Assignment 5

Paul Vrbik : 301056796 : MATH 895 : Summer 2007

August 9, 2007

Question 1: Minimal Polynomials

(i)

Let α be algebraic over $\mathbb{C}$. Let $m(z) \in \mathbb{Q}[z]$ be a non-zero monic polynomial of minimal degree such that $m(\alpha) = 0$. Prove that $m(z)$ is irreducible over $\mathbb{Q}$ and unique.

Uniqueness

> Suppose there are two monic polynomials $m(z)$ and $n(z) \in \mathbb{Q}[z]$ of minimal degree ($\texttt{degree}(m) = \texttt{degree}(n)$) where $m(\alpha) = n(\alpha) = 0$. Consider the polynomial $f(z) = m(z) - n(z)$ where $f(\alpha) = m(\alpha) - n(\alpha) = 0$. Since $m(z)$ and $n(z)$ are monic and of the same degree their leading terms will cancel when taking the difference. This implies that $\texttt{degree}(f) < \texttt{degree}(m)$ and it follows that $m(z)$ is not minimal (f is), a contradiction. Therefore $m(z)$ is unique. □

Irreducibility

> Suppose $m(z) = f(z) \cdot g(z)$ where $f, g \in \mathbb{Q}[z]$, $\texttt{degree}(f) \neq 0$ and $\texttt{degree}(g) \neq 0$. We have $m(\alpha) = 0 \Rightarrow f(\alpha) \cdot g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \vee g(\alpha) = 0$. Without loss of generality suppose $f(\alpha) = 0$. Since $\texttt{degree}(m) = \texttt{degree}(f) + \texttt{degree}(g)$ we have that $\texttt{degree}(f) < \texttt{degree}(m)$ which means that $m(z)$ is not minimal (f is), a contradiction. Therefore $m(z)$ is irreducible. □

(ii)

I define the maple functions:

```
> r:=(ma,mb)->resultant(ma,resultant(mb,z-x-y,y),x):
> check:=(f,x)->expand(eval(f,z=x)):
```

$\alpha = 1 + \sqrt{2}$

```
> c:=1+sqrt(2):
>
> ma:=x-1:
> mb:=y^2-2:
>
> mc:=sort(r(ma,mb));
                                      2
                              mc := z  - 2 z - 1

> check(mc,c);
                                       0

> irreduc(mc);
                                      true
```

$\alpha = 1 + \sqrt{2} + \sqrt[4]{2}$

```
> c:=1+2^(1/2)+2^(1/4):
>
> ma:=eval(mc,z=x):
> mb:=y^4-2:
>
> mc:=sort(r(ma,mb));
                8       7       6       5       4       3       2
        mc := z  - 8 z  + 20 z  - 8 z  - 30 z  + 24 z  - 52 z  + 120 z - 63
```

```
> check(mc,c);
                                        0

>
> mc1,mc2:=op(factor(mc));
                    4      3      2               4      3      2
      mc1, mc2 := z  - 4 z  + 2 z  + 12 z - 9, z  - 4 z  + 2 z  - 4 z + 7

> check(mc1,c); #non-zero so mc2 must be the minimal poly.
                                   1/2       (1/4)
                               16 2    + 16 2

> check(mc2,c);
                                        0

>
> mc:=mc2:
> irreduc(mc);
                                      true
```

$\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$

```
> c:=sqrt(2)+sqrt(3)+sqrt(5):
>
#We have that the minimal polynomial for sqrt(2)+sqrt(3) is
> ma:=x^4-10*x^2+1:
> mb:=y^2-5:
>
> mc:=r(ma,mb);
                               6    8        4               2
                  mc := -40 z  + z  + 352 z  + 576 - 960 z

> check(mc,c);
                                        0

> irreduc(mc);
                                      true
```

