tal utom talen np. Antalet heltal mellan 1 och p^k som INTE är relativt prima med p^k är alltså p^{k-1}, eftersom n kan vara $1, 2, \ldots, p^{k-1}$. Detta ger oss att $\varphi(p^k) = p^k - p^{k-1}$. □

Proposition 2.22. Om $m_1, m_2 \in \mathbb{Z}$ är relativt prima så gäller

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

Bevis. Först konstruerar vi en funktion mellan mängderna $\mathcal{F}(m_1 m_2)$ och $\mathcal{F}(m_1) \times \mathcal{F}(m_2)$, där $\mathcal{F}(n)$ är det fullständiga restklassystemet $\{0, 1, \ldots, n-1\}$. Vi visar sedan att denna funktion är en bijektion.

Vi definierar τ på följande sätt:

$$\begin{aligned} \tau : \mathcal{F}(m_1 m_2) &\to \mathcal{F}(m_1) \times \mathcal{F}(m_2) \\ x &\mapsto (x_1, x_2) \end{aligned}$$

där $x \equiv x_1 \pmod{m_1}$ och $x \equiv x_2 \pmod{m_2}$. Vi vill nu visa att för varje $(x_1, x_2) \in \mathcal{F}(m_1) \times \mathcal{F}(m_2)$ så finns det precis ett $x \in \mathcal{F}(m)$ så att

$$\begin{cases} x \equiv x_2 \pmod{m_1}, \\ x \equiv x_1 \pmod{m_2}. \end{cases}$$

Men Kinesiska restsatsen säger oss att det finns ett sådant x och att det är unikt (modulo $m_1 m_2$). Vi har nu visat att τ är en bijektion.

Låt nu $\mathcal{R}(n)$ vara den delmängd $\mathcal{F}(n)$ som innehåller alla element som är relativt prima med n. Antalet element i $\mathcal{R}(n)$ är alltså $\varphi(n)$. Vi påstår nu att bilden av $\mathcal{R}(m_1 m_2)$ är precis $\mathcal{R}(m_1) \times \mathcal{R}(m_2)$, med andra ord $\tau(x) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$ om och endast om $x \in \mathcal{R}(m_1 m_2)$. Om detta är sant så ger restriktionen av τ till $\mathcal{R}(m_1 m_2)$ en bijektion

$$\tau : \mathcal{R}(m_1 m_2) \to \mathcal{R}(m_1) \times \mathcal{R}(m_2).$$

Detta betyder i så fall att mängderna innehåller lika många element, d.v.s. att $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.

Så antag nu att $x \in \mathcal{R}(m_1 m_2)$, d.v.s. $\text{sgd}(x, m_1 m_2) = 1$. Men då måste även $\text{sgd}(x, m_1) = 1 = \text{sgd}(x, m_2)$ vara sant (om x och $m_1 m_2$ inte har några gemensamma delare så kan inte x och m_1 respektive m_2 ha några gemensamma delare). Eftersom $x \equiv x_i \pmod{m_i}$ så har vi enligt Lemma 2.14 $\text{sgd}(x_1, m_1) = 1 = \text{sgd}(x_2, m_2)$, d.v.s. $\tau(x) = (x_1, x_2) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$. Vi har alltså visat att

$$x \in \mathcal{R}(m_1 m_2) \Rightarrow \tau(x) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2).$$

Antag istället att $\tau(x) = (x_1, x_2) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2)$, d.v.s.

$$\text{sgd}(x_1, m_1) = 1 = \text{sgd}(x_2, m_2).$$

Om vi använder Lemma 2.14 igen så ser vi att

$$\text{sgd}(x, m_1) = 1 = \text{sgd}(x, m_2).$$

Vi kan nu använda Sats 1.12 för att dra slutsatsen

$$\text{sgd}(x, m_1 m_2) = 1,$$

d.v.s. $x \in \mathcal{R}(m_1 m_2)$. Vi har alltså visat att

$$\tau(x) \in \mathcal{R}(m_1) \times \mathcal{R}(m_2) \Rightarrow x \in \mathcal{R}(m_1 m_2).$$

Detta betyder att restriktionen av τ till $\mathcal{R}(m_1 m_2)$ är en bijektion mellan $\mathcal{R}(m_1 m_2)$ och $\mathcal{R}(m_1) \times \mathcal{R}(m_2)$, alltså gäller $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. □

Exempel 2.23.

$$\varphi(12) = \varphi(3 \cdot 4) = \varphi(3)\varphi(2^2) = 2 \cdot (2^2 - 2^1) = 4$$

Övning 2.24. Hitta en formel för $\varphi\left(\prod_{i=1}^{N} p_i^{k_i}\right)$ där $p_1, \ldots, p_N$ är distinkta primtal.

Lösning. Här använder vi oss först av Proposition 2.22 för att skriva:

$$\varphi\left(\prod_{i=1}^{N} p_i^{k_i}\right) = \prod_{i=1}^{N} \varphi\left(p_i^{k_i}\right).$$

Sedan behöver vi komma ihåg att för ett primtal p gäller

$$\varphi(p^k) = p^k - p^{k-1}.$$

Om vi sätter samman detta får vi:

$$\varphi\left(\prod_{i=1}^{N} p_i^{k_i}\right) = \prod_{i=1}^{N} \varphi\left(p^{k_i}\right) = \prod_{i=1}^{N} \left(p^{k_i} - p^{k_i - 1}\right).$$

3 Eulers och Fermats satser samt RSA-kryptering

3.1 Eulers och Fermats satser

Proposition 3.1. Låt $\text{sgd}(a, m) = 1$. Om $\{r_1, \ldots, r_m\}$ är ett fullständigt restklassystem modulo m och $\{s_1, \ldots, s_{\varphi(m)}\}$ är ett reducerat restklassystem modulo m, då är även $\{ar_1, \ldots, ar_m\}$ är ett fullständigt restklassystem modulo m och $\{as_1, \ldots, as_{\varphi(m)}\}$ är ett reducerat restklassystem modulo m.

Bevis. För att bevisa att $\{ar_1, \ldots, ar_m\}$ är ett fullständigt restklassystem modulo m måste vi visa att $ar_i \equiv ar_j \pmod{m}$ om och endast om $i = j$. Vi antar därför att $ar_i \equiv ar_j \pmod{m}$, vilket enligt definition innebär att $m|a(r_i - r_j)$. Eftersom att $\text{sgd}(a, m) = 1$ så måste $m|(r_i - r_j)$, d.v.s. $r_i \equiv r_j \pmod{m}$. Men eftersom vi från början hade ett fullständigt restklassystem så innebär detta att $i = j$.

Nu vill vi visa att $\{as_1, \ldots, as_m\}$ är ett reducerat restklassystem modulo m. Vi måste visa två saker:

$$as_i \equiv as_j \pmod{m} \Leftrightarrow i = j$$

och att $\text{sgd}(m, as_i) = 1$ för alla i. Att visa att elementen är parvis icke-kongruenta visar vi på precis samma sätt som innan. Nu återstår det att $\text{sgd}(m, as_i) = 1$ för alla i. Vi vet att både $\text{sgd}(m, a) = 1$ och $\text{sgd}(m, s_i) = 1$, och enligt Sats 1.12 gäller då även $\text{sgd}(m, as_i) = 1$. □

Vi kommer använda den här satsen för att bevisa Eulers sats:

Sats 3.2 (Eulers sats)**.** Om $\text{sgd}(a, m) = 1$, så har vi

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Bevis. Låt $\{s_1, \ldots, s_{\varphi(m)}\}$ vara ett reducerat restklassystem modulo m. Då är enligt föregående sats även $\{as_1, \ldots, as_{\varphi(m)}\}$ ett reducerat restklassystem modulo m.

Det första vi behöver göra är att inse att för varje $i = 1, \ldots, \varphi(m)$ så finns precis ett j så att $as_i \equiv s_j \pmod{m}$. Det betyder att om vi multiplicerar ihop alla representanter i de båda reducerade restklassystemen så kommer produkterna vara kongruenta modulo m, d.v.s.:

$$\prod_{i=1}^{\varphi(m)} as_i \equiv \prod_{i=1}^{\varphi(m)} s_i \pmod{m}.$$

Nästa steg är att bryta ut $a^{\varphi(m)}$ från vänsterledet:

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} s_i \equiv \prod_{i=1}^{\varphi(m)} s_i \pmod{m}.$$

När vi gjort detta är vi redo att övergå till definitionen av kongruens, vi har nämligen att $m| \left((a^{\varphi(m)} - 1) \prod_{i=1}^{\varphi(m)} s_i \right)$. Men eftersom att $\text{sgd}(m, s_i) = 1$ för alla i så får vi att $m|(a^{\varphi(m)} - 1)$, vilket är ekvivalent med att $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Sats 3.3 (Fermats lilla sats)**.** Om p är ett primtal, och $p \nmid a$, så har vi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dessutom gäller det att för varje heltal a att $a^p \equiv a \pmod{p}$.

Bevis. Den första delen följer direkt från Eulers sats eftersom $\varphi(p) = p-1$ för ett primtal p. Om $p \nmid a$ så följer det andra resultatet genom att multiplicera den första kongruensen med a på båda sidor. Om $p|a$ så är både a och a^p kongruent med 0 modulo p, och därmed följer det andra reultatet. □

Exempel 3.4. • $99^{12} \equiv 1 \pmod{13}$, eftersom $13 \nmid 99$.

• $15^6 \equiv 1 \pmod{14}$, eftersom $\text{sgd}(15, 14) = 1$ och $\varphi(14) = \varphi(2)\varphi(7) = 6$.

• $15^5 \equiv 15 \equiv 0 \pmod{5}$, eftersom $5 \mid 15$.

• $5^8 \equiv 10 \pmod{15}$ motsäger inte Eulers sats eftersom $\text{sgd}(5, 15) = 5 > 1$.

Sats 3.5. Antag att m är ett positivt kvadratfritt heltal, d.v.s. att varje primtal i en faktorisering $m = p_1 p_2 \dots p_r$ av m bara förkommer en gång, och låt e och d vara positiva heltal sådana att $ed \equiv 1 \pmod{\varphi(m)}$. Då gäller

$$a^{ed} \equiv a \pmod{m}$$

för varje heltal a.

Bevis. Det vi vill visa är alltså att $m|(a^{ed} - a)$. Kom ihåg satsen som säger att om $\text{sgd}(a, b) = 1$, $a|c$ och $b|c$ så gäller även $ab|c$ (Sats 1.11). Eftersom m är kvadratfritt så betyder detta att det räcker med att visa att varje primfaktor p av m delar $a^{ed} - a$.

Om $p|a$ så har vi såklart också att $p|(a^{ed} - a)$, antag därför att $p \nmid a$. Först ska vi göra en liten omskrivning av $\varphi(m)$. Eftersom p och $\frac{m}{p}$ är relativt prima (då m är kvadratfritt) så kan vi använda satsen från slutet av förra föreläsningen (Proposition 2.22):

$$\varphi(m) = \varphi(p \cdot \frac{m}{p}) = \varphi(p)\varphi(\frac{m}{p}) = (p-1)\varphi(\frac{m}{p}).$$

Vidare så har vi $ed - 1 = \varphi(m)n = (p-1)\varphi(\frac{m}{p})n$. Vad $\varphi(\frac{m}{p})n$ är spelar inte så stor roll, förutom att det är ett heltal, så vi kommer beteckna detta med N. Sammanfattningsvis har vi alltså

$$ed = 1 + (p-1)N.$$

Det ger oss det vi behöver för att slutföra beviset:

$$a^{ed} \equiv a^{1+(p-1)N} \equiv a \cdot (a^{p-1})^N \overset{\text{Fermat}}{\equiv} a \cdot 1^N \equiv a \pmod{p}.$$

Vi har alltså visat att för varje primfaktor p så delar p talet $a^{ed} - a$, och därför delar även m talet $a^{ed} - a$. Detta ekvivalent med att $a^{ed} \equiv a \pmod{m}$. □

3.2 RSA-kryptering

På den här föreläsningen ska vi lära oss matematiken bakom RSA-kryptering. Vi börjar att prata lite allmänt om problemen kring att skicka krypterade meddelanden.

Säg att vi har två personer, Alice och Bob, som vill skicka hemliga meddelanden mellan varandra. Men Alice och Bob bor långt ifrån varandra, så de kan inte alltid träffas och viska meddelandet till varandra. Bob kommer på den smarta idén att de istället kan skicka krypterade meddelanden till varandra.

Alice kommer ihåg vad hon lärt sig i Algebra II och hittar på ett sätt som Bob kan kryptera meddelandet så att bara hon kan dekryptera det! Det spelar ju ingen roll om andra vet hur man krypterar, så länge de inte vet hur man dekrypterar. (Egentligen var det Ron Rivest, Adi Shamir och Len Adleman som först beskrev metoden 1977.)

Alice använder sig av följande sats från förra avsnittet:

Sats 3.6. Antag att m är ett positivt kvadratfritt heltal, d.v.s. att varje primtal i en faktorisering $m = p_1 p_2 \dots p_r$ av m bara förkommer en gång, och låt e och d vara positiva heltal sådana att $ed \equiv 1 \pmod{\varphi(m)}$. Då är

$$a^{ed} \equiv a \pmod{m}$$

för varje heltal a.

Så frågan är nu hur vi ska utnyttja detta för att skicka krypterade meddelanden? Tanken är följande:

- En person A som vill få krypterade meddelanden skickade till sig väljer ut m, e och d som uppfyller villkoren i satsen. D.v.s. m är kvadratfritt och e, d uppfyller $ed \equiv 1 \pmod{\varphi(m)}$.
- A håller talparet (m, d) hemligt, men offentliggör talparet (m, e).
- Om en person B vill skicka ett hemligt meddelande $'a'$ till A så beräknar B kongruensen $b \equiv a^e \pmod{m}$ och skickar $'b'$ till A.
- För att dekryptera meddelandet så beräknar A kongruensen $b^d \pmod{m}$. Enligt satsen ovan så får vi $b^d \equiv (a^e)^d \equiv a^{ed} \equiv a \pmod{m}$.
- Eftersom ingen annan har tillgång till den hemliga nyckeln (m, d) så är det ingen som vet vilket tal d vi ska använda för att få fram meddelandet $'a'$.

Eftersom talen m och e är offentliga så måste vi ställa lite krav på dessa för att ingen ska kunna lista ut talet d utifrån denna information. Först och främst är det svårt att dra e:te roten ur ett tal modulo m om man inte känner till talet d. För att hitta d måste man hitta $\varphi(m)$, och för att göra det måste man faktorisera m. Det som gör att RSA-kryptering fungerar är att det inte på något tillräckligt snabbt sätt går att faktorisera stora tal.

Så om vi kan faktisera talet m, då är vår kryptering helt meningslös!

Exempel 3.7. Alice och Bob vill kunna skicka krypterade meddelanden mellan varandra. För att kunna ta emot meddelanden skapar Alice en offentlig och en hemlig nyckel:

- Alice börjar med att välja $m = pq = 8892498047231$, där $p = 2218339$ och $q = 4008629$ är två slumpade primtal, och sedan $e = 2^{16} + 1 = 65537$.
- Alice har fått tips från sina datavetarvänner om att välja e på den här formen för att beräkningarna på datorn ska gå snabbt. Dessutom är e ett primtal, så chansen är hög att e och $\varphi(m)$ är relativt prima.
- Sedan kontrollerar Alice att talet e är relativt primt med $\varphi(m) = (p-1)(q-1) = 8892491820264$.
- Eftersom e är ett primtal är $\text{sgd}(e, n) > 1$ om och endast om $e|n$. Det räcker alltså att kontrollera ifall $\frac{p-1}{e}$ och $\frac{q-1}{e}$ är heltal eller ej.
- Genom att lösa ekvationen $65537 \cdot d \equiv 1 \pmod{\varphi(m)}$ så kommer Alice fram till att hon ska välja d som:
$$d = 8406055407617.$$
- Alice har nu tal m, e, d som uppfyller de kriterier som behövs för att RSA-krypteringen ska fungera, d.v.s. m är kvadratfritt och $ed \equiv 1 \pmod{\varphi(m)}$.
- Nu publicerar Alice sin offentliga nyckel $(m, e) = (8892498047231, 65537)$ och håller den andra hemliga nyckeln, $(m, d) = (8892498047231, 8406055407617)$ hemlig.
- Nu vill Bob skicka det otroligt hemliga meddelandet "ALGEBRA" till Alice. Först så väljer Bob ett lämpligt sätt att representera ordet med siffror. Bob väljer att representera "A" med 01, "B" med 02 osv.
- Talet Bob vill skicka blir då:
$$a = 01120705021801$$
- För att kryptera meddelandet använder Bob den offentliga nyckeln (m, e) som han har fått av Alice och beräknar $a^e \pmod{m}$, d.v.s.:
$$1120705021801^{65537} \equiv 6563200906018 \pmod{8892498047231}.$$
- Bob kan nu helt öppet skicka meddelandet "6563200906018" till Alice.
- När Alice får meddelandet så använder hon sin hemliga nyckel (m, d) för att dekryptera meddelandet och beräknar $b^d \pmod{m}$, d.v.s.:
$$6563200906018^{8406055407617} \equiv 1120705021801 \pmod{8892498047231}$$
- Alice kan nu läsa ut meddelandet "01120705021801" som "ALGEBRA"!

4 Introduktion till ringar

4.1 Definitionen av begreppet ring

Nu går vi in i den andra delen av kursen och vi ska nu prata om något som heter ringar. Det vi kommer göra är att ta de viktigaste egenskaperna hos additionen och multiplikationen hos heltal och skriva ner dem i en lista. Sedan kallar vi alla mängder tillsammans med två operationer som uppfyller allt på denna lista för en ring!

♪♪En ring är en mängd och två funktioner,
och som krav ställs på dessa därvid
att det är en abelsk grupp med additionen,
och med gånger en monoid. ♪♪

Definition 4.1. En *ring* är en mängd R med två (binära) funktioner, $+, \cdot$, från $R \times R$ till R, så att följande gäller:

(i) Det existerar ett element $0_R \in R$ så att för alla $a \in R$ gäller $a + 0_R = a = 0_R + a$. (Additivt neutralt element)

(ii) För alla $a \in R$ finns ett element $b \in R$ så att $a + b = 0 = b + a$. Vi betecknar detta element med $-a$. (Additiv invers)

(iii) För alla $a, b, c \in R$ gäller $(a + b) + c = a + (b + c)$. (Additativ associativitet)

(iv) För alla $a, b \in R$ gäller $a + b = b + a$. (Additiv kommutativitet)

(v) Det existerar ett element $1_R \in R$ så att för alla $a \in R$ gäller $1_R \cdot a = a = a \cdot 1_R$. (Multiplikativt neutralt element)

(vi) För alla $a, b, c \in R$ gäller $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (Multiplikativ associativitet)

(vii) För alla $a, b, c \in R$ gäller $a \cdot (b + c) = a \cdot b + a \cdot c$ samt $(a + b) \cdot c = a \cdot c + b \cdot c$. (Distributivitet)

Anmärkning 4.2. Vi skriver ofta ab istället för $a \cdot b$.

Om en mängd och en binär funktion + uppfyller egenskap (i)-(iii) kallas detta för en grupp. Om dessutom egenskap (iv) gäller så kallas detta för en abelsk (eller kommutativ) grupp (efter Niels Henrik Abel). Vi kommer inte studera dessa objekt i den här kursen, utan det gör man i kursen Algebraiska strukturer! Om en mängd och en binär funktion $\cdot$ uppfyller egenskap (v) och (vi) kallas detta för en monoid. Detta är inte heller något som ni behöver veta för den här kursen.

Det är inte bara en tillfällighet att funktionerna i definitionen betecknas precis som plus och gånger, för t.ex. heltalen $\mathbb{Z}$ tillsammans med ”vanliga” additionen och multiplikationen är ett exempel på en ring!

Exempel 4.3. Exempel på ringar:

1. $(\mathbb{Z}, +, \cdot)$,

2. $(\mathbb{Q}, +, \cdot)$,

3. $(\mathbb{R}, +, \cdot)$,

4. $(\mathbb{C}, +, \cdot)$,

5. $(\mathbb{Z}_{\geq}, +, \cdot)$ är INTE en ring. Vi har inte någon additiv invers!

6. Polynom med heltals-/rationella/reella/komplexa koefficienter med funktionerna:

$$(p+q)(x) = p(x) + q(x)$$

$$(p \cdot q)(x) = p(x)q(x)$$

7. Restklasser modulo $n \in \mathbb{Z}$, denna ring betecknas som $\mathbb{Z}_n$,

8. $\mathrm{M}_{2\times 2}(\mathbb{R})$, ringen av alla reella $n \times n$-matriser.

