LMA110 VT2008
ARITMETIK OCH ALGEBRA DEL 2

Övningshäfte 3: Polynom och polynomekvationer

Syftet med denna övning är att repetera gymnasiekunskaper om polynom och polynomekvationer samt att bekanta sig med en del nya egenskaper hos polynom. Vi kommer att undersöka hur olika egenskaper hos polynom beror på deras koefficienter. Därför betraktar vi polynom med koefficienter i olika talområden: $\mathbb{Z}$ (heltaliga koefficienter), $\mathbb{Q}$ (rationella koefficienter), $\mathbb{R}$ (reella koefficienter), $\mathbb{C}$ (komplexa koefficienter). Vi betecknar med $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ alla polynom med koefficienter i respektive $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$. Om R betecknar ett av dessa talområden så skriver vi $R[X]$ för alla polynom med koefficienter i R. $R[X]$ kallas **polynomringen över** R. De viktigaste begreppen i detta avsnitt är

- Delbarhet av polynom
- Divisionsalgoritmen
- Största gemensamma delaren
- Reducibla och irreducibla polynom
- Nollställen till polynom (dubbla rötter, multipla rötter)
- Faktoruppdelningar av polynom i olika polynomringar

Vi följer kapitel 7 i Vretblads bok. För repetition av förkunskaper, läs R. Petterssons stencil från del 1 av kursen, avsnitt 6, 7, 8.

Övning A

Divisionsalgoritmen och faktorsatsen. Om $f(X)$ och $g(X) \neq 0$ är två polynom med koefficienter i R så betecknar vi med $q(X)$ och $r(X)$ *kvoten* och *resten* vid division av $f(X)$ med $g(X)$. Man har (om det "går att dividera" i talområdet R)

$$f(X) = g(X)q(X) + r(X), \text{ där grad } r(X) < \text{grad } g(X) \text{ eller } \ r(X) = 0.$$

Jämför detta med divisionsalgoritmen för heltal. Då får man ju

$$f = g \cdot q + r, \text{ där } \ 0 \leq r < g,$$

dvs. resten r är mindre än det man dividerar med, g. Nu får man istället en rest $r(X)$ som har *lägre grad* än det man dividerar med, $g(X)$.

För att få fram kvoten och resten kan man utföra en *polynomdivision*. (Detta är analogt med den heltalsdivision man gör när man beräknar kvot och rest för två stycken heltal.)

1. Bestäm kvoten och resten vid division av följande polynom:

   (a) $f(X) = X^2,\ g(X) = X - 1$ (testa att sätta $X = 1$ och kolla att ditt resultat stämmer!)

   (b) $f(X) = X^2 - X + 1,\ g(X) = X - 2$ (testa att sätta $X = 2$ och kolla att ditt resultat stämmer!)

   (c) $f(X) = X^4 + 2X^3 + 4X^2 + 2X + 3,\ g(X) = X^2 + 2X + 3$

2. Vad kan man säga om resten vid division av ett polynom $f(X)$ med ett polynom $X - a$? Vilken grad har resten? Bevisa att resten av $f(X)$ vid division med $X - a$ är lika med $f(a)$. Jämför 1a och 1b!

   Ledning. Enligt divisionsalgoritmen är $f(X) = (X - a)q(X) + r(X)$. Vad kan man säga om graden av $r(X)$? Beräkna resten genom insättning av $X = a$.

3. Beräkna resten vid division av $f(X)$ med $X - a$ då

   (a) $f(X) = X^3 - 2X^2 + 8X + 5,\ a = 3$

   (b) $f(X) = 3X^4 + 5X^2 - 4X - 11,\ a = -1$

   Du behöver inte utföra divisionen! Utnyttja istället förra uppgiften.