Question 2: Cyclotomic Polynomials

(i)

```
> T:=table():
> T[1]:={x-1}:
> all:=T[1]:
> for n from 2 to 12 do
>     fs:=factor(x^n-1):
>     T[n]:={op(fs)} minus all:
>     all:=all union T[n]:
> end do:
> for i from 1 to 12 do
>     printf("%d  %a \n", i, sort(op(T[i]))):
> end do:
```

```
n  \phi_n(x)
1  x-1
2  x+1
3  x^2+x+1
4  x^2+1
5  x^4+x^3+x^2+x+1
6  x^2-x+1
7  x^6+x^5+x^4+x^3+x^2+x+1
8  x^4+1
9  x^6+x^3+1
10  x^4-x^3+x^2-x+1
11  x^10+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1
12  x^4-x^2+1
```

(ii)

Denoting ζ_n to be the primitive nth root of unity we define

$$\Phi_n(x) = \prod_{\mathtt{gcd}(m,n)=1} (x - \zeta_n^m)$$

and show that

$$\Phi_n(x) = \frac{x^n - 1}{\mathtt{lcm}\left(x^m - 1 \middle| m|n, m \neq n\right)}$$

where $x^n - 1 = \prod_{m=1}^{n}(x - \zeta_n^m)$

Claim

$$\mathtt{lcm}\left(x^m - 1 \middle| m|n, m \neq n\right) = \prod_{\mathtt{gcd}(m,n)\neq 1} (x - \zeta_n^m)$$

- Since I am lazy I will write $\mathtt{lcm}\,(-)$ and $\prod(-)$ instead.

Proof of claim

Consider any m such that $m|n$, $m \neq n \Rightarrow \mathtt{gcd}\,(m,n) \neq 1$ it follows

$$\begin{aligned} x^m - 1 &= (x - \zeta_{n/m}) \cdots (x - \zeta_{n/m}^k) \cdots (x - \zeta_{n/m}^{n/m}) \\ &= (x - \zeta_n^m) \cdots (x - \zeta_n^{m \cdot k}) \cdots (x - \zeta_n^n) \end{aligned}$$

For any k we have $\texttt{gcd}\,(m \cdot k, n) \neq 1 \Rightarrow (x - \zeta_n^{m \cdot k}) \big| \prod(-)$ and it follows that for any m where $m|n$ and $m \neq n$,

$$(x^m - 1) \big| \prod(-) \Rightarrow \texttt{lcm}\,(-) \big| \prod(-).$$

For any m such that $\texttt{gcd}\,(m, n) = g \neq 1$ we have $\bar{m}$ such that $g \cdot \bar{m} = m$. Giving $(x - \zeta_n^m) = (x - \zeta_n^{g \cdot \bar{m}}) = (x - \zeta_{n/g}^{\bar{m}}) \big| (x^{n/g} - 1)$. Since $\frac{n}{g} \big| n \Rightarrow (x^{n/g} - 1) \big| \texttt{lcm}\,(-) \Rightarrow (x - \zeta_n^m) \big| \texttt{lcm}\,(-)$ it follows that

$$\prod(-) \Big| \texttt{lcm}\,(-)\,.$$

Collectively these two conclusions imply the claim.

Proof of main result

$$\frac{x^n - 1}{\texttt{lcm}\left(x^m - 1 \middle| m|n, m \neq n\right)} = \frac{\prod_{m=1}^{n}(x - \zeta_n^m)}{\prod_{\texttt{gcd}(m,n) \neq 1}(x - \zeta_n^m)} = \prod_{\texttt{gcd}(m,n)=1}(x - \zeta_n^m) = \Phi_n(x)$$

□

Justification of algorithm

The algorithm that implements this result uses $\texttt{lcm}\left(x^{n/p} - 1 \middle| p \text{ is a prime divisor of } n\right)$ instead. We observe for any m such that $m|n$, $m \neq n$ that

$$(x^m - 1) = \prod_{\bar{k}=1}^{m}(x - \zeta_m^{\bar{k}}) = \prod_{\bar{k}=1}^{m}(x - \zeta_n^{\frac{\bar{k}n}{m}})$$

where there is some prime divisor p of n such that $1 \leq \frac{\bar{k}n}{mp} \leq \frac{mn}{mp} = \frac{n}{p}$ and choosing $k = \frac{\bar{k}n}{mp}$ we have that $(x - \zeta_n^{\frac{\bar{k}n}{m}}) = (x - \zeta_n^{kp}) = (x - \zeta_{n/p}^{k})$.