Vi ska kolla lite närmare på ett exempel på en ring, nämligen ringen $\mathbb{Z}_3$. Elementen i ringen $\mathbb{Z}_3$ är restklasser modulo 3, d.v.s. $\overline{0}, \overline{1}, \overline{2}$. Vi definierar additionen och multiplikationen på följande sätt:

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Att denna addition och multiplikation är väldefinierad, d.v.s. ger samma resultat vilken representant vi än väljer, följer från Proposition 2.9. Vi skriver upp additions- och multiplikationstabellerna:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

(i) $0_{\mathbb{Z}_3} = \overline{0}$ enligt additionstabellen,

(ii) $-\overline{a} = \overline{3-a} = \overline{-a}$ enligt additionstabellen,

(iii) $(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\overline{b+c} = \overline{a}+(\overline{b}+\overline{c})$ enligt definitionen av addition och additiv associativitet hos heltalen,

(iv) $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+\overline{a}$ enligt definitionen av addition och additiv kommutativitet hos heltalen (även enligt additionstabellen),

(v) $1_{\mathbb{Z}_3} = \overline{1}$ enligt multiplikationstabellen,

(vi) $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a\cdot b}\cdot\overline{c} = \overline{(a\cdot b)\cdot c} = \overline{a\cdot(b\cdot c)} = \overline{a}\cdot\overline{b\cdot c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$ enligt definitionen av multiplikation och multiplikativ associativitet hos heltalen,

(vii) $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b+c} = \overline{a(b+c)} = \overline{a\cdot b+a\cdot c} = \overline{a\cdot b}+\overline{a\cdot c} = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$, och på samma sätt: $(\overline{a+b})\cdot\overline{c} = \overline{a}\cdot\overline{c}+\overline{b}\cdot\overline{c}$, enligt definitionen av addition och multiplikation, samt distributivitet hos heltalen.

4.2 Lite notation och grundläggande räkneregler

För att bekanta oss med begreppet ”ring” lite mer ska vi titta på några grundläggande egenskaper. Först och främst pratar vi i definitionen av en ring om ett speciellt element ”0”. Vi ska börja med att visa att det bara finns ett enda element med denna egenskap! Antag att det finns två element, 0 och 0’, som uppfyller (i) Då får vi:

$$0 = 0 + 0' = 0'.$$

På samma sätt kan vi visa att elementet ”1” är unikt: Antag att det finns två element, 1 och 1’, som uppfyller (v). Då får vi:

$$1 = 1 \cdot 1' = 1'.$$

Till sist vill vi även visa att den additiva inversen alltid är unik. Antag därför att både b och c är additiva inverser till ett element a.

$$b = 0 + b = (c + a) + b = c + (a + b) = c + 0 = c.$$

För att göra notationen lite enklare skriver vi ibland $a - b$ istället för $a + (-b)$ för två ringelement a, b.

Sats 4.4. Låt $a, b, c \in R$ där R är en ring. Om $a + c = b + c$ så är $a = b$.

Bevis. Enligt egenskap (ii) i definitionen av en ring så finns det ett element $-c$ så att $c + (-c) = 0$. Om vi adderar detta element till båda sidor av likheten får vi:

$$\begin{gathered} a + c = b + c \\ \Leftrightarrow \\ a + c + (-c) = b + c + (-c) \\ \Leftrightarrow \\ a + 0 = b + 0 \\ \Leftrightarrow \\ a = b. \end{gathered}$$

□

Exempel 4.5. Vi har däremot inte att om $ac = bc$ så är $a = b$. Titta t.ex. på exemplet med restklasser modulo 6:

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{10} = \overline{5} \cdot \overline{2}$$

Men vi har $\overline{2} \neq \overline{5}$ modulo 6.

Vi kommer senare att titta på vilken egenskap vi måste lägga till för att just detta ska gälla!

Sats 4.6. $0 \cdot a = 0 = a \cdot 0$ för alla $a \in R$.

Bevis.

$$\begin{gathered}
1 \cdot a = a \\
(1+0) \cdot a = a \\
1 \cdot a + 0 \cdot a = a \\
a + 0 \cdot a = a \\
-a + a + 0 \cdot a = -a + a \\
0 + 0 \cdot a = 0 \\
0 \cdot a = 0
\end{gathered}$$

□

Sats 4.7. $(-1) \cdot a = -a$ för alla $a \in R$.

Bevis.

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a = 0 \cdot a = 0$$

Men vi har visat att den additiva inversen är unik, så $(-1) \cdot a = -a$. □

Sats 4.8. Om $|R| > 1$ så är $0 \neq 1$.

Bevis. Antag att $0 = 1$, då har vi att föra varje $a \in R$

$$a = 1 \cdot a = 0 \cdot a = 0.$$

Så $a = 0$ för varje $a \in R$, alltså är $R = \{0\}$ och $|R| = 1$. Om $|R| > 1$ måste alltså $0 \neq 1$ gälla. □

4.3 Delringar

Definition 4.9. En delmängd $S \subseteq R$ av en ring R kallas för en *delring* om följande gäller:

(i) S, tillsammans operationerna från R, är en ring;

(ii) $0_R = 0_S \in S$ och $1_R = 1_S \in S$.

Anmärkning 4.10. Observera att i det första kriteriet så gömmer sig en viktig detalj, nämligen att S ska vara sluten under både addition och multiplikation. Anledningen till detta att $+$ och $\cdot$ ska vara funktioner från $S \times S$ till S (d.v.s. målmängden är S, inte hela R).

Ni kan jämföra detta med ett delrum från Linjär algebra-kurserna!

Exempel 4.11. Följande är delringar: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Exempel 4.12. Om vi kollar på $\mathbb{Z}_6$ så är $\{\overline{0}, \overline{3}\}$ en delmängd som är en ring med samma multiplikation och addition ($\overline{3}+\overline{3} = \overline{0}, \overline{3} \cdot \overline{3} = \overline{3}$). Restklassen $\overline{3}$ är alltså vårt multiplikativt neutrala element, men det är inte SAMMA multiplikativt neutrala element som i $\mathbb{Z}_6$.

Sats 4.13. Låt R vara en ring och $S \subseteq R$. Då är S en delring om och endast om följande gäller:

(i) $\forall s, t \in S$ så gäller $s + t \in S$, $s \cdot t \in S$ samt $-s \in S$.

(ii) $0_R, 1_R \in S$.

Bevis. Antag först att S är en delring. Att $s + t \in S$, $s \cdot t \in S$ gäller enligt Anmärkning 4.10. Att $-s \in S$ gäller följer från faktumet att den additiva inversen är unik, och det additivt neutrala elementet är samma i R och S. Kriterium (ii) ingår i definitionen av en delring.

Antag istället att (i) och (ii) gäller för en delmängd $S \subseteq R$. Att $0_R = 0_S$ och $1_R = 1_S$ gäller följer från unikheten av additiva och multiplikativa neutrala element. Eftersom att (i) gäller så kan vi begränsa additionen till S och vi får en funktion $+ : S \times S \to S, (s, t) \mapsto s +_R t$. Det viktiga här är alltså att funktionens målmängd faktiskt är S. På samma sätt får vi en funktion $\cdot : S \times S \to S, (s, t) \mapsto s \cdot_R t$. Existensen av invers följer från kriterium (i), d.v.s. $-s \in S$. Existensen av neutrala additiva och multiplikativa element följer direkt från kriterium (ii). Att resten av ringaxiomen gäller följer från att funktionerna $+$ och $\cdot$ är ringoperationer. Om något gäller för alla element i R, gäller det såklart även för alla element i $S \subseteq R$. □

Exempel 4.14. Nu kan vi lätt kontrollera att varken $2\mathbb{Z} \subseteq \mathbb{Z}$ eller $I = \{ri | r \in \mathbb{R}\} \subseteq \mathbb{C}$ är delringar. Varför inte? Jo, i första fallet är (i) uppfylld men inte (ii): $1_{\mathbb{Z}} \notin 2\mathbb{Z}$ och i andra fallet är varken (i) eller (ii) uppfyllt, t.ex. har vi $i \cdot i = -1 \notin I$, fastän $i \in I$, vilket motsäger (i), och $1_{\mathbb{C}} \notin I$, vilket motsäger (ii).

Däremot kan vi nu enkelt kontroller att t.ex.

$$\mathbb{R}[x^2] = \{a_{2n}x^{2n} + a_{2(n-1)}x^{2(n-1)} + \cdots + a_2x^2 + a_0 \mid a_{2k} \in \mathbb{R}\} \subseteq \mathbb{R}[x]$$

är en delring.

- Först konstaterar vi att de konstanta polynomet 0 och 1 ligger i $\mathbb{R}[x^2]$.
- Det är även lätt att se att om $p(x) \in \mathbb{R}[x^2]$, så gäller även $-p(x) \in \mathbb{R}[x^2]$.
- Samma sak gäller för additionen: om $a_{2k+1} = 0 = b_{2k+1}$ så är såklart också $a_{2k+1} + b_{2k+1} = 0$, och alltså gäller $p(x), q(x) \in \mathbb{R}[x^2] \Rightarrow p(x) + q(x) \in \mathbb{R}[x^2]$.
- Koefficienten framför x^k i $p(x) \cdot q(x)$ är $\sum_{i+j=k} a_i b_j$. Om k är udda och $k = i + j$, så måste minst en av i, j vara udda. Om $p(x), q(x) \in \mathbb{R}[x^2]$ så är då minst en av a_i, b_j lika med 0, vilket innebär att $a_i b_j = 0$. Det betyder att hela summan $\sum_{i+j=k} a_i b_j = 0$, om k är udda. Alltså har vi $p(x) \cdot q(x) \in \mathbb{R}[x^2]$.

4.4 Kartesiska produkten av två ringar

Ett viktigt exempel på hur man kan skapa en ny ring ur två ringar är att titta på par av element från de två ringarna.

Sats 4.15. Låt $(R, +_R, \cdot_R)$ och $(S, +_S, \cdot_S)$ vara två stycken ringar. Då är deras *kartesiska produkt*

$$R \times S := \{(r, s) \mid r \in R, s \in S\}$$

igen en ring med *komponentvis* addition och multiplikation, det vill säga, $(r, s)+(r', s') = (r +_R r', s +_S s')$ och $(r, s) + (r', s') = (r \cdot_R r', s \cdot_S s')$. Det additivt neutrala elementet är $(0_R, 0_S)$ och det multiplikativt neutrala elementet är $(1_R, 1_S)$.

Anmärkning 4.16. Ni kommer se senare att vi kan välja additionen och multiplikationen på $R \times S$ på olika sätt, men om inget annat anges antar man alltid att man menar komponentvis addition och multiplikation.

Exempel 4.17. Låt $R = \mathbb{Z}_2$ och $S = \mathbb{Z}_2$. Additionstabellen för $\mathbb{Z}_2 \times \mathbb{Z}_2$ ser då ut på följande sätt:

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Multiplikationstabellen för $\mathbb{Z}_2 \times \mathbb{Z}_2$ ser ut på följande sätt:

·	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
(1,0)	(0,0)	(0,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(1,0)	(1,1)

5 Egenskaper hos ringar

5.1 Olika typer av ringar och element

På den här föreläsningen ska vi gå igenom en del (extra) egenskaper som en ring kan ha och se vad det får för konsekvenser. I första delen av kursen jobbade vi massor med *ringen* $\mathbb{Z}$. T.ex. såg vi följande:

- Det finns "odelbara" element, primtal, och varje heltal kan på ett entydigt sätt skrivas som en produkt av dessa
- Vi kan hitta största gemensamma delare med hjälp av Euklides algoritm.
- Varje ideal I är på formen $g\mathbb{Z}$.

Så nu vill vi undersöka om dessa egenskaper (och många fler) gäller för alla ringar, och om så inte är fallet, vilka extra egenskaper måste vi lägga till för att det nödvändigtvis ska gälla?

5.1.1 Kommutativa ringar

Första extra egenskapen en ring kan här är följande:

Definition 5.1. En ring R är *kommutativ* om $ab = ba$ för alla $a, b \in R$.

Exempel 5.2. Exempel på kommutativa ringar är $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n, \mathbb{Z}[x]$.

Exempel 5.3. Ett exempel på en icke-kommutativ ring är $n \times n$-matriser.

Ett annat exempel på en icke-kommutativ ring är kvaternionerna, $\mathbb{H}$. Kvaternionerna består av element på formen

$$q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$

där $a, b, c, d \in \mathbb{R}$.

Additionen definieras på följande sätt:

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k}.$$

Multiplikationen definieras med hjälp av följande regler för multiplikation av $\mathbf{i}, \mathbf{j}, \mathbf{k}$:

	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\mathbf{i}$	-1	$\mathbf{k}$	-$\mathbf{j}$
$\mathbf{j}$	$-\mathbf{k}$	-1	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	-1

Produkten av två element blir alltså:

$$\begin{aligned}(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) \cdot (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = {} & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) \\ & + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} \\ & + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} \\ & + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k}\end{aligned}$$

Vi ser här att t.ex. $\mathbf{ij} = \mathbf{k} \neq -\mathbf{k} = \mathbf{ji}$, alltså är ringen INTE kommutativ.

5.1.2 Nolldelare och integritetsområden

En annan sak ni behöver komma ihåg från förra föreläsningen är att det INTE alltid är sant att $ac = bc \Rightarrow a = b$ om $c \neq 0$. Vi ska nu titta på vilken egenskap vi behöver för att detta ska gälla.

$$\begin{gathered} ac = bc \\ [-(bc) = (-1)(bc) = (-1b)c = (-b)c] \\ ac + (-b)c = 0 \\ (a + (-b))c = 0 \end{gathered}$$

Nu vill vi säga att antingen är $a + (-b) = 0$ eller så är $c = 0$. Men det kan vi inte alltid göra. Vi inför följande definition:

Definition 5.4. Vi säger att ett element $a \in R$ är en *nolldelare* om $a \neq 0$ och det finns ett $b \in R$ s.a. $b \neq 0$ och $ab = 0$ eller $ba = 0$.

Till exempel i $\mathbb{Z}_6$ är $\overline{2}$ en nolldelare:

$$\overline{2} \cdot \overline{3} = \overline{6} = 0.$$

Om vi tittar tillbaka på ekvationen

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{5} \cdot \overline{2}$$

såg vi att vi inte kunde "dela bort" 2:an. Anledningen till detta är att $\overline{2}$ är en nolldelare!

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{5} \cdot \overline{2}$$

$$\Leftrightarrow (\overline{5} - \overline{2}) \cdot \overline{2} = \overline{3} \cdot \overline{2} = 0$$

Exempel 5.5. Alla element som inte är relativt prima med n är nolldelare i $\mathbb{Z}_n$. T.ex. i $\mathbb{Z}_6$ har vi:

$$\overline{2} \cdot \overline{3} = \overline{0}$$

Mer allmänt har vi: Antag att $\text{sgd}(a, n) = d > 1$ och $\overline{a} \neq 0$. Då finns det $\overline{b}, \overline{c} \in \mathbb{Z}_n \setminus \{0\}$ så att $n = bd$ och $a = cd$. Men då har vi $a \cdot b \equiv (cd)b \equiv c(bd) \equiv cn \equiv 0 \pmod{n}$. Alltså är $\overline{a}$ en nolldelare i $\mathbb{Z}_n$.

Exempel 5.6. Det multiplikativt neutrala elementet 1 är aldrig en nolldelare eftersom för varje $a \neq 0$ har vi $1 \cdot a = a \cdot 1 = a \neq 0$.

Nu kommer vi till andra extra egenskapen en ring kan ha:

Definition 5.7. Ett *integritetsområde* är en nollskild kommutativ ring som saknar nolldelare.

Exempel 5.8. Exempel på integritetsområden är $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[x], \mathbb{Z}_p$ där p är ett primtal. Om R är ett integritetsområde så är varje delring till R ett integritetsområde.

Proposition 5.9. Om R är ett integritetsområde och $c \neq 0$ så medför $ac = bc$ att $a = b$.

Bevis.

$$\begin{aligned} ac &= bc \\ ac - bc &= 0 \\ (a-b)c &= 0 \end{aligned}$$

Eftersom $c \neq 0$, så måste $a - b = 0$ eftersom vi inte har några nolldelare! Alltså är $a = b$. □

5.1.3 Inverterbara element och kroppar

Nästa fråga vi vill ställa oss är om ekvationen $ax = b$ har en lösning för varje $a, b \in R$. Eller ännu mer specifikt, har ekvationen $ax = 1$ en lösning för varje $a \in R$? Till exempel i $\mathbb{Z}$ har $(-1)x = 1$ en lösning, men inte $2x = 1$. När det gäller $\mathbb{Z}_n$ har vi tidigare sett en sats som säger att ekvationen $ax \equiv 1 \pmod{n}$ har en lösning om och endast om $\text{sgd}(a, n) = 1$.

Definition 5.10. Om R är en ring och $a \in R$ så säger vi att a är *inverterbart* om det finns ett b så att $ab = ba = 1$. Vi kallar b för a:s invers och betecknar $b = a^{-1}$

Exempel 5.11. I $\mathbb{Z}$ är bara ± 1 inverterbara, men i $\mathbb{Q}$ är alla nollskilda element inverterbara! Om vi kollar på $\mathbb{Z}_4$ och dess multiplikationstabell så ser vi att $\overline{1}$ och $\overline{3}$ har inverser, men inte $\overline{0}$ och $\overline{2}$. Anledningen till detta är att $\overline{1}$ och $\overline{3}$ är relativt prima modulo 4, men att $\overline{0}$ och $\overline{2}$ inte är det.

Om ringen inte är kommutativ kan det finnas bara en höger- respektive vänsterinvers, d.v.s. det finns b så att $ab = 1$, men $ba \neq 1$ (och vice versa). Men om det finns både en höger- och en vänsterinvers, då måste detta vara samma element:

$$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c.$$

Exempel 5.12. • 1 är alltid inverterbart: $1 \cdot 1 = 1$.

- 0 är aldrig ett inverterbart element om $|R| > 1$.
- En nolldelare är aldrig inverterbar. Antag att a är både inverterbar och en nolldelare. Då existerar $b \neq 0$ så att $ab = 0$ och det existerar a^{-1} så att $a^{-1}a = 1$.

$$\begin{aligned} ab &= 0 \\ a^{-1}(ab) &= a^{-1} \cdot 0 \\ (a^{-1}a)b &= 0 \\ 1 \cdot b &= 0 \\ b &= 0. \end{aligned}$$

Men detta är en motsägelse då b antogs vara nollskild.

Nu ska vi kolla på en mycket speciell typ av ring, nämligen en kommutativ ring där alla element utom 0:an är inverterbara:

Definition 5.13. En kommutativ ring $K \neq \{0\}$ kallas för en *kropp* om alla nollskilda element är inverterbara.

Om K inte är kommutativ, men alla alla nollskilda element är inverterbara så kallas K för en *skevkropp* eller en *divisionsring*.

Proposition 5.14. En kropp är ett integritetsområde.

Bevis. Vi bevisade tidigare att ett inverterbart element aldrig är en nolldelare, och eftersom varje nollskilt element är inverterbart (och 0:an inte är en nolldelare enligt definition) så är kroppen ett integritetsområde. □

Exempel 5.15. • $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ är kroppar.

• $\mathbb{Z}_3$ är en kropp. Detta kan vi se genom att titta på dess multiplikationstabell!

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Sats 5.16. $\mathbb{Z}_p$ är en kropp om och endast om p är ett primtal.

Bevis. Till och börja med noterar vi att $\mathbb{Z}_p$ är kommutativ och nollskild, så vi behöver endast undersöka för vilka heltal p alla nollskilda element är inverterbara.

Antag att p är ett primtal. Enligt Korollarium 2.11 har $ax = 1$ en lösning i $\mathbb{Z}_p$ om och endast om $\text{sgd}(a, p) = 1$. Men för varje nollskild $\overline{a} \in \mathbb{Z}_p$, så har vi $\text{sgd}(a, p) = 1$. Alltså är varje nollskilt tal inverterbart och $\mathbb{Z}_p$ är alltså en kropp.

Antag nu att $p = mn$. Elementen $\overline{m}$ och $\overline{n}$ är då nolldelare, eftersom $\overline{m}, \overline{n} \neq \overline{0}$ och $\overline{m} \cdot \overline{n} = \overline{0}$ i $\mathbb{Z}_p$. Detta betyder att ringen inte är ett integritetsområde, och därmed inte heller en kropp. □

Vi kan dela upp elementen i en ring på följande sätt: 0, nolldelare, övriga, inverterbara. Ett integritetsområde har inga nolldelare, en kropp har dessutom inga ”övriga” element.

5.2 Bråkkroppen av en ring

Vi såg att egenskaperna hos en ring härmade egenskaperna hos heltalen. Om vi igen utgår ifrån heltalen så kan vi ju skapa de rationella talen. De rationella talen är som ni vet en kropp med heltalen som delring. Konstruktionen går till på följande sätt.

Först så tittar vi på par av heltal (a, b) där $b \neq 0$. För varje sånt par är $\frac{a}{b}$ ett rationellt tal, och varje rationellt tal kan (enligt definition) skrivas på det sättet. Vi har alltså mängden

$$M = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

Men i den här mängden finns ju massa dubbletter. Till exempel paret $(2, 6)$ och $(1, 3)$ motsvarar samma rationella tal $\frac{1}{3}$. Vi vet att följande gäller för rationella tal:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Vi kan införa följande ekvivalensrelation för att säga att två talpar i M ska betraktas som lika:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Att detta är en ekvivalensrelation är såklart något som måste bevisas. Om vi nu kollar på alla ekvivalensklasser så motsvarar detta precis de rationella talen!

Exempel 5.17.

$$\overline{(1, 3)} = \{(1, 3), (-1, -3), (2, 6), (-2, -6), \dots\}$$

Men denna konstruktion kan vi generalisera! Låt R vara en ring och titta på mängden

$$M = \{(a, b) \mid a, b \in R, b \neq 0\}.$$

För att denna mängd ska vara icke-tom behöver vi $R \neq \{0\}$. Vi tittar tillbaka på vad vi använt för egenskaper hos heltalen: När vi multiplicerar två talpar får vi

$$(a, b)(c, d) = (ac, bd).$$

För att detta fortfarande ska vara ett element i mängden M måste $bd \neq 0$. Vi får alltså inte ha några nolldelare i R. Vi vill att resultatet ska vara en kropp, och för att den nya multiplikationen ska vara kommutativ, så måste multiplikationen i R vara kommutativ. Vi behöver alltså anta att R är ett integritetsområde.