4. Vad säger faktorsatsen? Försök förklara hur man utnyttjar faktorsatsen för att lösa polynomekvationer.

5. Lös ekvationen $X^3 - 6X^2 + 11X - 6 = 0$ som har en rot $X = 1$.

Övning B

Reducibla och irreducibla polynom. Denna uppgift handlar om att dela upp polynom i en produkt av polynom av lägre grad. Man kan jämföra detta med att faktorisera heltal i primtalsfaktorer. Irreducibla polynom (sådana som inte kan faktoriseras) svarar då mot primtalen. Vi låter $K[X]$ vara en av polynomringarna $\mathbb{Q}[X]$, $\mathbb{R}[X]$ eller $\mathbb{C}[X]$.

1. Vad menas med ett reducibelt, respektive irreducibelt, polynom i $K[X]$?

2. Om möjligt, uppdela följande polynom i produkt av minst två polynom av lägre grad i $\mathbb{Q}[X]$, $\mathbb{R}[X]$ och $\mathbb{C}[X]$:

   (a) $f(X) = X^2 + 1$

   (b) $f(X) = X^2 - 2$

   (c) $f(X) = X^4 - 1$

   (d) $f(X) = X^4 + 2X^2 + 9$

   Vilka av polynomen är irreducibla i respektive polynomring?

   Ledning. Bestäm först alla faktorer $X - a$ av grad 1, dvs. sök lösningar a till $f(X) = 0$. Detta ger alltid en faktorisering i $\mathbb{C}[X]$. Om några av rötterna inte är reella så är det däremot inte en faktorisering i $\mathbb{R}$. Däremot kan man få reella faktorer av grad 2 genom

att multiplicera två förstagradsfaktorer med varandra på följande sätt: Om $f(X)$ har reella koefficienter och $f(a) = 0$ så är också $f(\bar{a}) = 0$. (Sats 7.20 i Vretblad) Det gäller att $(X - a)(X - \bar{a}) \in \mathbb{R}[X]$ och detta ger en faktor av grad 2 i $\mathbb{R}[X]$ även om inte a är reellt.

3. Låt $f \in K[X]$. Visa att

   (a) Om grad $f \geq 2$ och f har ett nollställe i K så är f reducibelt i $K[X]$.

   (b) Om grad $f = 2$ eller 3 så är f reducibelt i $K[X]$ då och endast då f har nollställen i K.

   (c) Konstruera ett exempel som visar att (b) inte gäller då grad $f = 4$. (Titta kanske på en uppgift du nyss löst.)

4. Utnyttja föregående uppgift för att visa att följande polynom är irreducibla i givna polynomringar.

   (a) $X^3 - 2$ i $\mathbb{Q}[X]$

   (b) $X^2 + 2X + 2$ i $\mathbb{R}[X]$

   (c) $X^4 + 1$ i $\mathbb{Q}[X]$

   Ledning till (c). Om ett polynom har heltaliga koefficienter och kan uppdelas i produkt av två polynom av lägre grad med rationella koefficienter så kan det också uppdelas i en produkt av två polynom med heltaliga koefficienter och samma grad. Detta påstående kallas ”Gauss lemma” och visas t ex i kursen ”Algebraisk talteori”. Du får använda detta (ganska enkla) resultat i (c).

Övning C

Delbarhet och största gemansamma delaren.

1. Vad menas med att ett polynom $d(X) \in K[X]$ delar ett polynom $f(X) \in K[X]$?

2. Vad menas med största gemensamma delaren till två polynom $f(X)$ och $g(X)$? Beräkna SGD(f, g) med hjälp av Euklides algoritm då

   (a) $f(X) = X^5 - X^4 + X^3 + X^2 - X + 1,\ g(X) = X^3 + 2X^2 + 2X - 1$

   (b) $f(X) = X^4 - 1,\ g(X) = 2X^3 - X^2 + 2X - 1$

   Anmärkning. På samma sätt som för heltal visar man att SGD$(f, g) = fp + gq$, där p och q är lämpliga polynom. Polynomen p och q kan beräknas med hjälp av Euklides algoritm.

3. Bevisa att om ett polynom d delar produkten fg av två polynom och d är relativt primt med f (dvs SGD$(d, f) = 1$) så d delar g. Vad säger motsvarande sats om heltalen?