Lemma 5.18. Låt R vara ett integritetsområde och låt $M = \{(a, b) \mid a, b \in R, b \neq 0\}$. Följande är en ekvivalensrelation på M:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Bevis. • Reflextivitet:

$$(a, b) \sim (a, b) \Leftrightarrow ab = ab \text{ Vilket är sant för alla } a, b \in R.$$

Så relationen är reflexiv.

• Symmetri:

$$\begin{aligned} (a, b) \sim (c, d) &\Leftrightarrow ad = bc \\ \text{[Kommutativitet!]} &\Leftrightarrow cb = da \\ &\Leftrightarrow (c, d) \sim (a, b) \end{aligned}$$

Så relationen är symmetrisk.

- Transitivitet:

$$\begin{aligned}
(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) &\Leftrightarrow ad = bc \wedge cf = de \\
\text{Om } c = 0 : & \\
&\Rightarrow ad = 0 \wedge de = 0 \\
[d \neq 0] &\Rightarrow a = 0 \wedge e = 0 \\
&\Rightarrow af = be \\
&\Leftrightarrow (a,b) \sim (e,f). \\
\text{Om } c \neq 0 : & \\
[\text{Multiplicera första likheten med } ef] &\Rightarrow (ad)(ef) = (bc)(ef) \\
[\text{Kommuativitet (och associativitet)}] &\Leftrightarrow (af)(de) = (be)(cf) \\
[cf = de] &\Rightarrow (af)(cf) = (be)(cf) \\
[\text{Integritetsområde, } cf \neq 0] &\Rightarrow af = be \\
&\Leftrightarrow (a,b) \sim (e,f).
\end{aligned}$$

Så relationen är transitiv, och vi har därmed visat att detta är en ekvivalensrelation! □

Definition 5.19. Låt R vara ett integritetsområde. Vi definierar *bråkkroppen* (fraktionskroppen) $Q(R)$ av R som mängden av ekvivalensklasser av $M = \{(a,b) \mid a,b \in R, b \neq 0\}$ under ekvivalensrelationen $(a,b) \sim (c,d) \Leftrightarrow ad = bc$, tillsammans med följande addition och multiplikation:

$$(a,b) + (c,d) = (ad + bc, bd)$$

$$(a,b)(c,d) = (ac, bd)$$

Proposition 5.20. Låt R vara ett integritetsområde. Då är $Q(R)$ en kropp.

Bevis. Vi måste visa följande:

1. Additionen och multiplikationen bevarar ekvivalensklasserna.
2. Visa att ringaxiomen är uppfyllda. Nollan är $\overline{(0,1)}$ och ettan är $\overline{(1,1)}$.
3. Visa att $Q(R)$ är kommutativ, nollskild och att varje element $\overline{(a,b)}$ där $a \neq 0$ är inverterbart, närmare bestämt är interversen $\overline{(a,b)}^{-1} = \overline{(b,a)}$.

Vi måste först kontrollera att additionen och multiplikationen är väldefinierad, d.v.s. att de bevarar ekvivalensklasserna. Först kontrollerar vi att additionen är väldefinierad, d.v.s. det spelar ingen roll vilken representant från en ekvivalensklass vi tar, summan kommer alltid tillhöra samma ekvivalensklass. Så låt $(a,b) \sim (a',b')$ och $(c,d) \sim (c',d')$. Då har vi $ab' = a'b$ och $cd' = c'd$. Om vi adderar dessa olika talpar får vi:

$$(a,b) + (c,d) = (ad + bc, bd)$$

$$(a',b') + (c',d') = (a'd' + b'c', b'd')$$

Vi vill nu kontrollera att $(a,b)+(c,d) \sim (a',b')+(c',d')$, d.v.s.;

$$(ad+bc)b'd' = (a'd'+b'c')bd.$$

$$\begin{aligned}
(ad+bc)b'd' &= (ad)(b'd') + (bc)(b'd') && \text{(Distributivitet)}\\
&= (ab')(dd') + (cd')(bb') && \text{(Associativitet, kommutativitet)}\\
&= (a'b)(dd') + (c'd)(bb') && (ab' = a'b, cd' = c'd)\\
&= (a'd')(bd) + (b'c')(bd) && \text{(Associativitet, kommutativitet)}\\
&= (a'd'+b'c')bd. && \text{(Distributivitet)}
\end{aligned}$$

Vi har alltså visat att $(a,b)+(c,d) \sim (a',b')+(c',d')$!

På samma sätt vill vi kontrollera att

$$(a,b)\cdot(c,d) = (ac,bd) \sim (a'c',b'd') = (a',b')\cdot(c',d').$$

Detta är ekvivalent med att

$$acb'd' = a'c'bd$$

vilket följer direkt från att $(ab' = a'b) \wedge (cd' = c'd)$ (inklusive associativitet och kommutativitet).

Vi vill nu visa att $Q(R)$ tillsammans med ovanstående addition och multiplikation är en ring. Det additivt neutrala elementet är ekvivalensklassen av $(0,1)$ och det multiplikativt neutrala element är ekvivalensklassen av $(1,1)$. Att alla ringaxiom är uppfyllda kommer att följa av det faktum att R är ett integritetsområde (en kommutativ ring utan nolldelare). Detta är inte svårt, men tar lite tid, så vi hoppar över det.

Att $Q(R)$ är kommutativ är enkelt att se, det följer direkt från det faktum att R är kommutativ:

$$\overline{(a,b)}\cdot\overline{(c,d)} = \overline{(ac,bd)} = \overline{(ca,db)} = \overline{(c,d)}\cdot\overline{(a,b)}.$$

Nu vill vi bara visa att varje nollskilt element har en invers. Först visar vi att (a,b) är nollskild om och endast om a är nollskild:

$$(0,1) \sim (a,b) \Leftrightarrow 0\cdot b = a\cdot 1 \Leftrightarrow a = 0.$$

Den multiplikativa inversen till (a,b), där $a \neq 0$, är (b,a):

$$(a,b)(b,a) = (ab,ab) \sim (1,1).$$

Observera att vi måste ha $a \neq 0$ för att (b,a) ska vara ett element i $Q(R)$. Tillsist, eftersom $Q(R) \neq \{0\}$, då t.ex. $(1,1) \in Q(R) \setminus \{0\}$, har nu bevisat att $Q(R)$ är en kropp. □

5.3 Karakteristik

Definition 5.21. (i) Låt n vara ett positivt heltal. Vi definierar då $n \in R$ som summan av n stycken 1:or

$$n := \underbrace{1+1+\cdots+1}_{n}.$$

(ii) Låt n vara ett negativt heltal. Vi definierar då $n \in R$ som $-(-n)$, där $(-n)$ definieras som ovan.

Detta ger oss följande: Låt n vara ett positivt heltal och $a \in R$. Vi får då att $na \in R$ är summan av n stycken a

$$na := \underbrace{a + a + \cdots + a}_{n}.$$

Exempel 5.22. Titta på mängden av reella 2×2-matriser. Detta är en ring med matrisaddition och matrismultiplikation. Det multiplikativt neutrala elementet här är ju enhetsmatrisen! Så $n \in \mathrm{Mat}_2(\mathbb{R})$ är matrisen med talet n på diagonalen, och nollor överallt annars.

$$\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix}$$

Definition 5.23. *Karakteristiken* hos en ring R är det minsta positiva heltal n så att $na = 0$ för alla $a \in R$. Om inget sådant tal existerar så definieras karakteristiken som 0. Vi betecknar detta som $\mathrm{char}(R)$.

Exempel 5.24. • $\mathbb{Z}_3$ har karakteristik 3.

• $\mathbb{R}$ har karakteristik 0.

Sats 5.25. Låt n vara karakteristiken hos ett integritetsområde. Då är antingen $n = 0$ eller så är n ett primtal.

6 Irreducibla element och primelement

Nu ska vi titta på lite fler egenskaper som vi återfinner hos heltalen. Mer exakt egenskapen att om p är ett primtal så gäller

$$p|ab \Rightarrow p|a \vee p|b$$

samt

$$p = ab \Rightarrow a = \pm 1 \vee b = \pm 1.$$

Observera här att de enda inverterbara heltalen är just ± 1. Vi härmar dessa egenskaper och inför två nya definitioner. Men innan det behöver vi kika lite snabbt på delbarhet i allmänna ringar och associering. I det här avsnittet kommer i princip alla ringar vara integritetsområden!

6.1 Delbarhet i allmänna ringar och associering

Definition 6.1. Låt $a, b \in R$ vara två element i ett integritetsområde. Vi säger att a är *associerat* med b om det finns ett inverterbart element $c \in R$ så att $a = bc$.

Obs: eftersom 1 är inverterbart så är varje element i en ring associerat med sig själv! Hos heltalen är de enda distinkta talen som är associerade med varandra n och $-n$.

Exempel 6.2. Om vi kollar på $\mathbb{R}[x]$, ringen av reella polynom, så är två polynom p, q associerade med varandra om och endast om $p = \lambda q$ där $\lambda \in \mathbb{R} \setminus \{0\}$.

- $2x + 4$ och $x + 2$ i $\mathbb{R}[x]$ är associerade, eftersom $2x + 4 = 2(x + 2)$ och 2 är inverterbart i $\mathbb{R}$.
- $2x + 4$ och $x + 2$ i $\mathbb{Z}[x]$ är INTE associerade, eftersom $2x + 4 = 2(x + 2)$ och 2 är INTE inverterbart i $\mathbb{Z}$.
- Allmänt gäller det att två polynom p och q i $R[x]$, där R är ett integritetsområde, är associerade om och endast om $p = \lambda q$ där $\lambda \in R$ är inverterbart!

Det är faktiskt så att "$a \sim b \Leftrightarrow a$ är associerat med b" är en ekvivalensrelation!

- 1 är alltid inverterbart, så $a \sim a$.
- Om $a \sim b$ så finns det ett inverterbart element e så att $a = be$, men då gäller även $ae^{-1} = b$ vilket betyder att $b \sim a$.
- Om $a \sim b$ och $b \sim c$ så finns e, f inverterbara så att $a = be$ och $b = cf$. Men då gäller att $a = be = (cf)e = c(fe)$. Om e och f är inverterbara så är även fe det. Så $a \sim c$.

Definition 6.3. Låt R vara ett integritetsområde och $a, b \in R$. Vi säger att a *delar* b, $a|b$, om det finns ett $c \in R$ så att $ac = b$.

Givet ett element $a \in R$ kallas alla element som är associerade med 1 eller med a för a:s *triviala delare*.

Anmärkning 6.4. Observera att de element som är associerade med 1 är precis de inverterbara elementen!

6.2 Irreducibla element

Definition 6.5. Vi säger att ett icke-inverterbart element $a \in R$, där R är ett integritetsområde, är *irreducibelt* om det för alla $b, c \in R$ gäller att $a = bc$ medför att b eller c är inverterbart.

Vi kallar ett element som är en produkt av två icke-inverterbara element för *reducibelt*.

Proposition 6.6. Låt $a \in R$. Då är a irreducibel om och endast om a endast har triviala delare.

Bevis. Antag att a är irreducibelt och att $b|a$. Då finns det ett $c \in R$ så att $a = bc$. Eftersom a är irreducibelt så är någon av b och c inverterbara. Om b är inverterbart så är det en trivial delare eftersom det är associerat med 1. Om c är inverterbart så är b associerat med a och är därmed en trivial delare.

Antag istället att a bara har triviala delare och att $a = bc$ för två godtyckliga element $b, c \in R$. Men då är både b och c delare till a. Vi har nu två alternativ för både b och c: de kan antingen vara inverterbara eller associerade med a.

Om b är inverterbar (d.v.s. associerat med 1) så är vi klara. Om b istället är associerat med a så gäller $bd = a = bc$ för något inverterbart element d. Men eftersom vi är i ett integritetsområde så gäller då $d = c$, och alltså är c inverterbart. Detta visar att a är irreducibelt om a endast har triviala delare. □

Obs: om a inverterbart och $a = bc$, då är också b och c inverterbara: $1 = b(ca^{-1}) = (a^{-1}b)c$. Men precis som att ± 1 inte räknas som primtal vill vi inte säga att inverterbara element är irreducibla. På nästa föreläsning kommer vi prata mer om faktorisering i allmänna ringar och vi ser då att av precis samma anledning som för heltalen vill vi inte räkna inverterbara element som irreducibla.

Exempel 6.7. • För ett primtal p är $\pm p$ irreducibelt.

- 0 är inte irreducibelt. Om $R \neq \{0\}$ har vi $0 = 0 \cdot 0$ och 0 är inte inverterbart. Om $R = \{0\}$ så är $0 = 1$ inverterbart och då ej irreducibelt.
- $x + 1 \in \mathbb{Z}[x]$ är irreducibelt: Om $x + 1 = p(x)q(x)$ då måste en av polynomen ha grad 1 och det andra grad 0, eftersom $\deg(pq) = \deg(p) + \deg(q)$. Antag att $p(x) = ax + b$ och $q(x) = c$. Alltså har vi $x + 1 = (ax + b)c = acx + bc$ vilket betyder att $ac = 1$. Det implicerar att $q(x) = c = \pm 1$ och är då inverterbart!
- $x^2 - 1 \in \mathbb{Z}[x]$ är reducibelt, ty $x^2 - 1 = (x + 1)(x - 1)$ och varken $x + 1$ eller $x - 1$ är inverterbara.

Anmärkning 6.8. Det är mycket lättare att visa att ett element INTE är irreducibelt (d.v.s. reducibelt eller inverterbart). Om a inte är inverterbart så behöver vi bara hitta ett motexempel där $a = bc$ och varken b eller c är inverterbara.

Om vi vill visa att a är irreducibelt måste vi titta på ALLA MÖJLIGA b, c så att $a = bc$. Det räcker alltså INTE att bara hitta ETT exempel så att $a = bc$ och någon av b eller c är inverterbara. Detta går ju nämligen alltid att göra: $a = 1 \cdot a$ och 1 är inverterbart!

Sats 6.9. Om a är irreducibelt så är alla b som är associerat till a också irreducibla.

6.3 Primelement

Definition 6.10. Låt R vara ett integritetsområde. Vi kallar ett nollskilt icke-inverterbart element $a \in R$ för *primelement* (primt) om

$$a|bc \Rightarrow a|b \vee a|c,$$

för alla element $b, c \in R$.

Exempel 6.11. I $\mathbb{Z}$ är $\pm p$ irreducibelt och primt för varje primtal p.

Sats 6.12. Låt R vara ett integritetsområde. Då är alla primelement i R irreducibla.

Bevis. Antag att a är ett primelement i R och att $a = bc$. Eftersom a är nollskilt, så är också b, c nollskilda. Vi vill visa att b eller c är inverterbart. Eftersom att $a = bc$ så har vi att $a|bc$. Men eftersom a är primt måste $a|b$ eller $a|c$. Detta är ekvivalent med att det finns $m, n \in R$ så att $b = am$ eller $c = an$. Eftersom $a = bc$ får vi att

$$b = (bc)m = b(cm) \quad \vee \quad c = (bc)n = c(bn).$$

I den sista likheten använde vi att R är kommutativ. Eftersom att R är ett integritetsområde gäller $xz = yz \Rightarrow x = y$, om z är nollskild. Detta ger oss att

$$1 = cm \quad \vee \quad 1 = bn.$$

Men detta betyder att antingen är c inverterbart, eller så är b inverterbart. Alltså är a irreducibelt! □

Exempel 6.13. Det gäller dock INTE att alla irreducibla element är primelement! Vi visar detta med ett motexempel, vilket vi finner i ringen $\mathbb{Z}[i\sqrt{5}]$. Vi måste först visa att detta är en delring av $\mathbb{C}$ så vi kan dra slutsatsen att detta är ett integritetsområde. Vi kommer ihåg vår favoritsats:

- Vi kollar först att 0 och 1 ligger i $\mathbb{Z}[i\sqrt{5}]$. Det gör de!
- Vi kontrollerar att mängden är sluten under multiplikation, addition och additiv invers. Att mängden är sluten under addition och additiv invers är enkelt att se. Vi har även:

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = ac - 5bd + i\sqrt{5}(ad + bc).$$

Så $\mathbb{Z}[i\sqrt{5}]$ är en delring av $\mathbb{C}$ och eftersom $\mathbb{C}$ är ett integritetsområde så är även $\mathbb{Z}[i\sqrt{5}]$ det enligt en tidigare sats!

Nu vill vi visa att 2 är irreducibelt, d.v.s. att om $2 = xy$ så måste x eller y vara inverterbart och 2 är själv inte inverterbart. Att 2 inte är inverterbart följer av att 2 inte är inverterbart i $\mathbb{Z}$:

$$1 = 2(a + bi\sqrt{5}) = 2a + 2bi\sqrt{5}.$$

Men inga heltal a, b uppfyller denna ekvation.

Antag nu att

$$2 = (a + bi\sqrt{5})(c + di\sqrt{5}).$$

Titta nu på kvadraten av absolutbeloppen:

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Vi ser nu att både $(a^2 + 5b^2), (c^2 + 5d^2) \leq 4$ vilket betyder att $b, d = 0$. Vi får alltså att $2 = ac$ där a, c är heltal. Men då måste en av dem vara ± 1 och är alltså inverterbart i $\mathbb{Z}[i\sqrt{5}]$. Detta visar att 2 är irreducibelt.

Nu ska vi visa att 2 inte är primt i $\mathbb{Z}[i\sqrt{5}]$. Vi har

$$2|(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6,$$

Men 2 delar varken $1 + i\sqrt{5}$ eller $1 - i\sqrt{5}$: Antag att 2 delar $1 \pm i\sqrt{5}$. Då ska det finnas $a + bi\sqrt{5}$ så att $2(a + bi\sqrt{5}) = 2a + 2bi\sqrt{5} = 1 \pm i\sqrt{5}$. Men för att det ska gälla måste $2a = 1$ och $2b = \pm 1$. Men det finns inga heltal a, b så att detta gäller. Alltså är 2 inte primt!

7 Faktoriella ringar och Polynomringar

7.1 Faktoriella ringar

Så vi har hittills pratat om två egenskaper hos heltal som är speciella för primtal. Som ni vet från Aritmetikens fundamentalsats kan alla heltal faktoriseras som en produkt av primtal på ett entydigt sätt upp till ordning och en faktor ± 1. Det är inte alla ringar som har denna egenskap, utan de ringar som har denna egenskap kallar vi för en faktoriell ring.

Definition 7.1. Vi säger att en ring R är *faktoriell* om R är ett integritetsområde och varje nollskilt icke-inverterbart element $a \in R$ är en produkt av irreducibla element. Dessutom ska denna produkt vara unik upp till ordning av faktorerna samt upp till associering.

Unik upp till associering betyder att om vi har två faktoriseringar,

$$p_1 p_2 \dots p_n = a = q_1 q_2 \dots q_m,$$

där p_i och q_j är irreducibla, så är $m = n$ och för varje $i \in \{1, \dots, n\}$ finns precis ett $j \in \{1, \dots, m\}$ så att p_i och q_j är associerade.

Exempel 7.2. Följande är exempel på faktoriella ringar:

- $\mathbb{Z}$
- $\mathbb{Z}[x]$ och $\mathbb{C}[x]$
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Beviset till följande sats är lättare än man kan tro!

Sats 7.3. Alla kroppar är faktoriella.

Bevis. Först och främst är varje kropp ett integritetsområde. Vidare så är alla nollskilda element inverterbara, alltså är villkoret "varje nollskilt icke-inverterbart element $a \in R$ är en produkt av irreducibla element" ett tomt villkor som är automatiskt uppfyllt. □

Exempel 7.4. $\mathbb{Z}[i\sqrt{5}]$ är INTE en faktoriell ring: $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ där $2, 3, (1+i\sqrt{5}), (1-i\sqrt{5})$ är irreducibla men ingen av elementen är associerade till varandra.

Proposition 7.5. I en faktoriell ring R är varje irreducibelt element ett primelement.

Bevis. Antag att $a \in R$ är irreducibel och $a|bc$. Då finns det $x \in R$ så att $ax = bc$. Men i en faktoriell ring har vi *entydig* faktorisering, så den irreducibla faktorn a måste finns i faktoriseringen av (minst en av) b eller c. Men ett element y innehåller en irreducibel faktor a om och endast om a delar y. Alltså gäller $a|b$ eller $a|c$. Detta visar att alla irreducibla element är primelement. □

Anmärkning 7.6. Vi vet redan att i ett integritetsområde så är varje primelement irreducibelt. Propositionen säger alltså att mängden av primelement är precis samma som mängden irreducibla element!

Nu har vi tittat på lite olika typer av ringar och vi har följande kedja av inklusioner:

$$\text{Kroppar} \subsetneq \text{Faktoriella ringar} \subsetneq \text{Integritetsområden} \subsetneq \text{Kommutativa ringar}$$

- Kropp: $\mathbb{Q}$,
- Faktoriell ring men inte en kropp: $\mathbb{Z}$,
- Integritetsområde men inte en faktoriell ring: $\mathbb{Z}[i\sqrt{5}]$,
- Kommutativ ring men inte ett integritetsområde: $\mathbb{Z}_4$,
- Ring men inte en kommutativ ring: $M_n(\mathbb{R})$.

7.2 Polynomringar och definitioner

Nu ska vi titta lite mer på polynomringar och se vilka egenskaper hos koefficientringen som överförs till polynomringen.

Definition 7.7. Givet en kommutativ ring R så definierar vi *polynomringen* $R[x]$ som mängden av polynom i x med koefficienter i R, d.v.s. formella summor $\sum_{i=0}^{n} a_i x^i$ där $a_i \in R$ och $n < \infty$. Addition och multiplikation definieras via

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m} b_j x^j \right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Man måste såklart bevisa att detta är en ring, men det är inte svårt att visa. Gör det!

Exempel 7.8. Detta är exempel på två polynom i $\mathbb{Z}_4[x]$:

$$2x^2 + x + 3, \quad 2x^2 + 2$$

$$(2x^2 + x + 3) + (2x^2 + 2) = 4x^2 + x + 5 = x + 1$$

$$(2x^2 + x + 3)(2x^2 + 2) = 4x^4 + 2x^3 + 10x^2 + 2x + 6 = 2x^3 + 2x^2 + 2x + 2$$

- När ni tänker på variabeln x ska ni INTE tänka på det som ett element i ringen R, utan som en symbol som man kan addera och multiplicera. Däremot kan vi *utvärdera* polynomet, först då får vi ett element i ringen R.
- Två polynom är lika om deras koefficienter i R är lika. Så även om t.ex. x^3 och x i $\mathbb{Z}_3[x]$ alltid ger samma värde om vi utvärderar i ett element ses de som olika polynom!
- Vi kallar ett polynom i $R[x]$ konstant om det är ett element i R, d.v.s. endast består av en konstantterm. Observera att tex $x^3 - x \in \mathbb{Z}_3[x]$ alltid blir 0 om vi utvärderar det i $\mathbb{Z}_3$. Så som funktion $\mathbb{Z}_3 \to \mathbb{Z}_3$ är $x^3 - x$ konstant. Men det är INTE ett konstant polynom!

Definition 7.9. Givet ett polynom $p(x)$ så definierar vi *graden* av p som det högsta heltal d så att koefficienten framför x^d är nollskild. Vi definierar graden av nollpolynomet som $-\infty$. Vi betecknar graden av ett polynom p med $\deg(p)$, eller som i kompendiet, $\delta(p)$.

Den här gradfunktionen har nästan lika trevliga egenskaper för allmänna kommutativa ringar som för reella eller komplexa polynom.

- $\deg(p+q) \leq \max(\deg(p), \deg(q))$.
- $\deg(pq) \leq \deg(p) + \deg(q)$. Likhet gäller om $R[x]$ är ett integritetsområde.

Exempel 7.10. Vi kan jämföra med exemplet ovan. I det adderade och multiplicerade vi två polynom av grad 2 i $\mathbb{Z}_4[x]$.

- $(2x^2 + x + 3) + (2x^2 + 2) = 4x^2 + x + 5 = x + 1$, så summan har grad 1.
- $(2x^2 + x + 3)(2x^2 + 2) = 4x^4 + 2x^3 + 10x^2 + 2x + 6 = 2x^3 + 2x^2 + 2x + 2$, så produkten har grad 1, vilket är strikt mindre än summan av graderna hos faktorerna.

7.3 Rötter och Faktorsatsen

Definition 7.11. Vi säger att $a \in R$ är en *rot* till polynomet $p(x) \in R[x]$ om $p(a) = 0$.

Från Algebra I kommer ni (förhoppningsvis) ihåg Faktorsatsen. Den gäller faktiskt för även för generella polynomringar.

Sats 7.12 (Faktorsatsen)**.** Ett polynom $p \in R[x]$ har en rot $a \in R$ om och endast om $p(x) = (x-a)q(x)$ för något $q(x) \in R[x]$.

Bevis. Om $p(x) = (x-a)q(x)$ så är uppenbarligen $p(a) = 0$. Antag nu istället att $p(a) = 0$. Vi vill visa att $p(x) = (x-a)q(x)$ för något polynom $q(x)$. Vi kan skriva

$$p(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n.$$

Då är

$$0 = p(a) = b_0 + b_1 a + b_2 a^2 + \cdots + b_n a^n,$$

vilket ger oss likheten

$$b_0 = -b_1 a - b_2 a^2 - \cdots - b_n a^n$$

Om vi i uttrycket för $p(x)$ substituerar b_0 med högerledet får vi:

$$p(x) = b_1(x-a) + b_2(x^2 - a^2) + \cdots + b_n(x^n - a^n).$$

Men för varje k har vi: $x^k - a^k = (x-a)(x^{k-1} + ax^{k-2} + \cdots + a^{k-2}x + a^{k-1})$. Detta ger oss att

$$p(x) = (x-a)(b_1 + b_2(x+a) + \cdots + b_n(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1})).$$

Vi har nu visat att $p(x) = (x-a)q(x)$ för $q(x) = b_1 + b_2(x+a) + \cdots + b_n(x^{n-1} + ax^{n-2} + \cdots + a^{n-2}x + a^{n-1}) \in R[x]$. □

Även om satsen är en väldigt bra sats, så är situationen inte riktigt så bra som man kunde hoppas.

Exempel 7.13. Titta på $2x \in \mathbb{Z}_4[x]$. Det finns två rötter: 0 och 2, så enligt Faktorsatsen är både x och $(x-2)$ faktorer i polynomet. Men $2x \neq x(x-2)g(x)$ för alla möjliga polynom $q(x) \in \mathbb{Z}_4[x]$.

För att undvika såna här konstigheter måste vi kräva att ringen är ett integritetsområde! Då får vi följande sats:

Sats 7.14 (Faktorsatsen för integritetsområden)**.** Låt $p \in R[x]$, där R är ett integritetsområde. Om a_i, $1 \leq i \leq n$, är parvis olika rötter till $p(x)$ så följer det att

$$p(x) = q(x)(x-a_1)(x-a_2)\dots(x-a_n)$$

för något polynom $q(x) \in R[x]$.

Bevis. Enligt Faktorsatsen kan vi skriva

$$f(x) = q_n(x)(x-a_n)$$

för något $q_n(x) \in R[x]$. Vi har då

$$0 = f(x_i) = q_n(a_i)(a_i - a_n)$$

för alla $i \leq n-1$. Eftersom $a_i \neq a_n$ och R är ett integritetsområde så måste $q_n(a_i) = 0$ för alla $i \leq n-1$. Vi kan då repetera detta argument och hitta $q_{n-1}(x)$ som uppfyller $q_n(x) = q_{n-1}(x)(x-a_{n-1})$ och som har nollställen a_i för $i \leq n-2$. Om vi upprepar detta för alla rötter får vi tillslut att

$$p(x) = q(x)(x-a_1)(x-a_2)\dots(x-a_n)$$

för något polynom $q(x) \in R[x]$. □

Exempel 7.15. • $2x \in \mathbb{C}[x]$ har en rot $x = 0$. Här är $q(x) = 2$

- $x^2 - 1 \in \mathbb{Z}_3[x]$ har två rötter, $x = 1$ och $x = 2$. Vi kontrollerar: $(x-1)(x-2) = x^2 - 3x + 2 = x^2 - 1$. Här är $q(x) = 1$.
- $x^4 - 1 \in \mathbb{R}[x]$ har två rötter, $x = \pm 1$. Vi får att $x^4 - 1 = (x-1)(x+1)(x^2+1)$. Här är $q(x) = x^2 + 1$.

Sats 7.16. En ring R är ett integritetsområde om och endast om $R[x]$ är ett integritetsområde.

Bevis. Om $R[x]$ är ett integritetsområde så måste R också vara det, eftersom att R är en delring av $R[x]$. Antag nu att R är ett integritetsområde och att $p(x), q(x) \neq 0$. Vi får då:

$$p(x) \cdot q(x) = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right) x^k,$$

där $a_n, b_m \neq 0$. Eftersom R saknar nolldelare så är $a_n b_m \neq 0$. Men vi får då att

$$p(x) \cdot q(x) = a_n b_m x^{n+m} + \sum_{k=0}^{n+m-1} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Eftersom att det inte finns några andra termer av grad $n+m$ som kan kancellera $a_n b_m x^{n+m}$ måste vi ha $p(x) \cdot q(x) \neq 0$. Alltså är varje produkt av nollskilda polynom igen ett nollskilt polynom. Alltså saknar $R[x]$ nolldelare. Då $R[x]$ även är kommutativ (eftersom R är det) så är $R[x]$ ett integritetsområde. □

Anmärkning 7.17. I beviset såg vi även att

$$\deg(pq) = \deg(p) + \deg(q).$$

7.4 Faktoriella polynomringar

Nu vill vi fråga oss när $R[x]$ är faktoriell. Vi har följande resultat:

Sats 7.18 (Gauss, 1801)**.** Om R är faktoriell så är $R[X]$ faktoriell.

Beviset är svårt och kan inte göras med de tekniker vi lär oss i den här kursen. Däremot kommer vi i slutet av kursen kunna bevisa följande specialfall (kom ihåg att varje kropp är faktoriell):

Sats 7.19. Om K är en kropp, så är $K[x]$ faktoriell.

8 Homomorfismer och isomorfismer

8.1 Homomorfismer

Hittills har vi pratat massa olika slags ringar och tittat på hur de hänger ihop. Nu vill vi istället titta på avbildningar mellan ringar. I olika kurser har ni hunnit se lite olika speciella funktioner. I Envariabelanalys tittade ni på kontinuerliga funktioner från $\mathbb{R}$ till $\mathbb{R}$. En viktig egenskap hos dem är att de bevarar gränsvärden, d.v.s. $\lim_{n\to\infty} f(a_n) = f(\lim_{n\to\infty} a_n)$. I Linjär algebra tittade ni på vektorrum som är en slags linjär struktur, d.v.s. vi kan addera element och multiplicera med skalärer. I dessa kurser var linjära avbildningar mellan vektorrum extra viktiga eftersom att de bevarade lineariteten hos vektorrummen. Så de avbildningar vi vill titta på är de som bevarar ringstrukturen. Vi vill också bestämma oss för när två ringa ska betraktas som lika.

Definition 8.1. En funktion $f : R \to S$ mellan två ringar R, S kallas för en *ringhomomorfism* om det för alla $a, b \in R$ gäller att

(i) $f(a +_R b) = f(a) +_S f(b)$,

(ii) $f(a \cdot_R b) = f(a) \cdot_S f(b)$,

(iii) $f(1_R) = 1_S$.

Anmärkning 8.2. Eftersom vi endast tittar på ringar i denna kurs, kommer vi säga homomorfism för ringhomomorfism. Det finns andra homomorfismer för andra typer av algebraiska strukturer (grupper, algebror, moduler etc.)

Anmärkning 8.3. En homomorfism avbildar alltid 0_R på 0_S:

$$f(a) = f(a + 0_R) = f(a) + f(0_R) \Rightarrow 0_S = f(0_R)$$

enligt kancelleringslagen för addition. Men vi har inte någon sådan kancelleringslag för multiplikation i allmänna ringar, därför behöver vi lägga till kravet $f(1_R) = 1_S$ i definitionen.

Dessutom gäller $f(-a) = -f(a)$ eftersom

$$0 = f(a + (-a)) = f(a) + f(-a) \Rightarrow -f(a) = f(-a).$$

Exempel 8.4. • Identitetsfunktionen på em ring R är en ringhomomorfism, d.v.s. $\mathrm{Id} : R \to R, x \mapsto x$.

- Konjugering med ett inverterbart element $a \in R$, d.v.s. $f_a : R \to R, x \mapsto a^{-1}xa$, är en ringhomomorfism:
  - $f_a(x + y) = a^{-1}(x + y)a = a^{-1}xa + a^{-1}ya = f_a(x) + f_a(y)$,
  - $f_a(xy) = a^{-1}(xy)a = a^{-1}xaa^{-1}ya = f_a(x)f_a(y)$,
  - $f_a(1) = a^{-1}1a = 1$.
- Om vi bara multiplicerar med $a \neq 1$ från ena sidan så får vi INTE en ringhomomorfism. Enklast att se detta är genom $1 \mapsto a \neq 1$.

- Låt R vara en kommutativ ring, $a \in R$ och titta på $ev_a : R[x] \to R, p(x) \mapsto p(a)$. Detta är en ringhomomorfism:
  - $ev_a(p+q) = (p+q)(a) = p(a) + q(a) = ev_a(p) + ev_a(q)$,
  - $ev_a(pq) = (pq)(a) = p(a)q(a) = ev_a(p)ev_a(q)$,
  - $ev_a(1) = 1$.
- Eftersom varje heltal n kan ses som ett element i en ring R har vi en ringhomomorfism $f : \mathbb{Z} \to R, n \mapsto n$. Kontrollera att detta är en ringhomomorfism!
- $f : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto \overline{a}$ är en ringhomomorfism.
- Det existerar ingen ringhomomorfism från $\mathbb{Z}_2$ till $\mathbb{Z}_3$. Antag att det fanns en sådan ringhomomorfism, då måste $f(0) = 0$ och $f(1) = 1$. Men $f(0) = f(1+1) = f(1)+f(1) = 1+1 = 2 \neq 0$. Motsägelse!
- $f : \mathbb{R} \to \mathbb{C}, a \mapsto a + 0i$ är en ringhomomorfism.
- Mer allmänt: Om S är en delring till R så har vi alltid en inklusionshomomorfism: $f : S \to R, x \mapsto x$.
- $f : \mathbb{R} \to \mathbb{C}, a \mapsto 0 + ai$ är INTE en ringhomomorfism. T.ex. så avbildas inte 1 i $\mathbb{R}$ på 1 i $\mathbb{C}$.

8.2 Mono-, epi- och isomorfismer

Definition 8.5. Låt $f : R \to S$ vara en ringhomomorfism. Vi kallar f för en:

(i) *epimorfism* om $f : R \to S$ är surjektiv,

(ii) *monomorfism* om $f : R \to S$ är injektiv,

(iii) *isomorfism* om $f : R \to S$ är bijektiv.

Exempel 8.6. • $\mathbb{Z} \to \mathbb{Z}_n$ är en epimorfism, eftersom den är surjektiv. Men då $0 \mapsto \overline{0}$ och $n \mapsto \overline{n} = \overline{0}$ så är det inte en injektion, d.v.s. inte en monomorfism.

- $f : \mathbb{Z} \to \mathbb{Q}, n \mapsto \frac{n}{1}$ är en monomorfism, men inte en epimorfism.

Kommer ni ihåg när vi pratade om bråkkroppen av en ring R. Då sa jag att det finns en delring av $Q(R)$ som beter sig precis som R, men elementen är egentligen inte samma. Bråkkroppen innehåller *par* av element av R, så ringarna kan omöjligen vara samma, men additionen och multiplikationen fungerar likadant. På liknande sätt beter sig bråkkroppen av $\mathbb{Z}$ precis som $\mathbb{Q}$. Det vi vill göra nu är att på ett matematiskt sätt formulera "beter sig likadant som". Detta gör vi genom isomorfi!

Definition 8.7. Två ringar R och S är *isomorfa* om det existerar en isomorfism $f : R \to S$. Vi skriver $R \cong S$.

Sats 8.8. Om en ringhomomorfism $f : R \to S$ är bijektiv och så är f^{-1} också är en ringhomomorfism.

Bevis. Om $x, y \in S$ är två godtyckliga element så finns det precis två element $x', y' \in R$ så att $f(x') = x \Leftrightarrow f^{-1}(x) = x'$ och $f(y') = y \Leftrightarrow f^{-1}(y) = y'$.

(i)

$$\begin{aligned} f^{-1}(x+y) &= f^{-1}(f(x') + f(y')) \\ &\quad [f \text{ är en homomorfism}] \\ &= f^{-1}(f(x'+y')) \\ &\quad [f^{-1} \circ f = \mathrm{Id}] \\ &= x' + y' \\ &= f^{-1}(x) + f^{-1}(y). \end{aligned}$$

(ii)

$$\begin{aligned} f^{-1}(xy) &= f^{-1}(f(x')f(y')) \\ &\quad [f \text{ är en homomorfism}] \\ &= f^{-1}(f(x'y')) \\ &\quad [f^{-1} \circ f = \mathrm{Id}] \\ &= x'y' \\ &= f^{-1}(x)f^{-1}(y). \end{aligned}$$

(iii) $f^{-1}(1_S) = 1_R$ eftersom $f(1_R) = 1_S$.

Detta visar att även f^{-1} uppfyller villkoren för en homomorfism. □

Anmärkning 8.9. Morfism är ett väldigt generellt begrepp, vilket bland annat används inom kategoriteori. Det finns exempel där ovanstående sats inte gäller, d.v.s. vi kan ha en bijektiv morfism, där inversen inte är en morfism. I detta fall måste vi lägga till detta som krav i definitionen av en isomorfism. Detta händer bland annat för något som kallas topologiska rum. Men detta behöver ni inte oroa er för än så länge!

Exempel 8.10. • Varje ring är isomorf med sig själv eftersom att identitetsmorfismen är en isomorfism.

- $\mathbb{Q}$ är isomorf med $Q(\mathbb{Z})$ via $f : \mathbb{Q} \to Q(\mathbb{Z}), \frac{a}{b} \mapsto (a, b)$. Vi kontrollerar att detta stämmer.
  - Funktionen är väldefinierad eftersom att om $\frac{a}{b} = \frac{c}{d}$ så är $ad = bc$ och då är även $f(\frac{a}{b}) = (a, b) = (c, d) = f(\frac{c}{d})$.
  - $f(\frac{a}{b} + \frac{c}{d}) = f(\frac{ad+bc}{bd}) = (ad + bc, bd) = (a, b) + (c, d) = f(\frac{a}{b}) + f(\frac{c}{d})$.
  - $f(\frac{a}{b}\frac{c}{d}) = f(\frac{ac}{bd}) = (ac, bd) = (a, b)(c, d) = f(\frac{a}{b})f(\frac{c}{d})$.
  - $f(1) = f(\frac{1}{1}) = (1, 1)$. Så f är en ringhomomorfism.
  - f är surjektiv eftersom att $\forall (a, b) \in Q(\mathbb{Z})$ så gäller $\frac{a}{b} \in \mathbb{Q}$ (viktigt att $b \neq 0$) och $f(\frac{a}{b}) = (a, b)$.

– f är injektiv eftersom att om $f(\frac{a}{b}) = (a, b) = (c, d) = f(\frac{c}{d})$ så är $ad = bc$ enligt definitionen av $Q(\mathbb{Z})$. Men detta betyder att $\frac{a}{b} = \frac{c}{d}$. f är alltså bijektiv.

Vi har nu visat att f är en isomorfism och $\mathbb{Q}$ och $Q(\mathbb{Z})$ är alltså isomorfa.

- Antag att $R \cong T$ och $S \cong U$. Då är $R \times S \cong T \times U$. För att visa detta använder vi det faktum att det finns två isomorfismer, $f : R \to T$ och $g : S \to U$. Vi kan nu skapa en ny funktion $h : R \times S \to T \times U$ via $(r, s) \mapsto (f(r), g(s))$.

  Nu kan vi visa att detta är en isomorfism! Först visar vi att det är en homomorfism:

$$\begin{aligned} h(r + r', s + s') &= (f(r + r'), g(s + s')) \\ &= (f(r) + f(r'), g(s) + g(s')) \\ &= (f(r), g(s)) + (f(r'), g(r')) \\ &= h(r, s) + h(r', s'). \end{aligned}$$

$$\begin{aligned} h(r \cdot r', s \cdot s') &= (f(r \cdot r'), g(s \cdot s')) \\ &= (f(r) \cdot f(r'), g(s) \cdot g(s')) \\ &= (f(r), g(s)) \cdot (f(r'), g(r')) \\ &= h(r, s) \cdot h(r', s'). \end{aligned}$$

$$\begin{aligned} h(1, 1) &= (f(1), g(1)) \\ &= (1, 1). \end{aligned}$$

  Sedan kan vi visa att funktionen är surjektiv. Låt $(t, u) \in T \times U$. Då finns $r \in R$ och $s \in S$ så att $f(r) = t$ och $g(s) = u$ eftersom både f och s är surjektiva. Men då är $h(r, s) = (t, u)$, och alltså är även h surjektiv.

  Till sist kan vi visa att h är injektiv. Antag att $h(r, s) = h(r', s')$. Det betyder att $(f(r), g(s)) = (f(r'), g(s'))$, och då måste $f(r) = f(r')$ och $g(s) = g(s')$. Eftersom f och g är injektiva, så är $r = r'$ och $s = s'$, vilket betyder att $(r, s) = (r', s')$. Detta betyder att h är injektiv.

  Nu har vi visat att h är en isomorfism från $R \times S$ till $T \times U$.

Anmärkning 8.11. Isomorfi, $\cong$, är en ekvivalensrelation.

Anmärkning 8.12. Att det finns en isomorfism mellan två ringar R och S betyder att R och S är ekvivalenta som ringar och det som är skillnaden är beteckningen av elementen i respektive ring. Detta innebär att de som algebraiska strukturer är ”samma”. Vilket återspeglas bland annat i följande resultat.