Övning D

Lösning av ekvationer. En polynomekvation är en ekvation av typen $f(X) = 0$, där $f(X)$ är ett polynom. Svårigheterna med att lösa sådana ekvationer växer med graden. Helt banalt löser man förstagradsekvationer: $ax+b = 0$, $a \neq 0$ ger $x = -\frac{b}{a}$. För andragradsekvationer $ax^2+bx+c = 0$, $a \neq 0$, har man den välkända formeln

$$x_{1,2} = -\frac{b}{2a} \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

som kan härledas med kvadratkomplettering. För ekvationer av grad 3 och 4 existerar mycket mer komplicerade formler som man lyckades härleda under 1500–talet. Man vet att för helt godtyckliga ekvationer av grad ≥ 5 är det inte möjligt att uttrycka rötterna med hjälp av de fyra räknesätten och rotutdragningar som tillämpas på ekvationens koefficienter. Detta visades av den store norske matematikern N.H. Abel* och den lika berömde franske matematikern É. Galois†. Rent praktiskt löser man ofta polynomekvationer med numeriska metoder som ger helt tillfredsställande närmevärden till lösningarna. Ibland utnyttjas enkla satser vars tillämpningsmöjligheter är ganska begränsade när det gäller att lösa ekvationer, men som är intressanta ändå. Vi har två sådana satser i kursboken:

Sats 7.27 *Om ett rationellt tal $\frac{p}{q}$, där $p, q \in \mathbb{Z}$, SGD$(p, q) = 1$, är ett nollställe till polynomet $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ med heltaliga koefficienter a_i, så är p en delare till den lägsta koefficienten a_0 och q är en delare till den högsta koefficienten a_n.*

Sats 7.20 *Om α är ett (komplext) nollställe till ett polynom $f(X)$ med reella koefficienter, dvs $f(\alpha) = 0$, så är också $\bar{\alpha}$ ett nollställe till $f(X)$, dvs $f(\bar{\alpha}) = 0$.*

1. Lös följande ekvationer:
   (a) $X^3 - 6X^2 + 11X - 6 = 0$
   (b) $2X^3 - X^2 + 2X - 1 = 0$
2. Man vet att polynomet $X^4 - 2X^3 + 3X^2 - 2X + 2$ har ett nollställe $1 + i$. Bestäm alla andra nollställen till polynomet.

*Nils Henrik Abel (5/8 1802 – 6/4 1829). Abel visade sina resultat om ekvationer av grad ≥ 5 när han var 19 år gammal. Han löste många viktiga matematiska problem inom flera olika områden. I Oslo finns hans monument i den Kungliga Parken. Sedan 2003 delar Norges vetenskapsakademi ut *abelpriset* varje år, en matematisk motsvarighet till nobelpriset.

†Évariste Galois (25/10 1811 – 30/5 1832). Under sitt mycket korta liv skapade Galois en mycket viktig teori idag kallad ”Galoisteori” som sysslar med polynomekvationer. Han visade hur abstrakta matematiska teorier kan bidra till att lösa komplicerade matematiska problem. På det sättet bidrog han till utvecklingen av den moderna matematiken. Galois lade grunden för gruppteorin och teorin för ändliga kroppar. Dessa teorier har stor betydelse för hela matematiken och dess tillämpningar inom fysik, kemi, kodningsteori och radarkommunikation.

Övning E

Derivatan av ett polynom och multipla rötter. Låt $f(X) = a_0 + a_1X + \ldots + a_nX^n \in K[X]$. Derivatan av $f(X)$ definieras helt formellt som

$$f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

Man kan utan svårigheter kontrollera de vanliga deriveringsreglerna

$$(f+g)' = f' + g' \quad \text{och} \quad (fg)' = f'g + fg'.$$

Det finns följande viktiga samband mellan multipla rötter till en polynomekvation $f(X) = 0$ och derivatan $f'(X)$:

Sats. Ett tal $a \in K$ är ett multipelt nollställe till $f \in K[X]$ (dvs a har multipliciteten > 1) då och endast då $f(a) = f'(a) = 0$.