Sats 8.13. Låt $f : R \to S$ vara en isomorfism. Då gäller

- R är kommutativ $\Leftrightarrow$ S är kommutativ;
- R är ett integritetsområde $\Leftrightarrow$ S är ett integritetsområde;
- R är faktoriell $\Leftrightarrow$ S är faktoriell;

- R är en kropp $\Leftrightarrow$ S är en kropp;
- $|R| = |S|$;
- $\text{char}(R) = \text{char}(S)$.

På samma sätt får vi följande resultat:

Sats 8.14. Låt $f : R \to S$ vara en isomorfism. Då gäller

- a är inverterbar i $R \Leftrightarrow f(a)$ är inverterbar i S,
- a är irreducibel i $R \Leftrightarrow f(a)$ är irreducibel i S,
- a är primt i $R \Leftrightarrow f(a)$ är primt i S,
- a är en nolldelare i $R \Leftrightarrow f(a)$ är en nolldelare i S.

Bevis. Vi visar att a är inverterbar i $R \Leftrightarrow f(a)$ är inverterbar i S, resterande delar lämnas som en övning. Eftersom även $f^{-1} : S \to R$ är en isomorfism så räcker det att visa att a är inverterbar i $R \Rightarrow f(a)$ är inverterbar i S. Detta eftersom vi helt enkelt kan ersätta f med f^{-1} i utsagan.

Då a är inverterbar existerar det en invers $a^{-1} \in R$. Vi påstår nu att $f(a^{-1})$ är en invers till $f(a)$ i S.

$$\begin{aligned} f(a)f(a^{-1}) &= f(aa^{-1}) \\ &= f(1_R) \\ &= 1_S. \end{aligned}$$

Detta visar att $f(a) \in S$ är inverterbar om och endast om $a \in R$ är inverterbar. □

8.3 Bilden och kärnan av en homomorfism

Definition 8.15. Låt $f : R \to S$ vara en ringhomomorfism. Vi definierar

- $\text{Im}(f) := \{f(r) \mid r \in R\}$, och kallas *bilden* av R i S under f,
- $\text{Ker}(f) := \{r \in R \mid f(r) = 0\}$, och kallas *kärnan* av f.

Sats 8.16. $\text{Im}(f) \subseteq S$ är en delring av S.

Bevis. Vi använder Sats 4.13:

(i) Om $a, b \in \text{Im}(f)$ så finns det $x, y \in R$ så att $f(x) = a$ och $f(y) = b$. Då gäller

$$a + b = f(x) + f(y) = f(x + y) \in \text{Im}(f)$$

och

$$ab = f(x)f(y) = f(xy) \in \text{Im}(f).$$

Dessutom har vi att

$$f(-x) = -f(x) = -a \in \text{Im}(f).$$

(ii) $f(0_R) = 0_S, f(1_R) = 1_S \in \mathrm{Im}(f)$.

Alltså är $\mathrm{Im}(f)$ en delring av S. □

Sats 8.17. Om $f : R \to S$ är en monomorfism så är $\mathrm{Im}(f) \cong R$.

Bevis. Vi vet redan att $\mathrm{Im}(f)$ är en (del)ring och enligt antagande är f injektiv. Från definitionen av $\mathrm{Im}(f)$ så ser vi att f är en surjektion från R till $\mathrm{Im}(f)$. □

Sats 8.18. En ringhomomorfism $f : R \to S$ är en monomorfism om och endast om $\mathrm{Ker}(f) = \{0_R\}$.

Bevis. Vi antar först att f är en monomorfism. Eftersom att varje homomorfism av bildar 0_R på 0_S så har vi alltid $\{0\} \subseteq \mathrm{Ker}(f)$. Men eftersom att f är injektiv kan inget annat element avbildas på 0_S, alltså är $\{0\} = \mathrm{Ker}(f)$.

Antag nu istället att $\{0\} = \mathrm{Ker}(f)$. Om vi för två element $x, y \in R$ har $f(x) = f(y)$ så implicerar detta att $0 = f(x) - f(y) = f(x - y)$. Men då ligger $x - y \in \mathrm{Ker}(f)$ och då måste $x - y = 0 \Leftrightarrow x = y$. Alltså är f injektiv och således en monomorfism. □

Anmärkning 8.19. Såklart gäller $\mathrm{Im}(f) = S$ om och endast om f är surjektiv, enligt definitionen av bilden och surjektivitet.

Exempel 8.20. Låt $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$ definieras via $\varphi(p(x)) = p(x^2)$. Detta kan man enkelt visa är en ringhomomorfism. Bilden $\mathrm{Im}(\varphi) = \mathbb{R}[x^2]$, d.v.s. reella polynom med endast jämna exponenter. Kärnan $\mathrm{Ker}(\varphi) = \{0\}$, alltså är avbildningen injektiv. Men det betyder att $\mathbb{R}[x] \cong \mathbb{R}[x^2]$ enligt Sats 8.17.

9 Kinesiska restsatsen som ringisomorfi och introduktion till ideal

9.1 Kinesiska restsatsen som isomorfi

På den här föreläsningen ska vi använda Kinesiska restsatsen till att avgöra när vi har en isomorfi mellan $\mathbb{Z}_m$ och $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Vi påminner oss först om vad satsen säger:

Sats 9.1 (Kinesiska restsatsen)**.** Systemet av kongruenser

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

där $m_1, m_2, \ldots, m_r$ är parvis relativt prima, har en unik lösning modulo $m_1 m_2 \cdot \ldots \cdot m_r$. Detta betyder att det finns en lösning, och om x_0 och x_1 är två lösningar så är $x_0 \equiv x_1 \pmod{m_1 m_2 \cdot \ldots \cdot m_r}$.

Lemma 9.2. Låt R och S vara två ringar. Då gäller

$$\operatorname{char}(R \times S) = \operatorname{mgm}(\operatorname{char}(R), \operatorname{char}(S)).$$

Bevis. Låt $k = \operatorname{mgm}(\operatorname{char}(R), \operatorname{char}(S))$. Då gäller $k \cdot (r, s) = (kr, ks) = 0$ för alla $(r, s) \in R \times S$ eftersom k är en multipel av både $\operatorname{char}(R)$ och $\operatorname{char}(S)$. Det betyder att

$$\operatorname{char}(R \times S) \leq k.$$

Antag att $j < \operatorname{mgm}(\operatorname{char}(R), \operatorname{char}(S))$. Då är j antingen inte en multipel av $\operatorname{char}(R)$ eller inte en multipel av $\operatorname{char}(S)$. Vi kan utan att förlora allmängiltighet anta att j inte är en multipel av $\operatorname{char}(R)$. Det betyder att $j = q \cdot \operatorname{char}(R) + x$ där $0 < x < \operatorname{char}(R)$. Låt (r, s) vara ett godtyckligt element i $R \times S$. Om vi multiplicerar detta element med j så får vi:

$$\begin{aligned} j \cdot (r, s) &= (jr, js) \\ &= ((q \cdot \operatorname{char}(R) + x)r, js) \\ &= ((q \cdot \operatorname{char}(R) \cdot r + xr, js) \\ &= (0 + xr, js) \\ &= (xr, js) \end{aligned}$$

Men då $0 < x < \operatorname{char}(R)$ så gäller $xr \neq 0$, och därför gäller även $j \cdot (r, s) \neq (0, 0)$. Alltså är $j \neq \operatorname{char}(R \times S)$. Detta visar att

$$\operatorname{char}(R \times S) = \operatorname{mgm}(\operatorname{char}(R), \operatorname{char}(S)).$$

□

Sats 9.3. Låt $m, n \in \mathbb{Z}_{>1}$. Då gäller $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ om och endast om m och n är relativt prima.

Bevis. Antag först att m och n inte är relativt prima. Då gäller

$$\operatorname{mgm}(m, n) = \frac{mn}{\operatorname{sgd}(m, n)} < mn.$$

Detta ger oss följande:

$$\begin{aligned}\operatorname{char}(\mathbb{Z}_m \times \mathbb{Z}_n) &= \operatorname{mgm}(\operatorname{char}(\mathbb{Z}_m), \operatorname{char}(\mathbb{Z}_n)) = \operatorname{mgm}(m, n) \\ &< mn = \operatorname{char}(\mathbb{Z}_{mn}).\end{aligned}$$

Men karakteristik är en egenskap som bevaras under isomorfi, vilket betyder att ringarna inte är isomorfa då deras karakteristik inte är samma.

Antag nu att m och n är relativt prima. Vi vill definiera en avbildning $\varphi : \mathbb{Z}_{mn} \to Z_m \times \mathbb{Z}_n$ via $x + nm\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$. Vi behöver visa att φ är:

1. väldefinierad,
2. en ringhomomorfism,
3. bijektiv

Vi visar först att avbildningen är väldefinierad, d.v.s.

$$x + mn\mathbb{Z} = y + mn\mathbb{Z} \Rightarrow (x + m\mathbb{Z}, x + n\mathbb{Z}) = (y + m\mathbb{Z}, y + n\mathbb{Z}).$$

Kom ihåg att $(a, b) = (c, d)$ om och endast om $a = c \wedge b = d$ i en kartesisk produkt. Det är alltså egentligen två implikationer vi behöver visa. Implikationen

$$x + mn\mathbb{Z} = y + mn\mathbb{Z} \Rightarrow x + m\mathbb{Z} = y + m\mathbb{Z}$$

följer från att $mn|(x - y) \Rightarrow m|(x - y)$. På samma sätt följer det att

$$x + mn\mathbb{Z} = y + mn\mathbb{Z} \Rightarrow x + n\mathbb{Z} = y + n\mathbb{Z}.$$

Tillsammans visar detta att följande implikation är sann:

$$x + mn\mathbb{Z} = y + mn\mathbb{Z} \Rightarrow (x + m\mathbb{Z}, x + n\mathbb{Z}) = (y + m\mathbb{Z}, y + n\mathbb{Z}).$$

Alltså är avbildningen väldefinierad.

Att avbildningen är en ringhomomorfism följer direkt från definitionen av addition och multiplikation av restklasser och i produkter av ringar. Att avbildningen är bijektiv följer från Kinesiska restsatsen. Låt $(a + m\mathbb{Z}, b + n\mathbb{Z}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, vi vill nu visa att det finns $x \in \mathbb{Z}_{mn}$ som avbildas på detta element. Detta kan formleras med hjälp av följande system av kongruenser:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Enligt Kinesiska restsatsen finns det ett sådant element x, alltså är φ surjektiv. Kinesiska restsatsen säger även att det är unikt modulo mn, vilket innebär att precis ett element träffar $(a + m\mathbb{Z}, b + n\mathbb{Z})$. Detta är precis definitionen av att vara injektiv. Alltså är φ en isomorfism! □

Exempel 9.4. • $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

• $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$

• $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$

• $\mathbb{Z}_{12} \ncong \mathbb{Z}_2 \times \mathbb{Z}_6$

Korollarium 9.5. Låt $n \in \mathbb{Z}_{>1}$ och $n = p_1^{k_1} p_2^{k_2} \cdot \cdots \cdot p_r^{k_r}$ en primtalsfaktorisering av n där $p_i \neq p_j$ för $i \neq j$. Då är $\mathbb{Z}_n \cong \prod_{j=1}^{r} \mathbb{Z}_{p_j^{k_j}}$.

Bevis. Vi bevisar detta med hjälp av induktion med avseende på antalet distinkta primtalsfaktorer, d.v.s. med avseende på r. Basfallet $r = 1$ är trivialt (eftersom varje ring är isomorf med sig själv).

För induktionssteget antar vi att påståendet gäller för $r - 1$. Vi kan skriva

$$n = \left(p_1^{k_1} p_2^{k_2} \cdot \cdots \cdot p_{r-1}^{k_{r-1}}\right) \cdot p_r^{k_r}.$$

Eftersom $m := p_1^{k_1} p_2^{k_2} \cdot \cdots \cdot p_{r-1}^{k_{r-1}}$ och $p_r^{k_r}$ är relativt prima, gäller enligt Sats 9.3 att $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_{p_r^{k_r}}$. Enligt induktionsantagandet gäller dock $Z_m \cong \prod_{j=1}^{r-1} \mathbb{Z}_{p_j^{k_j}}$. Alltså har vi isomorfin $\mathbb{Z}_n \cong \prod_{j=1}^{r} \mathbb{Z}_{p_j^{k_j}}$. □

Exempel 9.6. • $\mathbb{Z}_{60} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5$

• $\mathbb{Z}_{60} \ncong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

9.2 Ideal

På förra föreläsningen visade vi att bilden, $\mathrm{Im}(f) \subseteq S$, av en homomorfism $f : R \to S$ är en delring, men vilken typ av struktur har kärnan, $\mathrm{Ker}(f) \subseteq R$?

Anmärkning 9.7. Låt $f : R \to S$ vara en homormofism. Då är följande sant:

• Om $a, b \in \mathrm{Ker}(f)$ så gäller $a + b \in \mathrm{Ker}(f)$:

$$f(a + b) = f(a) + f(b) = 0 + 0 = 0.$$

• Om $a \in \mathrm{Ker}(f)$ och $r \in R$ så gäller $ar, ra \in \mathrm{Ker}(f)$:

$$f(ar) = f(a)f(r) = 0 \cdot f(r) = 0,$$

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0.$$

Men detta liknar väldigt mycket definitionen av ett ideal i $\mathbb{Z}$!

Vi inför följande definition:

Definition 9.8. Låt I vara en delmängd av en ring R. Vi säger att I är ett *ideal* i R om

(i) I är icke-tom,

(ii) $a, b \in I \Rightarrow a + b \in I$,

(iii) $a \in I, r \in R \Rightarrow ar, ra \in I$.

Om $R = \mathbb{Z}$ så är detta precis definitionen av ett ideal i $\mathbb{Z}$ som vi arbetat med tidigare.

Anmärkning 9.9. • Om I är ett ideal så ligger alltid 0 i I. Detta eftersom I är icke-tom och därför innehåller ett element x, och $0 \cdot x = 0 \in I$.

• $\{0\}$ och R är alltid ideal i R, dessa kallas de *triviala* idealen.

Exempel 9.10. I $\mathbb{Z}_6$ har vi, förutom de triviala idealen, de två idealen $\{\overline{0}, \overline{3}\}$ och $\{\overline{0}, \overline{2}, \overline{4}\}$. Vi kan lätt kontrollera att de faktiskt är ideal.

Sats 9.11. Om $f : R \to S$ är en homomorfism så är $\mathrm{Ker}(f)$ ett ideal.

Anmärkning 9.12. Om $1 \in I$ så är $I = R$ eftersom att $r \cdot 1 = r \in I$ för alla $r \in R$. Detta gäller även ifall $a \in I$ och a är inverterbart. Detta eftersom att vi då får $a^{-1} \cdot a = 1 \in I$.

Sats 9.13. Hos en kropp är de triviala idealen de enda idealen.

Bevis. Antag K är en kropp och $I \subseteq K$ ett ideal. Om $I \neq \{0\}$ så innehåller I ett nollskilt element a. Eftersom att K är en kropp är a inverterbart. Enligt anmärkningen ovanför så är då $I = K$. □

Sats 9.14. Låt I och J vara ideal i en ring R. Då är deras snitt $I \cap J$ ett ideal.

Bevis. Vi vill visa att $I \cap J$ är en icke-tom delmängd av R som är sluten under addition och multiplikation med ringelement. Till och börja med så ligger 0 i både I och J, och därför även i deras snitt. Snittet är alltså icke-tomt.

Antag att $a, b \in I \cap J$. Då ligger a, b i både I och J. Eftersom dessa är ideal så ligger $a + b$ i båda dessa delmängder, och därför även deras snitt. Desamma gäller ar, ra, där $a \in I \cap J$ och $r \in R$. Detta visar att $I \cap J$ är ett ideal i R. □

9.3 Olika typer av ideal

När vi pratade om ideal i $\mathbb{Z}$ kom vi fram till att $I \cup J$ inte alltid var ett ideal, men att $\{ax + by \mid x, y \in \mathbb{Z}\}$ var ett ideal. Det här ideal är det minsta idealet som innehåller både a och b.

Definition 9.15. Låt $a_1, a_2, \ldots, a_n \in R$, där R är en kommutativ ring. Vi definierar idealet som *genereras* av $a_1, a_2, \ldots, a_n$ som

$$\langle a_1, a_2, \ldots, a_n \rangle = Ra_1 + Ra_2 + \cdots + Ra_n$$

$$:= \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

Sats 9.16. Låt $a_1, a_2, \ldots, a_n \in R$, där R är en kommutativ ring. Då är $\langle a_1, a_2, \ldots, a_n \rangle$ det minsta idealet som innehåller elementen $a_1, a_2, \ldots, a_n$.

Definition 9.17. Vi kallar ett ideal $I \subseteq R$ *ändligt genererat* om $I = \langle a_1, a_2, \ldots, a_n \rangle$ för några element $a_1, a_2, \ldots, a_n \in R$.

Anmärkning 9.18. Generatorerna $a_1, a_2, \ldots, a_n$ är inte unika. T.ex. är $\langle a \rangle = \langle -a \rangle$ för varje $a \in R$.

Definition 9.19. Vi säger att ett ideal $I \subseteq R$ är ett *huvudideal* om $I = \langle a \rangle$ för något $a \in R$.

Exempel 9.20. • De triviala idealen är huvudideal, dessa genereras av 0 respektive 1.

- Mängden av alla heltalspolynom där $x = 1$ är en rot är ett huvudideal i $\mathbb{Z}[x]$, detta ideal genereras av $x - 1$. Det här följer av Faktorsatsen.
- Mängden av alla jämna tal är ett huvudideal i $\mathbb{Z}$.

Anmärkning 9.21. Låt $\langle p \rangle$ vara ett huvudideal. Då gäller det att $a \in \langle p \rangle$ om och endast om $p|a$. Detta eftersom att båda dessa egenskaper är ekvivalenta med att det finns ett $r \in R$ så att $a = rp$.

Proposition 9.22. Låt R vara ett integritetsområde och $a, b \in R$. Då gäller

$$\langle a \rangle \subseteq \langle b \rangle \Leftrightarrow b \mid a \text{ och } \langle a \rangle = \langle b \rangle \Leftrightarrow a, b \text{ är associerade.}$$

Definition 9.23. Vi säger att I är ett *äkta ideal* om I är ett ideal och $I \neq R$.

Exempel 9.24. Titta på idealet $2\mathbb{Z} = \langle 2 \rangle$. Vi vill nu undersöka om det finns något äkta ideal J så att $2\mathbb{Z} \subsetneq J \subsetneq \mathbb{Z}$. Om vi ska lägga till ett tal till $2\mathbb{Z}$ som inte redan ligger där så måste detta vara ett udda tal, alltså $2k + 1$. Men talet $-2k$ ligger i $2\mathbb{Z} \subseteq J$. Om både $2k + 1$ och $-2k$ ligger i J, då ligger även $2k + 1 + (-2k) = 1$ i J. Men då är $J = \mathbb{Z}$.

Definition 9.25. Vi säger att $I \subseteq R$ är ett *maximalt ideal* om I är ett äkta ideal och det inte ligger i något strikt större äkta ideal.

Vi kan även formulera detta på följande sätt: om I är ett maximalt ideal och $I \subseteq J$, där J är ett ideal, då är $J = I$ eller $J = R$.

Exempel 9.26. Det kan finnas flera maximala ideal i en ring. T.ex. är både $\langle 2 \rangle$ och $\langle 3 \rangle$ maximala ideal i $\mathbb{Z}$.

Definition 9.27. Ett äkta ideal I kallas för *primideal* om $ab \in I$ medför att $a \in I$ eller $b \in I$.

Exempel 9.28. Om p är ett primtal så är $p\mathbb{Z}$ både ett primideal och ett maximalt ideal. Detta visade ni på den första inlämningsuppgiften!

Sats 9.29. Låt R vara en kommutativ ring. Om $I \subseteq R$ är ett maximalt ideal så är I ett primideal.

Bevis. Antag att $ab \in I$ och att $a \notin I$. Vi vill visa att då måste $b \in I$. Titta på mängden $J := \{x + ra \mid x \in I, r \in R\}$. Det är lätt att visa att J är ett ideal. Genom att sätta $r = 0$ ser vi att $I \subseteq J$, men då $a \in J$ så är inklusionen strikt. Eftersom I är ett maximalt ideal måste $J = R$. Men då finns det $x \in I$ och $r \in R$ så att $1 = x + ra$. Om vi multiplicerar med b på båda sidor får vi likheten

$$b = xb + rab.$$

Men $xb \in I$, eftersom $x \in I, b \in R$, och $rab \in I$, eftersom $ab \in I, r \in R$, och då måste även $b = xb + rab \in I$ gälla. Detta visar att I är ett primideal. □

10 Huvudidealringar

10.1 Huvudidealringar

Anmärkning 10.1. När vi tittade på ideal i $\mathbb{Z}$ så konstaterade vi att varje ideal var på formen $a\mathbb{Z} = \langle a \rangle$. Detta är en mycket speciell egenskap som inte gäller i alla ringar.

Definition 10.2. Ett integritetsområde R är en *huvudidealring* om alla ideal $I \subseteq R$ är huvudideal.

Exempel 10.3. • $\mathbb{Z}$ är en huvudidealring.

- Varje kropp är en huvudidealring. Detta eftersom att de enda idealen som finns i en kropp är de triviala idealen, och dessa är huvudideal.
- Polynomringar över en kropp. För att bevisa detta behöver vi använda divisionsalgoritmen för polynom över en kropp. Ringar som har en divisionsalgoritm kallas för Euklidiska ringar, och dessa kommer vi prata om senare. Då kommer också beviset till varför (bland annat) polynomringar över en kropp är en huvudidealring!
- $\mathbb{Z}[x]$ är inte en huvudidealring: t.ex. $\langle 2, x \rangle$ är inte ett huvudideal. Antag att det finns en generator $p(x)$. Då har vi $p(x)q(x) = 2$ för något polynom $q(x)$. Men då måste $p(x)$ vara något av de konstanta polynomen $p(x) = \pm 1$ eller $p(x) = \pm 2$. Vi kan inte ha $p(x) = \pm 1$ eftersom $\pm 1 \notin \langle 2, x \rangle$, då det inte finns några polynom $r(x), s(x)$ så att $2r(x) + x \cdot s(x) = \pm 1$. Om generatorn $p(x) = \pm 2$, då skulle $x = \pm 2q(x)$ för något polynom $q(x)$. Men detta är inte heller möjligt!

  Alltså är $\langle 2, x \rangle$ inte ett huvudideal.

10.2 Huvudidealringar är faktoriella

Vårt nästa mål är att visa att varje huvudidealring är faktoriell. Detta kommer dock kräva en hel del arbete. Det vi måste visa är följande:

- I en huvudidealring är varje irreducibelt element är primt.
- Varje växande kedja av ideal i en huvudidealring stabiliserar sig.
- Varje icke-inverterbart element i en huvudidealring har en irreducibel faktor.
- Varje icke-inverterbart element i en huvudidealring kan faktoriseras i irreducibla faktorer.
- Denna faktorisering är unik upp till ordning och association.

Sats 10.4. I en huvudidealring R är varje irreducibelt element ett primelement.

Bevis. Antag att $a \in R$ är ett irreducibelt element och att $a|bc$. Vi vill visa att $a|b$ eller $a|c$. Titta nu på idealet $\langle a, b \rangle$. Eftersom att R är en huvudidealring så vet vi att det finns ett element d så att $\langle a, b \rangle = \langle d \rangle$. Detta betyder att $a \in \langle d \rangle$ och då finns $r \in R$ så att $a = rd$. Eftersom att a är irreducibel måste antingen d vara inverterbart, eller så måste r vara inverterbart.

Antag först att d är inverterbart. Då är $\langle d \rangle = R$, enligt tidigare anmärkning. Men då är även $\langle a, b \rangle = R$ och det måste finnas $s, t \in R$ så att $as + bt = 1$. Multiplicera detta med c och vi får:

$$c = a(sc) + (bc)t.$$

Eftersom att $a|a$ och $a|bc$ så måste $a|c$.

Antag nu istället att r är inverterbar. Då är $d = r^{-1}a$. Eftersom att $b \in \langle a, b \rangle = \langle d \rangle$ så är $b = sd = (sr^{-1})a$. Alltså har vi $a|b$. Vi har nu visat att om $a|bc$ så gäller $a|b$ eller $a|c$, alltså är a primt. □

Exempel 10.5. • Vi har redan sett att i $\mathbb{Z}$ är primelementen och de irreducibla elementen precis $\pm p$, där p är ett primtal.

- Vi vet nu även att primelementen i $K[x]$, där K är en kropp, är precis de irreducibla polynomen.
- Till exempel i $\mathbb{C}[x]$ så är primelementen alla förstagradspolynom.

Nu ska vi titta på följande fenomen hos ideal av heltal:

Exempel 10.6. Låt $I \subseteq \mathbb{Z}$ vara ett ideal. Då finns ett heltal m så att $I = \langle m \rangle$. Vi vet att $\langle m \rangle \subseteq \langle k \rangle$ om och endast om $k \mid m$. Men det finns endast ändligt många delare till m, så om vi har en oändlig kedja av inklusioner,

$$\langle m \rangle \subseteq \langle k_1 \rangle \subseteq \langle k_2 \rangle \subseteq \langle k_3 \rangle \subseteq \langle k_4 \rangle \subseteq \dots$$

så måste kedjan till sist "stabilisera sig", d.v.s. det måste finnas ett heltal N så att $k_i = k_N$ för alla $i \geq N$. Alla k_i är ju nämligen delare till m, och det finns bara ändligt många sådana!

Definition 10.7. Låt R vara en ring. Vi kallar en familj av ideal $\{I_j\}_{j=1}^{\infty}$ för en *växande kedja av ideal* om $I_j \subseteq I_{j+1}$ för $j = 1, 2, \dots$.

Vi kallar R för *Noethersk* om varje växande kedja stabiliserar sig, d.v.s. om det finns ett n så att för varje $j \geq n$ gäller $I_j = I_n$.

Lemma 10.8. Varje huvudidealring är Noethersk.

Bevis. Låt

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

vara en växande kedja av ideal. Vi påstår att unionen av dessa är ett ideal. Låt $I = \bigcup_{i=1}^{\infty} I_i$. Då I_1 är icke-tom är även I det. Låt $a, b \in I$, då måste $a \in I_i$ och $b \in I_j$ för något i, j. Vi kan anta att $i \geq j$, då gäller $b \in I_j \subseteq I_i$. Eftersom att I_i är ett ideal och $a, b \in I_i$ så gäller $a + b \in I_i$ samt $ra \in I_i$. Men då gäller även $a + b, ra \in I$. Alltså är I ett ideal i R.

Eftersom att R är en huvudidealring så måste det finnas ett $g \in I$ så att $I = \langle g \rangle$. Men då $g \in I = \bigcup_{i=1}^{\infty} I_i$ så måste det finnas ett n så att $g \in I_n$. Vi påstår då att kedjan stabiliserar sig vid I_n, d.v.s. $I_j = I_n$ för alla $j \geq n$. Låt $a \in I_j$, där $j \geq n$. Eftersom att vi då även har $a \in I = \langle g \rangle$ så finns det $r \in R$ så att $a = rg$. Men $a = rg \in I_n$. Alltså måste $I_j = I_n$ för alla $j \geq n$. □

Vi kommer nu att använda att varje huvudidealring är Noethersk för att bevisa de kommande två resultaten. Observera att egenskapen "varje växande kedja av ideal stabiliserar sig" är ekvivalent med egenskapen "det finns ingen *strikt* växande kedja av ideal". Först påminner vi oss om följade proposition:

Proposition 10.9. Låt R vara ett integritetsområde och $a, b \in R$. Då gäller

$$\langle a \rangle \subseteq \langle b \rangle \Leftrightarrow b \mid a \text{ och } \langle a \rangle = \langle b \rangle \Leftrightarrow a, b \text{ är associerade.}$$

Lemma 10.10. Låt R vara en huvudidealring. Varje nollskilt icke-inverterbart element $a \in R$ har en irreducibel faktor.

Bevis. Idéen till beviset är följande: om vi har ett element som inte är irreducibelt (och inte heller inverterbart) kan vi skriva det som en produkt av två icke-inverterbara faktorer. Om vi fortsätter dela upp faktorerna men aldrig hittar en irreducibel faktor kommer detta ge upphov till en strikt växande kedja av ideal. Men detta är omöjligt i en huvudidealring då de är Noetherska.

Om a själv är irreducibel är påståendet såklart sant, så antag att a är reducibel (kom ihåg att vi har antagit att a inte är inverterbar). Då finns det icke-inverterbara a_1, b_1 så att $a = a_1 b_1$. Vi har alltså $a \mid a_1$ och a, a_1 är inte associerade (eftersom b_1 inte är inverterbar). Det följer att

$$\langle a \rangle \subsetneq \langle a_1 \rangle.$$

Om a_1 inte är irreducibel (annars skulle vi vara klara) så måste det på samma sätt finnas icke-inverterbara a_2, b_2 så att $a_1 = a_2 b_2$. Om vi upprepar det vi nyss gjorde så får vi

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle.$$

Antag att vi aldrig hittar en irreducibel faktor, då skulle vi få en strikt växande kedja

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$$

som aldrig stabiliserar sig. Men detta är omöjligt då R är Noethersk. Alltså måste vi tillslut hitta en irreducibel faktor. □

Lemma 10.11. Låt R vara en huvudidealring. Varje nollskilt icke-inverterbart element $a \in R$ kan skrivas som en produkt av ändligt många irreducibla element.

Bevis. Idéen till beviset liknar det förra beviset. Vi börjar med att faktorisera vårt element i en irreducibel faktor gånger en annan faktor. Om vi hela tiden fortsätter att dela upp "den andra" faktorn så måste detta tillslut ta slut, annars får vi en strikt växande kedja av ideal. Vilket är omöjligt!

Antag att a är ett icke-inverterbart element. Om a är irreducibel är vi klara, annars finns det enligt Lemma 10.10 ett irreducibelt element p_1 så att $a = p_1 c_1$ för något icke-inverterbart $c_1 \in R$. Om c_1 är irreducibel är vi klara, annars finns p_2 så att $c_1 = p_2 c_2$ för något icke-inverterbart $c_2 \in R$. Om vi fortsätter detta måste vi tillslut få ett c_n som är irreducibel, annars får vi nämligen en strikt växande kedja av ideal:

$$\langle a \rangle \subsetneq \langle c_1 \rangle \subsetneq \langle c_2 \rangle \subsetneq \dots.$$

Men då R är Noethersk är detta omöjligt. Alltså måste vi tillslut få $c_n = p_n$ där p_n är irreducibel. Detta betyder att $a = p_1 p_2 \dots p_n$, där alla p_k är irreducibla. □

Sats 10.12. Varje huvudidealring är faktoriell.

Bevis. Det som återstår att visa är att faktoriseringen av varje icke-inverterbart element i irreducibla faktorer är unik upp till ordning och association.

Låt $p_1p_2 \dots p_n = q_1q_2 \dots q_m$ och antag att $n \leq m$. Vi påstår att $n = m$ och p_i är associerat med q_i för varje $i = 1, \dots, n$. Vi bevisar påståendet med hjälp av induktion på n.

Basfall ($n = 1$): Vi har alltså $p_1 = q_1q_2 \dots q_m$. Vi vet att varje irreducibelt element i R även är primt, därför måste p_1 dela någon av faktorerna i högerledet, eftersom ringen är kommutativ kan vi anta att $p_1|q_1$, d.v.s. $q_1 = p_1c$. Men då q_1 är irreducibelt och p_1 är icke-inverterbart så måste c vara inverterbart. Alltså är p_1 och q_1 associerade.

Eftersom vi är i ett integritetsområde kan vi nu förkorta med p_1 och får

$$1 = (c^{-1}q_2)q_3 \cdot \dots \cdot q_m.$$

Men detta ger oss att $q_2, \dots, q_m$ är inverterbara. Det är omöjligt eftersom alla q_i är irreducibla, alltså måste även $m = 1 = n$.

Induktionssteg: Antag att påståendet gäller för vänsterled med $n - 1$ element. Induktionssteget ser precis likadant ut som basfallet.

Vi vet att varje irreducibelt element i R även är primt, därför måste p_1 dela någon av faktorerna i högerledet, eftersom ringen är kommutativ kan vi anta att $p_1|q_1$, d.v.s. $q_1 = p_1c$. Men då q_1 är irreducibelt och p_1 är icke-inverterbart så måste c vara inverterbart. Alltså är p_1 och q_1 associerade.

Vi kan nu förkorta med p_1 och får

$$p_2 \dots p_n = (c^{-1}q_2) \dots q_m.$$

Eftersom att $c^{-1}q_2$ är irreducibelt om och endast om q_2 är det så är vi nu i samma situation som vi började, men med ett element mindre på varje sida. Enligt induktionsantagandet är $n - 1 = m - 1$ och p_i associerat med q_i för $i = 2, \dots, n$. Alltså gäller resultatet även för n. Enligt induktionsprincipen gäller alltså resultatet för alla positiva heltal n. □

10.3 Egenskaper hos huvudideal

Nu när vi har visat att varje huvudidealring är faktoriell kan vi till exempel använda detta för att visa följande samband mellan ett huvudideal och dess generator.

Sats 10.13. Låt $p \neq 0$. Ett huvudideal $Rp = \langle p \rangle$ i en huvudidealring R är ett maximalt ideal om och endast om p är ett irreducibelt element.

Bevis. Antag att $p \neq 0$ inte är irreducibelt, då är antingen p inverterbart eller så är $p = ab$ där varken a eller b är inverterbara. Om p är inverterbart så är $\langle p \rangle = R$ och $\langle p \rangle$ är därmed inte maximalt. Om istället $p = ab$ där vaken a eller b är inverterbara så gäller $\langle p \rangle \subsetneq \langle a \rangle \subsetneq R$. Alltså är inte $\langle p \rangle$ ett maximalt ideal i detta fall heller.

Antag att p är irreducibelt och att $\langle p \rangle \subseteq I$ för något ideal I. Då R är en huvudidealring så finns det ett element a så att $\langle a \rangle$. Då gäller framför allt att $p \in \langle a \rangle$, så $p = ab$ för något $b \in R$. Men då p är irreducibelt så gäller att a är inverterbart eller att b är inverterbart. Om a är inverterbart så är $\langle a \rangle = R$. Om istället b är inverterbart så är $pb^{-1} = a$, så

$a \in \langle p \rangle$ vilket implicerar att $\langle a \rangle \subseteq \langle p \rangle$. De två inklusionerna innebär att $\langle p \rangle = \langle a \rangle$. Alltså måste $I = R$ eller $I = \langle p \rangle$ för varje ideal I så att $\langle p \rangle \subseteq I \subseteq R$. Detta visar att $\langle p \rangle$ är ett maximalt ideal! □

Exempel 10.14. Vi vet nu exakt vilka maximala ideal vi har i $\mathbb{Z}$, nämligen alla ideal som genereras av ett primtal!

Exempel 10.15. Kom ihåg exemplet där vi visade att $\langle 2, x \rangle \subseteq \mathbb{Z}[x]$ var ett huvudideal. Från detta ser vi även att ovanstående sats inte gäller generellt sätt om vi inte kräver att vi ska ha en huvudidealring. Elementet 2 är irreducibelt i $\mathbb{Z}[x]$, men $\langle 2 \rangle$ är inte ett maximalt ideal då

$$\langle 2 \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x].$$

Vi kan även visa ytterligare ett resultat om huvudideal och dess generator. Men den här gången behöver vi inte anta att ringen är en huvudidealring, det räcker med att anta att ringen är ett integritetsområde. (Kom ihåg att vi endast definierat primelement (och irreducibla element) för integritetsområden.)

Sats 10.16. Ett nollskilt huvudideal $Rp = \langle p \rangle$ i ett integritetsområde R är ett primideal om och endast om p är ett primelement.

Bevis. Vi börjar med att visa att om p är ett primelement så är $\langle p \rangle$ ett primideal. Antag att $ab \in \langle p \rangle$. Då finns det $r \in R$ så att $ab = rp$. Men detta är ekvivalent med att $p|ab$, och eftersom att p är primt så följer det att $p|a$ eller $p|b$. Detta är i sin tur ekvivalent med att $a = sp \in \langle p \rangle$ eller $b = tp \in \langle p \rangle$. Alltså är $\langle p \rangle$ ett primideal.

Antag nu istället att $\langle p \rangle$ är ett nollskilt primideal och att $p|ab$. Då är $ab = rp$, för något $r \in R$. Alltså gäller $ab \in \langle p \rangle$ vilket medför att $a \in \langle p \rangle$ eller $b \in \langle p \rangle$. Men detta är ekvivalent med att $p|a$ eller $p|b$. Alltså är p ett primelement. □

11 Kvotringar och Noethers första isomorfisats

11.1 Definitionen av en kvotring

Vi definierade $\mathbb{Z}_n$ som alla mängden av alla restklasser modulo n. Vi sa då att två tal a och b sågs som "samma" om $n|a-b$. Men som vi precis har sett så är detta ekvivalent med att $a-b$ ligger i idealet som genereras av n. Detta kommer ge oss definitionen av en kvotring! Vi visar först att relationen $a-b \in I$, där $I \subseteq R$ är ett ideal, är en ekvivalensrelation.

(i) $a-a=0 \in I$, så relationen är reflexiv.

(ii) Om $a-b \in I$ så gäller även $b-a=(-1)(a-b) \in I$, så relationen är symmetrisk.

(iii) Om $a-b, b-c \in I$ så gäller även $a-c=(a-b)+(b-c) \in I$, så relationen är transitiv.

Definition 11.1. Om $I \subseteq R$ är ett ideal så definierar vi en ring R/I som följer:

- R/I består av ekvivalensklasser $\overline{a}$ av element från R med $\overline{a}=\overline{b}$ om och endast om $a-b \in I$.
- $\overline{a}+\overline{b}=\overline{a+b}$.
- $\overline{a}\cdot\overline{b}=\overline{ab}$.

Vi måste såklart visa att additionen och multiplikationen är väldefinierad och att alla ringaxiom är uppfyllda. Detta är en utmärkt övning!

Exempel 11.2. • Ett välkänt exempel är $\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$.

- Man kan tänka på kvotringen som en ny ring där vi "klumpar ihop", eller mer korrekt "identifierat" vissa element. I $\mathbb{Z}_n$ har vi t.ex. identifierat alla element som har samma rest.
- Vi kan även titta på kvoten $\mathbb{R}[x]/\langle x^2-(-1)\rangle$. Här har vi identifierat x^2 med -1. T.ex. x^7 är lika med $-x$ eftersom $x^7-(-x)=(x^2-(-1))(x^5-x^3+x) \in \langle x^2-(-1)\rangle$. Vi kan "förenkla" alla polynom till ett polynom på formen $a+bx$ och x har egenskapen $x\cdot x=-1$. Men detta påminner väldigt mycket om de komplexa talen, och faktum är att $a+bx \mapsto a+bi$ är en isomorfi mellan $\mathbb{R}[x]/\langle x^2-(-1)\rangle$ och $\mathbb{C}$.
- Man kan också tänka på kvotringar som att vissa element ska "försvinna", alltså identifieras med 0. Titta till exempel på $R[x]/\langle x^2\rangle$, här kommer alla termer av grad ≥ 2 identifieras med 0 eftersom dessa tillhör idealet vi kvotar med. Ekvivalensklasserna i denna kvot är alla på formen $ax+b$, och om vi multiplicerar två element får vi $(ax+b)(cx+d)=acx^2+(ad+bc)x+bd=(ad+bc)x+bd$.

Anmärkning 11.3. • Vi kallar detta "kvot(ring)en av R modulo I", eller "R kvotat med I".

- För att på ett smidigt sätt hålla koll på vilket ideal vi har "kvotat" med så betecknar vi ofta $\overline{a}=a+I$. Detta är faktiskt väldigt intuitivt eftersom att $\overline{a}=\overline{b}$ om och endast om det finns $k \in I$ så att $b=a+k$.

11.2 Noethers första isomorfisats

Det kan ofta vara svårt att inse hur en kvotring beter sig, med andra ord, ifall den är isomorf med någon annan välkänd ring. Nu ska vi gå igenom ett väldigt användbar sats för att hitta just isomorfismer mellan en kvotring och en annan ring.

Sats 11.4 (Noethers första isomorfisats)**.** Låt φ vara en homomorfism från R till S. Då gäller $R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.

Bevis. Vi skapar en isomorfism $f : R/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ på följande sätt: Låt $\overline{x} \in R/\operatorname{Ker}(\varphi)$ och definiera $f(\overline{x}) = \varphi(x) \in \operatorname{Im}(\varphi)$. Denna avbildning är väldefinierat eftersom om $\overline{x} = \overline{y}$ så gäller $y - x \in \operatorname{Ker}(\varphi)$ och vi får då:

$$\begin{aligned} f(\overline{x}) = \varphi(x) = \varphi(x) + 0 = \varphi(x) + \varphi(y - x) \\ = \varphi(x) + \varphi(y) - \varphi(x) = \varphi(y) = f(\overline{y}). \end{aligned}$$

Alltså är f väldefinierad. Eftersom att φ är en homomorfism så kommer det direkt att följa att f är det (men vi måste egentligen visa detta).

Vi vill nu visa att f är bijektiv. Funktionen f är uppenbarligen surjektiv eftersom att för varje $y \in \operatorname{Im}(\varphi)$ så finns det ett $x \in R$ så att $\varphi(x) = y$. Men då gäller även $f(\overline{x}) = y$. Nu vill vi visa att f är injektiv. Antag att $f(\overline{x}) = f(\overline{y})$. Vi får:

$$\begin{aligned} & f(\overline{x}) = f(\overline{y}) \\ \Leftrightarrow\ & f(\overline{x}) - f(\overline{y}) = 0 \\ \Leftrightarrow\ & f(\overline{x} - \overline{y}) = 0 \\ \Leftrightarrow\ & f(\overline{x - y}) = 0 \\ \Leftrightarrow\ & \varphi(x - y) = 0 \\ \Leftrightarrow\ & x - y \in \operatorname{Ker}(\varphi) \\ \Leftrightarrow\ & \overline{x} = \overline{y}. \end{aligned}$$

Alltså är f en bijektiv homomorfism och således en isomorfism! □

Anmärkning 11.5. Noethers första isomorfisats säger alltså att vi kan identifiera de element i R som avbildas på samma element i S. Om vi gör detta så får vi något som beter sig likadant som bilden (vilket är en delring i S).

Exempel 11.6. • $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ eftersom $\varphi : \mathbb{Z} \to \mathbb{Z}_n, x \mapsto \overline{x}$ är en epimorfism, så $\operatorname{Im}(\varphi) = \mathbb{Z}_n$, och $\operatorname{Ker}(\varphi) = n\mathbb{Z}$.