Bevis. "$\Rightarrow$" Antag att a har multipliciteten åtminstone 2. Då är enligt faktorsatsen $f(X) = (X-a)^2q(X)$ för något polynom $q(X) \in K[X]$. Det ger $f'(X) = 2(X-a)q(X)+(X-a)^2q'(X)$ så att $f(a) = f'(a) = 0$.

"$\Leftarrow$" Omvänt antag att $f(a) = f'(a) = 0$ och att multipliciteten av a är 1, dvs $f(X) = (X - a)q(X)$ och $q(a) \neq 0$. Då är $f'(X) = q(X) + (X - a)q'(X)$ så att $f'(a) = q(a) \neq 0$. Detta är en motsägelse och därmed kan inte a ha multipliciteten 1 om $f(a) = f'(a) = 0$. Alltså måste den vara åtminstone 2 och därmed är saken klar.

1. Visa att 1 är ett multipelt nollställe till
   (a) $X^6 - 6X + 5 = 0$
   (b) $X^n - nX + (n-1) = 0$, där n är ett heltal med $n > 1$.
2. Bestäm reella tal a och b så att polynomet $f(X) = aX^{2000} + bX^{1999} + 1$ är delbart med $(X-1)^2$.
3. Lös uppgift 7.113 (7.58) i Vretblads bok.

Övning F

Samband mellan koefficienter och rötter

1. Lös följande kvadratiska ekvationer genom att utnyttja sambandet mellan rötter och koefficienter, Vretblad sid. 172 (177) (utan formler eller kvadratkomplettering):

(a) $X^2 - 6X + 8 = 0$

(b) $X^2 + 5X + 6 = 0$

2. Låt x_1, x_2, x_3 beteckna rötterna till ekvationen $aX^3 + bX^2 + cX + d = 0$, $a \neq 0$. Skriv ut sambanden mellan ekvationens rötter och koefficienter. Ange en ekvation av grad 3 med rötterna 1,2,3.

3. Låt x_1, x_2 och x_3 vara rötterna till ekvationen $X^3 - 5X^2 + 6X + 7 = 0$. Beräkna $x_1^2 + x_2^2 + x_3^2$ och $x_1^3 + x_2^3 + x_3^3$ (utan att bestämma rötterna).

Övning G

Låt $N = a_n a_{n-1} \ldots a_1 a_0$ beteckna ett naturligt tal med siffrorna a_i (t ex $N = 452 = a_2 a_1 a_0$ med $a_0 = 2$, $a_1 = 5$, $a_2 = 4$). Betrakta polynomet

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

(a) **Delbarhetskriterium vid division med 3 och 9.** Visa att N är delbart med 3 (respektive 9) då och endast då siffersumman i N är delbar med 3 (respektive 9).

Ledning. Dividera $f(X)$ med $X - 1$. Observera att $N = f(10)$ och att siffersumman i N är lika med $f(1)$. Sätt in $X = 10$ och drag slutsatsen att N och dess siffersumma ger samma rest vid division med 3 (respektive 9).

(b) **Delbarhetskriterium vid division med 11.** Visa att N ger samma rest vid division med 11 som sin *alternerande siffersumma* $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ (exempel: 1936 är delbart med 11 ty $6 - 3 + 9 - 1 = 11$ är delbart med 11).

Ledning. Gör som i (a), men ersätt $X - 1$ med $X + 1$.

Följande övningar i Vretblads bok rekommenderas för självstudier:

Vretblad: 7.24 (7.9), 7.25 (7.10), 7.35 (7.16), 7.41 (7.21), 7.45 (7.22), 7.48 (7.23), 7.49 (7.24), 7.52 (7.25), 7.65 (7.30), 7.67 (7.33), 7.107 (7.52), 7.109 (7.54), 7.114 (7.59), 7.117 (7.62).