- $R/\{0\} \cong R$ eftersom $\operatorname{Ker}(\operatorname{Id}_R) = \{0\}$ och $\operatorname{Im}(\operatorname{Id}_R) = R$. Det följer även att $R \cong \operatorname{Im}(\varphi)$ om φ är en monomorfism.
- $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$.

  Bevis. Vi använder oss av Noethers första isomorfisats!

  Låt $\varphi : \mathbb{R}[x] \to \mathbb{C}$ definieras via $p(x) \mapsto p(i)$. Vi kan se varje reellt polynom som ett komplext polynom, så utvärdering i det komplexa talet i är en vettig avbildning.

Vi behöver nu visa två saker, först att φ är surjektiv och sedan att $\text{Ker}(\varphi) = \langle x^2 + 1 \rangle$. Att φ är surjektiv är lätt att se då för varje komplext tal $a + bi$ så har vi polynomet $a + bx \in \mathbb{R}[x]$ som avbildas på detta.

Antag nu att $\varphi(p(x)) = 0$, alltså att $p(i) = 0$. Från Faktorsatsen så får vi att $p(x) = (x - i)h(x)$, där $h(x) \in \mathbb{C}[x]$. Men vi vill inte ha ett komplext polynom, utan ett reellt! Men från Algebra I så vet vi att om ett reellt polynom har en komplex rot z, så är även konjugatet $\overline{z}$ en rot. Vi har då att $p(x) = (x - i)(x + i)g(x) = (x^2 + 1)g(x)$. Eftersom att $p(x)$ och $x^2 + 1$ är reella så måste även $g(x)$ vara det.

Vi har nu visat att $\text{Ker}(\varphi) \subseteq \langle x^2 + 1 \rangle$. Men då $\varphi((x^2 + 1)g(x)) = (i^2 + 1)g(i) = 0$ så har vi även $\langle x^2 + 1 \rangle \subseteq \text{Ker}(\varphi)$. Alltså har vi visat att $\text{Ker}(\varphi) = \langle x^2 + 1 \rangle$. Från Noethers första isomorfisats följer det nu att $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$. $\square$

12 Ideal i kvotringar

12.1 Ideal i kvotringar

Eftersom att R/I också är en ring så finns det ideal även här! Det visar sig att vi kan säga väldigt mycket om vilka ideal som finns i denna nya ring.

Lemma 12.1. Låt $I \subseteq R$ vara ett ideal. Vi har då alltid en epimorfism $\pi : R \to R/I$ som ges av $x \mapsto x + I$ och där $\text{Ker}(\pi) = I$.

Bevis. Att π är en homomorfism följer direkt från definitionen av kvotringen: $(x + y) + I = (x + I) + (y + I)$, $(xy) + I = (x + I)(y + I)$ och $1_R + I = 1_{R/I}$. Att den är surjektiv är också uppenbart. Det som återstår att visa är att $\text{Ker}(\pi) = I$. Antag att $\pi(x) = x + I = 0 + I = 0_{R/I}$, detta gäller om och endast om $x - 0 = x \in I$. □

Exempel 12.2. I $\mathbb{Z}_6$ har vi idealet $\{\overline{0}, \overline{2}, \overline{4}\} = \overline{2}\mathbb{Z}_6$. Titta nu på homomorfismen $f : \mathbb{Z} \to \mathbb{Z}_6$. De element som avbildas på idealet $\overline{2}\mathbb{Z}_6$ är precis alla jämna element. Men detta är ett ideal i $\mathbb{Z}$.

På samma sätt är mängden av element som avbildas på idealet $\{\overline{0}, \overline{3}\} = \overline{3}\mathbb{Z}_6$ precis alla multiplar av 3, vilket också är ett ideal i $\mathbb{Z}$.

Lemma 12.3. Låt R och S vara två ringar, och $f : R \longrightarrow S$ en homomorfism. Låt I vara ett ideal i S. Då är den inversa bilden $f^{-1}(I)$ av I ett ideal i R. Eller med andra ord, delmängden

$$\{x \in R \mid f(x) \in I\}$$

i R är ett ideal.

Bevis. Eftersom $0_S \in I$ och $f(0_R) = 0_S$ så är mängden icke-tom. Låt nu $x, y \in f^{-1}(I)$, då gäller alltså att $f(x), f(y) \in I$. Men då $f(x + y) = f(x) + f(y) \in I$, eftersom I är ett ideal, så har vi $x + y \in f^{-1}(I)$.

Låt $x \in f^{-1}(I)$ och $r \in R$. Då har vi $f(rx) = f(r)f(x) \in I$ eftersom $f(x) \in I$ och I är ett ideal. Men detta betyder att $rx \in f^{-1}(I)$. Alltså är $f^{-1}(I)$ ett ideal. □

Exempel 12.4. Titta igen på epimorfismen $f : \mathbb{Z} \to \mathbb{Z}_6$. I $\mathbb{Z}$ har vi t.ex. idealet $4\mathbb{Z}$. Om vi delar ett tal i $4\mathbb{Z}$ med 6 så får vi alltid en jämn rest, och vi ser att $f(0) = \overline{0}$, $f(8) = \overline{2}$ och $f(4) = \overline{4}$. Alltså är $f(4\mathbb{Z}) = \overline{2}\mathbb{Z}_6$.

Lemma 12.5. Låt R och S vara två ringar, och $f : R \longrightarrow S$ en epimorfism. Låt I vara ett ideal i R. Då är bilden av I ett ideal i S. Med andra ord, delmängden

$$\{y \in S \mid y = f(x) \text{ för något } x \in I\}$$

är ett ideal i S.

Bevis. Bilden av I under f, $f(I)$, är icke-tom eftersom att I är icke-tom. Låt $x, y \in f(I)$, då finns $a, b \in I$ så att $f(a) = x, f(b) = y$. Då gäller $x+y = f(a)+f(b) = f(a+b) \in f(I)$ eftersom $a + b \in I$.

Låt $x \in f(I)$ och $s \in S$. Eftersom f är surjektiv finns det $r \in R$ så att $f(r) = s$, och såklart $a \in I$ så att $f(a) = x$. Då har vi $sx = f(r)f(a) = f(ra) \in f(I)$ eftersom $ra \in I$. Alltså är $f(I)$ ett ideal. □

Exempel 12.6. Titta på projektionen $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ och kom ihåg att $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$. I $\mathbb{Z}/6\mathbb{Z}$ har vi idealet $\langle\overline{2}\rangle$ och vi såg tidigare att $\pi^{-1}(\langle\overline{2}\rangle) = \overline{2}\mathbb{Z}$. Vi kan nu se att $6\mathbb{Z} \subseteq 2\mathbb{Z}$.

Lemma 12.7. Om $\overline{J} \subseteq R/I$ är ett ideal, så är $\pi^{-1}(\overline{J}) \subseteq R$ ett ideal som innehåller I, där $\pi : R \to R/I$ är projektionen på kvotringen.

Bevis. Att $\pi^{-1}(\overline{J}) \subseteq R$ är ett ideal följer från Lemma 12.3. Eftersom $\overline{0} \in \overline{J}$ så gäller $\pi^{-1}(\overline{0}) \subseteq \pi^{-1}(\overline{J})$. Men eftersom $\pi^{-1}(\overline{0}) = I$ så har vi $I \subseteq \pi^{-1}(\overline{J})$. □

Exempel 12.8. Titta på projektionen $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Vi såg att både $\pi(2\mathbb{Z}) = \langle\overline{2}\rangle$ och $\pi(4\mathbb{Z}) = \langle\overline{2}\rangle$. Observera att $\pi^{-1}(\langle\overline{2}\rangle) = 2\mathbb{Z}$ och alltså har vi $\pi^{-1} \circ \pi(2\mathbb{Z}) = 2\mathbb{Z}$, men $\pi^{-1} \circ \pi(4\mathbb{Z}) \neq 4\mathbb{Z}$. Skillnaden är att $6\mathbb{Z} \subseteq 2\mathbb{Z}$, och $6\mathbb{Z} \nsubseteq 4\mathbb{Z}$.

Lemma 12.9. Om $J \subseteq R$ är ett ideal som innehåller I så är $\pi^{-1} \circ \pi(J) = J$, där $\pi : R \to R/I$ är projektionen på kvotringen.

Bevis. Notera att om $x \in J$ och $\pi(x) = \pi(x')$ måste även $x' \in J$ eftersom

$$x - x' \in \mathrm{Ker}(\pi) = I \subseteq J.$$

Alltså gäller i detta fall $\pi^{-1}(y) \subseteq J$. Med hjälp av detta kan vi nu dra slutsatsen att $\pi^{-1} \circ \pi(J) \subseteq J$.

$$\begin{aligned}\pi^{-1} \circ \pi(J) &= \pi^{-1}\left(\{y \in R/I \mid y = \pi(x) \text{ för något } x \in J\}\right) \\ &= \bigcup_{y=\pi(x) \text{ för något } x \in J} \pi^{-1}(y) \\ &\subseteq J.\end{aligned}$$

Men varje $x \in J$ träffar ju något y i R/I, så vi måste ha en likhet ovan, alltså gäller $\pi^{-1} \circ \pi(J) = J$. □

Exempel 12.10. Titta på projektionen $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$. Vi har $\pi \circ \pi^{-1}(\langle\overline{2}\rangle) = \langle\overline{2}\rangle$ och $\pi \circ \pi^{-1}(\langle\overline{3}\rangle) = \langle\overline{3}\rangle$.

Lemma 12.11. Om $\overline{J} \subseteq R/I$ är ett ideal, så är $\pi \circ \pi^{-1}(\overline{J}) = \overline{J}$, där $\pi : R \to R/I$ är projektionen på kvotringen.

Bevis. Eftersom att π är surjektiv så finns det ett $x \in R$ som träffar $y \in \overline{J}$ för varje element y i $\overline{J}$. Vi får därför:

$$\begin{aligned}\pi \circ \pi^{-1}(\overline{J}) &= \pi\left(\{x \in R \mid \pi(x) \in \overline{J}\}\right) \\ &= \overline{J}.\end{aligned}$$

□

Exempel 12.12. I $\mathbb{Z}/6\mathbb{Z}$ har vi precis 4 ideal, nämligen $\mathbb{Z}_6, \{\overline{0}\}, \langle\overline{2}\rangle, \langle\overline{3}\rangle$. I $\mathbb{Z}$ finns precis 4 ideal som innehåller $6\mathbb{Z}$, nämligen $\mathbb{Z}, 6\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}$.

Sats 12.13. Låt R vara en kommutativ ring och $I \subsetneq R$ ett äkta ideal. Då finns det en bijektion mellan mängden av ideal J i R som innehåller I och mängden av alla ideal i R/I.

Bevis. Vi påstår att projektionen $\pi : R \to R/I$ ger oss en bijektion mellan dessa två mängder. Kom ihåg att en funktion f är en bijektion om och endast om det finns en invers f^{-1} så att $f \circ f^{-1} = \text{Id}$ och $f^{-1} \circ f = \text{Id}$.

Låt $f : \{\text{Ideal i } R \text{ som innehåller } I\} \to \{\text{Ideal i } R/I\}$ definieras via $J \mapsto \pi(J)$. Enligt Lemma 12.5 så $\pi(J)$ detta ett ideal i R/I, så målmängden är korrekt. Inversen till denna avbildning påstår vi nu är $\overline{J} \mapsto \pi^{-1}(\overline{J})$, där $\overline{J}$ är ett ideal i R/I. Enligt Lemma 12.7 är $\pi^{-1}(\overline{J})$ ett ideal i R som innehåller I, så även här är målmängden korrekt.

Men enligt Lemma 12.9 så gäller

$$f^{-1} \circ f(J) = \pi^{-1} \circ \pi(J) = J$$

och enligt Lemma 12.11 så gäller

$$f \circ f^{-1}(\overline{J}) = \pi \circ \pi^{-1}(\overline{J}) = \overline{J}.$$

Alltså får vi identitetsavbildningen om vi sammansätter de två funktionerna från vardera håll, och f är därmed en bijetion mellan de två mångderna. □

Med hjälp av detta lemma kommer vi kunna koppla ihop egenskaper hos idealet med egenskaper hos kvotringen. Först tittar vi på ett exempel.

Exempel 12.14. Vi har tidigare sett att följande gäller:

- $\mathbb{Z}_n$ är en kropp om och endast om n är ett primtal.
- $\langle n \rangle \subseteq \mathbb{Z}$ är ett maximalt ideal om och endast om n är ett primtal.
- $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$.

Om vi kombinerar dessa tre saker kan vi dra slutsaten att kvoten är en kropp om och endast om idealet vi kvotar med är ett maximalt ideal.

Sats 12.15. Låt R vara en kommutativ ring. Ett ideal $I \subseteq R$ är maximalt om och endast om R/I är en kropp.

Bevis. Antag att R/I är en kropp, då finns endast två ideal. Men enligt förgående sats finns då precis två ideal som uppfyller $I \subseteq J \subseteq R$. Men $J = I$ och $J = R$ uppfyller detta, så inga andra ideal kan göra det. Alltså är I maximalt.

Antag att R/I inte är en kropp. Då finns det ett nollskilt icke-inverterbart element $a + I \in R/I$. Titta på $a \in R$. Eftersom att $a + I$ är nollskilt så gäller $a \notin I$. Vi kan då skapa idealet $I + aR = \{m + ar \mid m \in I, r \in R\}$. Att detta faktiskt är ett ideal är lätt att visa. Vi påstår att $I \subsetneq I + aR \subsetneq R$. Den första strikta inklusionen är uppenbar då $I \subseteq I + aR$, men $a \notin I$ och $a \in I + aR$.

Om $I + aR = R$ så skulle vi ha $1 = m + ar$ för något $m \in I, r \in R$. Men då är $1 + I = ar + I = (a + I)(r + I)$, alltså skulle $a + I$ vara inverterbart vilket är en motsägelse. Alltså har vi hittat ett mellanliggande ideal och I är därför inte maximalt. □

Exempel 12.16. Precis som med kroppar och maximala ideal kan vi göra samma jämförelse med integritetsområden och primideal:

- $\mathbb{Z}_n$ är ett integritetsområde om och endast om n är ett primtal.

- $\langle n \rangle \subseteq \mathbb{Z}$ är ett primideal om och endast om n är ett primtal.
- $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$.

Om vi kombinerar dessa tre saker kan vi dra slutsaten att kvoten är ett integritetsområde om och endast om idealet vi kvotar med är ett primideal.

Sats 12.17. Låt R vara en kommutativ ring. Ett ideal $I \subseteq R$ är ett primideal om och endast om R/I är ett integritetsområde.

Bevis. Antag att I är ett primideal och att $(a+I)(b+I) = 0$. Då gäller $ab+I = 0+I \Rightarrow ab \in I$. Men eftersom I är ett primideal så gäller $a \in I \vee b \in I \Rightarrow a + I = 0 \vee b + I = 0$. Alltså har R/I inga nolldelare. Eftersom att R är kommutativ så är även R/I kommutativ, vilket betyder att R/I är ett integritetsområde.

Antag att R/I är ett integritetsområde och att $ab \in I$. Då är $(a+I)(b+I) = ab+I = 0$, men eftersom att R/I är ett integritetsområde så måste $a + I = 0 \vee b + I = 0$. Men detta är ekvivalent med att $a \in I$ eller $b \in I$. Alltså är I primt. □

Anmärkning 12.18. Kom ihåg att varje kropp är ett integritetsområde och varje maximalt ideal är ett primideal. Så den första satsen kan ses som ett specialfall av den andra!

13 Euklidiska ringar

13.1 Euklidiska ringar

En riktigt bra egenskap hos heltalen är divisionsalgoritmen, d.v.s. om vi tar vilka $a, b \in \mathbb{Z}$ som helst, men $b \neq 0$, så finns det $q, r \in \mathbb{Z}$ så att $a = qb + r$ där $0 \leq r < b$. Vi har en liknande divisionsalgoritm för reella polynom, nämligen om a, b är reella polynom, där b är nollskilt, så finns polynom q, r så att $r = 0$ eller $\deg(r) < \deg(b)$ och

$$a(x) = q(x)b(x) + r(x).$$

En av de viktiga sakerna här var just att $r < b$. Vi behöver alltså en "ordningsfunktion", eller en så kallad "norm"! Vi fångar upp dessa egenskaper i följande definition:

Definition 13.1. Ett integritetsområde R kallas för en *Euklidisk ring* om det finns en funktion $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ så att

(i) $N(a) \leq N(ab)$ för alla $a, b \in R \setminus \{0\}$,

(ii) För varje $a, b \in R \setminus \{0\}$ finns det $q, r \in R$ så att $a = qb + r$ och antingen $r = 0$ eller $N(r) < N(b)$.

En funktion med dessa egenskaper kallas för en *Euklidisk norm* på R.

Exempel 13.2. 1. Heltalen bildar en Euklidisk ring. $\mathbb{Z}$ är ett integritetsområde och $N(a) = |a|$ är en Euklidisk norm!

2. Låt K vara en kropp och sätt $N(a) = 1$ för varje $a \in K \setminus \{0\}$. Då är K en Euklidisk ring.

3. $\mathbb{Z}[\sqrt{-2}]$ är en Euklidisk ring tillsammans med den Euklidiska normen $N(a+b\sqrt{-2}) = a^2 + 2b^2$.

4. $\mathbb{Z}[\sqrt{2}]$ är en Euklidisk ring tillsammans med den Euklidiska normen $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.

5. $\mathbb{R}[x]$ är en Euklidisk ring tillsammans med gradfunktionen. Observera att graden av ett polynom är icke-negativ om polynomet är nollskilt.

   Vi tittar på ett exempel hur vi hittat $q(x)$ och $r(x)$. Låt $f(x) = 3x^3 - \frac{5}{2}x^2 + \sqrt{2}$ och $g(x) = 2x^2 + x$. Vi använder liggande stolen för att beräkna kvoten och resten.

$$\begin{array}{l|l} & \frac{3}{2}x - 2 \\ \hline 3x^3 - \frac{5}{2}x^2 + \sqrt{2} & \big| \; 2x^2 + x \\ -(3x^3 + \frac{3}{2}x^2) & \\ \hline -4x^2 + \sqrt{2} & \\ -(-4x^2 - 2x) & \\ \hline 2x + \sqrt{2} & \end{array}$$

   Detta ger oss att $q(x) = \frac{3}{2}x - 2$ och $r(x) = 2x + \sqrt{2}$.

Lemma 13.3. Låt K vara en kropp. För varje $f(x), g(x) \in K[x] \setminus \{0\}$ så finns det $q(x), r(x) \in K[x]$ så att

$$f(x) = q(x)g(x) + r(x)$$

där $r(x) = 0$ eller $\deg(r) < \deg(g)$.

Bevis. Om $\deg(g) > \deg(f)$ så kan vi sätta $q(x) = 0$ och $r(x) = f(x)$. Antag därför att $\deg(g) \leq \deg(f)$. Vi bevisar påståendet med hjälp av induktion på $\deg(f)$.

Basfall: Antag att $\deg(f) = 0$, då är $f(x) = a$ och $g(x) = b$ och vi kan sätta

$$q(x) = ab^{-1} \text{ och } r(x) = 0.$$

Induktionssteg: Antag att påståendet gäller för alla polynom av grad $< m$. Om

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0, \\ g(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \end{aligned}$$

så kan vi skriva

$$f(x) = a_m b_n^{-1} x^{m-n} \cdot g(x) + h(x),$$

där $\deg(h) < m$. Observera att $m - n \geq 0$.

Men nu kan vi använda induktionsantagandet och skriva $h(x) = q_h(x)g(x) + r(x)$ där $r(x) = 0$ eller $\deg(r) < \deg(g)$. Om vi sätter in detta i likheten ovan så får vi

$$\begin{aligned} f(x) &= a_m b_n^{-1} x^{m-n} \cdot g(x) + h(x) \\ &= a_m b_n^{-1} x^{m-n} \cdot g(x) + q_h(x)g(x) + r(x) \\ &= (a_m b_n^{-1} x^{m-n} + q_h(x))g(x) + r(x) \\ &= q(x)g(x) + r(x) \end{aligned}$$

där $q(x) = a_m b_n^{-1} x^{m-n} + q_h(x)$ och $r(x) = 0$ eller $\deg(r) < \deg(g)$. Alltså gäller påståendet för alla polynom $f(x), g(x) \in K[x] \setminus \{0\}$. □

Anmärkning 13.4. Notera att det är viktigt att vi har en kropp, annars är det inte säkert att b_n^{-1} existerar!

Exempel 13.5. Vi jämför med exemplet ovan:

$\frac{3}{2}x - 2$	$= a_m b_n^{-1} x^{m-n} + q_h(x)$
$3x^3 - \frac{5}{2}x^2 + \sqrt{2} = f(x)$	$2x^2 + x = g(x)$
$-(3x^3 + \frac{3}{2}x^2)$	$= a_m b_n^{-1} x^{m-n} \cdot g(x)$
$-4x^2 + \sqrt{2}$	$= h(x)$
$-(-4x^2 - 2x)$	
$2x + \sqrt{2}$	$= r(x)$

Exempel 13.6. Låt $\overline{5}x^2 + \overline{2}x + \overline{4}$ och $\overline{3}x + \overline{2}$ vara två polynom i $\mathbb{Z}_7[X]$. Då får vi:

$$\overline{5}x^2 + \overline{2}x + \overline{4} = (\overline{4}x + \overline{5})(\overline{3}x + \overline{2}) + \overline{1}.$$

Sats 13.7. Om K är en kropp så är $K[x]$ en Euklidisk ring med gradfunktionen deg som Euklidiska norm.

Bevis. Eftersom varje kropp är ett integritetsområde så är $K[x]$ ett integritetsområde och dessutom uppfyller då gradfunktionen $\deg : K[x] \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ följande:

$$\deg(fg) = \deg(f) + \deg(g) \geq \deg(f)$$

för alla $f, g \in K[x] \setminus \{0\}$. Enligt Lemma 13.3 uppfylls även det andra villkoret för att en ring ska vara Euklidisk. □

Exempel 13.8. $\mathbb{C}[x], \mathbb{Q}[x], \mathbb{Z}_7[x]$ är Euklidiska ringar.

Exempel 13.9. • De inverterbara heltalen är ± 1, vilket är precis de heltal som uppfyller $|n| = 1$.

- De inverterbara polynomen i $K[x]$, där K är en kropp, är precis de nollskilda konstanta polynomen, d.v.s. polynom av grad 0.
- Man kan visa att de enda inverterbara elementen i $\mathbb{Z}[\sqrt{2}]$ är ± 1, d.v.s. de enda elementen med norm 1.

I Euklidiska ringar är det enkelt att avgöra om ett element är inverterbart!

Lemma 13.10. Låt R vara en Euklidisk ring, med tillhörande norm N. Ett nollskilt element $a \in R$ är inverterbart om och endast om $N(a) = N(1_R)$.

Bevis. Antag att $a \in R$ är inverterbart. Då har vi att $N(1) \leq N(1 \cdot a)$ och $N(1) = N(a \cdot a^{-1}) \geq N(a)$ enligt egenskap (i) hos en Euklidisk norm och därför gäller $N(a) = N(1)$ om a är inverterbar.

Antag nu istället att $N(a) = N(1)$. Vi vet att det ska finnas q, r så att $1 = qa + r$ där antingen $r = 0$ eller $N(r) < N(a) = N(1)$. Det kan inte gälla att $N(r) < N(1)$ ty $N(1) \leq N(1 \cdot r) = N(r)$. Alltså är $r = 0$. Men det betyder att $1 = aq$ och a är alltså inverterbart! □

Sats 13.11. Varje Euklidisk ring är en huvudidealring.

Bevis. Låt R vara en Euklidisk ring och $I \subseteq R$ ett ideal. Vi vill visa att det finns ett element d så att $I = \langle d \rangle$. Vi kan anta att $I \neq \{0\}$, eftersom vi redan vet att nollidealet är ett huvudideal.

Låt nu d vara ett (nollskilt) element i I med minimal norm. Vi påstår nu att $I = \langle d \rangle$. Ta ett godtyckligt nollskilt element $a \in I$. Vi vet att det finns $q, r \in R$ så att $a = qd + r$ där $r = 0$ eller $N(r) < N(d)$ eftersom att R är Euklidisk. Men $N(r) < N(d)$ kan inte gälla eftersom att d hade minimal norm. Alltså är $r = 0$ och vi har $a = qd$. Detta gäller för alla $a \in I$ och alltså är $I = \langle d \rangle$. □

Anmärkning 13.12. Från beviset ser vi även att generatorn d är det elementet med minimal norm.

Korollarium 13.13. Varje Euklidisk ring är faktoriell.

Korollarium 13.14. Varje polynomring $K[x]$ över en kropp är faktoriell.

Proposition 13.15. Låt R vara en Euklidisk ring (eller mer generellt, en huvudidealring) och $I = \langle a_1, \ldots, a_n \rangle$. Då genereras I av den största gemensamma faktorn av $a_1, \ldots, a_n$.

Bevis. Eftersom att R är en Euklidisk ring så är det även en huvudidealring och dessutom en faktoriell ring. Det betyder att vi har en generator b. Vi vill nu visa att b kan väljas som den största gemensamma faktorn av $a_1, \ldots, a_n$, vilket existerar eftersom att R är faktoriell. Låt d beteckna den största gemensamma faktorn av $a_1, \ldots, a_n$. Då är d en faktor i varje element i I och därför gäller $I \subseteq \langle d \rangle$.

Eftersom varje a_i ligger i $I = \langle b \rangle$ så finns det $r_i \in R$ så att $r_i b = a_i$. Detta betyder att b är en gemensam delare hos $a_1, \ldots, a_n$. Men om b är en gemensam delare till samtliga a_i, då måste b vara en delare till den största gemensamma delaren, d.v.s. det finns $r \in R$ så att $br = d$. Men detta ger oss följande inklusion:

$$\langle d \rangle = \langle br \rangle \subseteq \langle b \rangle = I.$$

Vi har nu visat att vi har två inklusioner: $\langle d \rangle \subseteq I \subseteq \langle d \rangle$, alltså är $I = \langle d \rangle$ där d är den största gemensamma faktorn av $a_1, \ldots, a_n$. □

Exempel 13.16. Hitta generatorn för idealet

$$\langle x^2 - 1, x^2 + 2x + 1 \rangle \subseteq \mathbb{R}[x].$$

Vi faktoriserar de två polynomen:

$$x^2 - 1 = (x-1)(x+1), \quad x^2 + 2x + 1 = (x+1)^2.$$

Alltså är $\text{sgd}(x^2-1, x^2+2x+1) = x+1$. Enligt Proposition 13.15 så är $\langle x^2-1, x^2+2x+1 \rangle = \langle x+1 \rangle$.

13.2 Kopplingen mellan olika typer av ringar

Anmärkning 13.17. Vi har nu sett många olika typer av ringar, vi sammanfattar detta:

$$\{\text{Kroppar}\} \subsetneq \{\text{Euklidiska ringar}\} \subsetneq \{\text{Huvudidealringar}\} \subsetneq \{\text{Faktoriella ringar}\}$$
$$\subsetneq \{\text{Integritetsområden}\} \subsetneq \{\text{Kommutativa ringr}\} \subsetneq \{\text{Ringar}\}$$

- $\text{Mat}_{n\times n}(\mathbb{R})$ är en ring, men inte en kommutativ ring.
- $\mathbb{Z}_4$ är en kommutativ ring, men inte ett integritetsområde.
- $\mathbb{Z}[i\sqrt{5}]$ är ett integritetsområde men inte en faktoriell ring.
- $\mathbb{Z}[x]$ är en faktoriell ring men inte en huvudidealring. (T.ex $\langle 2, x \rangle$ är inte ett huvudideal.)
- $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ är en huvudidealring men inte en Euklidisk ring. (Beviset är svårt och kan inte bevisas med hjälp av det vi lärt oss i kursen.)
- $\mathbb{Z}$ är en Euklidisk ring men inte en kropp.
- $\mathbb{R}$ är en kropp.

Anmärkning 13.18. Om vi är i ett integritetsområde så har vi:

$$\{\text{Primelement}\} \subseteq \{\text{Irreducibla element}\} \subseteq \{\text{Nollskilda icke-inverterbara element}\}$$

I en faktoriell ring är dock den första inklusionen en likhet, d.v.s. ett element är primt om och endast om det är irreducibelt.

14 Gaussiska heltal

14.1 Definitionen av Gaussiska heltal

Nu ska vi titta på en speciellt exempel av en Euklidisk ring, nämligen de Gaussiska heltalen!

Lemma 14.1. Delmängden $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ är en delring.

Bevis. Vi kan enkelt kontrollera att $\mathbb{Z}[i]$ är sluten under multiplikation, addition och additiv invers, samt att $0, 1 \in \mathbb{Z}[i]$. Alltså är detta en delring. □

Korollarium 14.2. $\mathbb{Z}[i]$ är ett integritetsområde.

Definition 14.3. Vi kallar delringen $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ för de *Gaussiska heltalen*.

Sats 14.4. De Gaussiska heltalen är en Euklidisk ring med norm $N(a+bi) = |a+bi|^2 = a^2 + b^2$.

Bevis. Kom ihåg att $|zw| = |z||w|$ för alla $z, w \in \mathbb{C}$. Detta ger oss:

$$N(zw) = |zw|^2 = |z|^2|w|^2 \geq |z|^2 = N(z),$$

för varje $z, w \in \mathbb{Z}[i] \setminus \{0\}$. Så det första kravet är uppfyllt.

Nu vill vi visa att även det andra kravet är uppfyllt. Låt $z, w \in \mathbb{Z}[i] \setminus \{0\}$. Vi behöver hitta $q, r \in \mathbb{Z}[i]$ så att $z = qw + r$ där $r = 0$ eller $|r|^2 < |w|^2$. Eftersom att $z, w \in \mathbb{C}$ så kan vi dividera dessa i $\mathbb{C}$:

$$\frac{z}{w} = x + iy$$

där $x, y \in \mathbb{R}$ - de är alltså inte nödvändigtvis heltal. Vi kan dock hitta $a, b \in \mathbb{Z}$ så att $|x - a| \leq \frac{1}{2}$ och $|y - b| \leq \frac{1}{2}$. Vi får då:

$$0 \leq |\frac{z}{w} - (a + bi)|^2 = |(x + yi) - (a + bi)|^2 = (x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Om vi sätter $q = a + bi$ och $r = z - qw$ så får vi

$$z = qw + r$$

och

$$N(r) = |r|^2 = |z - qw|^2 = |w(\frac{z}{w} - q)|^2 = |w|^2|\frac{z}{w} - q|^2 \leq \frac{1}{2}|w|^2 < |w|^2 = N(w).$$

Vi har alltså hittat q, r så att $z = qw + r$ där $r = 0$ ($\Leftrightarrow |r| = 0$) eller $N(r) < N(w)$. Detta visar att de Gaussiska heltalen är en Euklidisk ring. □

Anmärkning 14.5. • Vi har alltså visat att de Gaussiska heltalen är en Euklidisk ring.

- Varje Euklidisk ring är en huvudidealring.
- Varje huvudidealring är faktoriell.
- De Gaussiska heltalen är en faktoriell ring!

14.2 Faktorisering av Gaussiska heltal

Vi ska nu ta fasta på att de Gaussiska heltalen är en faktoriell ring och undersöka hur vi faktorer ett Gaussiskt heltal. Vi behöver veta vilka de inverterbara elementen och de irreducibla elementen är innan vi börjar försöka faktorisera.

Anmärkning 14.6. Enligt Lemma 13.10 så är de inverterbara Gaussiska heltalen precis de med norm $1 = N(1)$. De enda Gaussiska heltalen med norm 1 är $\pm 1, \pm i$.

Sats 14.7. De irreducibla elementen i $\mathbb{Z}[i]$ är:

(i) Primtal $p \in \mathbb{Z}_{>0}$ så att $p \equiv 3 \pmod 4$,

(ii) Gaussiska heltal $a + bi$ sådana att $N(a + bi) = a^2 + b^2$ är ett primtal.

(iii) Gaussiska heltal som är associerade med de i (i) och (ii).

För att visa detta behöver vi följande resultat:

Sats 14.8. Ett primtal $p \in \mathbb{Z}_{>0}$ kan skrivas som $p = a^2 + b^2$, $a, b \in \mathbb{N}$ om och endast om $p = 2$ eller $p \not\equiv 3 \pmod 4$.

Anmärkning 14.9. Kom ihåg att $\mathbb{Z}[i]$ är en Euklidisk ring, och därför även en huvudidealring. Men då gäller det att ett element är irreducibelt om och endast om det är primt.

Nu kan vi bevisa föregående sats.

Bevis av Sats 14.7. Vi visar först att ifall ett element ingår i något av de tre fallen ovan så är det irreducibelt.

(i) Vi visar först att varje primtal p så att $p \equiv 3 \pmod 4$ är irreducibelt. Antag motsatsen, alltså att detta primtal p är reducibelt. Då finns Gaussiska heltal $a + bi, c + di$ så att

$$p = (a + bi)(c + di)$$

och $N(a + bi), N(c + di) > 1$. Då får vi att

$$(a^2 + b^2)(c^2 + d^2) = N(a + bi)N(c + di) = N(p) = p^2.$$

Men eftersom p är ett primtal så måste $p = a^2 + b^2$, men detta är en motsägelse då $p \equiv 3 \pmod 4$. Alltså är p irreducibelt.

(ii) Nu vill vi visa att om $N(a + bi) = a^2 + b^2$ är ett primtal, då är $a + bi$ irreducibelt. Antag att $a + bi = (c + di)(e + fi)$, då får vi

$$a^2 + b^2 = N(a + bi) = N(c + di)N(e + fi).$$

Men eftersom $a^2 + b^2$ är ett primtal så måste $N(c + di) = 1$ eller $N(e + fi) = 1$, men det betyder att $c + di$ eller $e + fi$ är inverterbart, alltså är $a + bi$ irreducibelt.

(iii) Varje element som är associerat till ett irreducibelt element är också irreducibelt. Detta visar att samtliga element som ingår i Fall (i), (ii) eller (iii) är irreducibla.

Vi vill nu visa att om ett element är irreducibelt så ingår det i Fall (i), (ii) eller (iii). Låt $z \in \mathbb{Z}[i]$ vara irreducibelt.

(i) Antag först att $N(z) \in \mathbb{Z}_{>1}$ innehåller en primtalsfaktor p som är kongruent med $3 \pmod 4$. Vi vill visa att vi är i Fall (i), upp till association. Vi vet alltså att p är irreducibelt i $\mathbb{Z}[i]$, och därför även primt. Men $p|N(z) = z\overline{z}$, vilket innebär att $p|z$ eller $p|\overline{z}$.

Om $p|z$ så är $z = pc$ för något $c \in \mathbb{Z}[i]$. Men z är irreducibelt och p är inte inverterbart, så då måste c vara inverterbart. Alltså är p och z associerade och vi är i Fall (i) (upp till associering).

Om $p|\overline{z}$ så finns det $x \in \mathbb{Z}[i]$ så att $\overline{z} = px$. Men eftersom $\overline{p} = p$ och $\overline{\overline{z}} = z$ så får vi $p\overline{x} = \overline{px} = \overline{\overline{z}} = z$, alltså har vi $p|z$ och likt ovan är p och z associerade. Vi är igen i Fall (i) (upp till association).

(ii) Antag nu att z är irreducibelt och det inte finns någon primtalsfaktor i $N(z)$ som är kongruent med $3 \pmod 4$. Vi vill visa att vi då är i Fall (ii), upp till association. Varje primtalsfaktor kan därför skrivas som $p = a^2 + b^2$ enligt Sats 14.8.

Titta nu på de Gaussiska heltalen $t = a + bi$ och $\bar{t} = a - bi$. Enligt det vi just visat är dessa irreducibla eftersom deras norm är ett primtal (Fall (ii)) och vi har $t\bar{t} = (a^2 + b^2)|N(z) = z\overline{z}$. Men då har vi såklart även $t|z\overline{z}$ och eftersom att t är primt så gäller $t|z$ eller $t|\overline{z}$, det senare är ekvivalent med att $\bar{t}|z$. Men eftersom z är irreducibelt betyder detta att antingen är t och z associerade eller $\bar{t}$ och z associerade. I vilket fall tillhör z Fall (ii) (upp till association).

□

Nu är vi redo att hitta en algoritm för att faktorisera ett Gaussiskt heltal!

Metod: $z = x + yi$	Exempel: $390 + 210i$
1. Bryt ut $d = \text{sgd}(x, y)$ och skriv $x + yi = d(s + ti)$, där $\text{sgd}(s, t) = 1$.	$d = \text{sgd}(390, 210) = 30$, $390 + 210i = 30 \cdot (13 + 7i)$, där $\text{sgd}(13, 7) = 1$
2. Faktorisera d i primtalsfaktorer: $d = p_1 p_2 \cdots p_k$	$30 = 2 \cdot 3 \cdot 5$
3. Faktorisera primtalsfaktorerna: a) $p \equiv 3 \pmod 4 \Rightarrow p$ irreducibelt.	$3 \equiv 3 \pmod 4 \Rightarrow 3$ irreducibelt
b) $p \not\equiv 3 \pmod 4 \Rightarrow$ $p = a^2 + b^2 = \underbrace{(a + bi)}_{\text{irreducibelt}} \underbrace{(a - bi)}_{\text{irreducibelt}}$	$2 \not\equiv 3 \pmod 4 \Rightarrow$ $2 = 1^2 + 1^2 = (1 + i)(1 - i)$
	$5 \equiv 1 \not\equiv 3 \pmod 4 \Rightarrow$ $5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i)$
	$\Rightarrow 30 = (1 + i)(1 - i) \cdot 3 \cdot (1 + 2i)(1 - 2i)$
Nu faktoriserar vi $w = s + ti$.	$w = 13 + 7i$
4. Beräkna normen $N(w) = s^2 + t^2$.	$N(13 + 7i) = 218$
5. Faktorisera normen i primtal p_i.	$218 = 2 \cdot 109$
6. Faktorisera faktorerna i irreducibla Gaussiska heltal: $p_i = q_i \cdot \overline{q_i}$.	$2 = (1 + i)(1 - i)$ $109 = 3^2 + 10^2 = (3 + 10i)(3 - 10i)$
$N(w) = q_1 \cdot \overline{q_1} \cdot q_2 \cdot \overline{q_2} \ldots q_m \cdot \overline{q_m}$	$N(13 + 7i) = (1 + i)(1 - i)(3 + 10i)(3 - 10i)$
7. Kontrollera om $q_i \mid w$ eller $\overline{q_i} \mid w$.	$\dfrac{13 + 7i}{3 - 10i} = \dfrac{-31 + 151i}{109} \notin \mathbb{Z}[i]$ $\dfrac{13 + 7i}{3 + 10i} = \dfrac{109 - 109i}{109} = 1 - i \in \mathbb{Z}[i]$
8. Om $q_i \mid w$ och $\dfrac{w}{q_i}$ inte är irreducibelt, börja om från 7. med $\dfrac{w}{q_i}$ istället för w.	$1 - i$ irreducibelt, annars hade vi fortsätt!

Sammanfattningsvis får vi:

$$\begin{aligned} 390 + 210i &= 30(13 + 7i) \\ &= 3(1 + i)(1 - i)(1 + 2i)(1 - 2i)(3 + 10i)(1 - i). \end{aligned}$$

Vi ser att $1 + i$ och $1 - i$ är associerade, eftersom $-i(1 + i) = 1 - i$, så vi kan skriva:

$$390 + 210i = -3(1 + i)^3(1 + 2i)(1 - 2i)(3 + 10i).$$

Anmärkning 14.10. (i) Observera att alla irreducibla faktorer i $N(w)$ kommer i konjugerade par, $q_i, \overline{q_i}$. Vi vet att $q_i \mid N(w) = w\overline{w}$. Eftersom q_i är irreducibel och därmed även primt så gäller $q_i \mid w$ eller $q_i \mid \overline{w}$. Men $q_i \mid \overline{w}$ är ekvivalent med $\overline{q_i} \mid w$. Vi har alltså $q_i \mid w$ eller $\overline{q_i} \mid w$.

(ii) Om en primfaktor $p = q_i\overline{q_i}$ i $N(w)$ uppfyller $p \equiv 1 \pmod 4$, så särskilt $p \neq 2 = (1+i)(1-i)$, så kommer precis en av q_i och $\overline{q_i}$ dela w. Om båda faktorerna skulle dela w så skulle $q_i\overline{q_i} = p|w$, där $w = s + ti$, eftersom i detta fall kommer q_i och $\overline{q_i}$ inte vara associerade. Men det är bara möjligt om $p|s$ och $p|t$ vilket är en motsägelse då $\text{sgd}(s,t) = 1$.

(iii) Faktorer $p \equiv 3 \pmod 4$ förekommer inte i $N(w)$, ty dessa är irreducibla, så om $p|N(w) = w\overline{w}$ så delar $p|w$ eller $p|\overline{w}$, där $w = s+ti$. I båda fallen måste $p|s$ och $p|t$ vilket inte kan vara fallet då $\text{sgd}(s,t) = 1$.

(iv) När man faktoriserar $N(z) = N(s+ti)$ i primtal i Steg 5, förekommer faktorn $2 = (1+i)(1-i)$ högst en gång. Annars kan man visa att $\text{sgd}(s,t) \neq 1$.

Tack för den här kursen!!

Kommande kurser

Vi ska nu prata om hur man kan generalisera olika saker inom matematiken som ni (troligtvis) sett tidigare. Det första är vektorrum. I Linjär algebra I och II har studerat reella vektorrum. Men istället för skalärer som är reella tal kan vi ha vilken kropp som helst. Mycket som ni har sett fungerar även för godtyckliga kroppar. Det här tittar man på i bland annat *Linjär algebra III*.

Om man tittar på en mängd tillsammans med endast en operation så kan man få något som kallas en grupp. Om vi t.ex. tar en ring och glömmer bort multiplikation får vi en (abelsk) grupp. Grupper studerar man i kursen *Algebraiska strukturer*.

Något som också är intressant är att se vad som händer ifall vi tittar på objekt som liknar vektorrum, men nu över en ring istället för en kropp. Detta kallas för en modul och det läser man om i *Moduler och homologisk algebra*. Moduler är väldigt användbara för att få mer information om en specifik ring.

Om man tar en ring som samtidigt är ett vektorrum över en kropp så får man något som kallas för en algebra. Precis som för ringar kan man titta på moduler över algebror. Det är precis detta som mitt forskningsområde handlar om! Dessa moduler kan vi även använda inom andra områden, som t.ex. topologi.