This means $\forall m\,(m|n, m \neq n)$, $\forall \bar{k}\,\left(1 \leq \bar{k} \leq m\right)$, $\exists p$, p a prime divisor of n such that $(x - \zeta_n^{\frac{\bar{k}n}{m}}) \Big| \prod_{k=1}^{n/p}(x - \zeta_n^{kp})$. So it suffices to only use prime divisors of n.

Code

```
getCyc:=proc(n)
local ds, ps, L:

    if n=1 then
        x-1:
    elif isprime(n) then
        add(x^i,i=0..n-1);
    else
        ps:=select(`isprime`,numtheory[divisors](n));
        ds:=seq(n/p, p in ps):
        L:=lcm(seq(x^d-1,d in ds)):
        quo(x^n-1,L,x);
    end if:

end proc:
```

Output

```
> f:=0: i:=0:
> while norm(f,infinity)<3 do
>     i:=i+1:
>     f:=getCyc(i):
> end do:

> i;
                                        385

> quit:
```

Question 3: Solving Linear Systems over Number Fields

Code

```
with(LinearAlgebra):

GE:=proc(A,b,m)
local n,B,L,k,i,j,piv:
#   cleaning up
    n:=(Dimensions(A))[1]:
    B:=<A|b>:
    B:=map(rem,B,m,e);
    L:=ilcm(seq(seq(denom(B[i,j]), i=1..n), j=1..n+1)):
    B:=B*L:

    for k to n do
        i:=k:

        while i<=n and B[i,k]=0 do
            i:=i+1:
        end do:

        if i>n then
            error "A is singular":
        end if:

#       interchange rows
        for j from k to n+1 do
            B[i,j],B[k,j]:=B[k,j],B[i,j]:
        end do:

        gcdex(B[k,k],m,e,'piv'):

        for j from k to n+1 do
            B[k,j]:=rem(piv*B[k,j],m,e):
        end do:

        for i from k+1 to n do
            for j from k+1 to n+1 do
                B[i,j]:=rem(B[i,j]-B[i,k]*B[k,j],m,e):
            end do:
            B[i,k]:=0:
        end do:
    end do:

    for k from n by -1 to 1 do
        for j from k-1 by -1 to 1 do
            B[j,n+1]:=rem(B[j,n+1]-B[j,k]*B[k,n+1],m,e):
            B[j,k]:=0;
        end do:
    end do:

    return Vector([seq(B[k,n+1],k=1..n)]):
end proc:
```

Output

```
> read "GE.mpl":
>
> read "systems/sys49.txt":
> Dimensions(A)[1];
                                        49

> st:=time():
> x:=GE(A,b,M):
> time()-st;
                                      29.932

> convert(map(rem,A.x-b,M,e),set);
                                       {0}

>
> read "systems/sys100.txt":
> Dimensions(A)[1];
                                       100

> st:=time():
> x:=GE(A,b,M):
> time()-st;
                                     672.371

> convert(map(rem,A.x-b,M,e),set);
                                       {0}

>
> read "systems/sys196.txt":
> Dimensions(A)[1];
                                       196

> st:=time():
> x:=GE(A,b,M):
> time()-st;
                                     1994.514

> convert(map(rem,A.x-b,M,e),set);

                                       {0}
```

Question 4: A Modular Algorithm

Code

```
MGE:=proc(inA,inb,m,k)
local n,A,L,b,p,P,x,badprime,betas,xpbs,beta,Apb,bpb,xpb,xp,i,xx,pass:

    n:=LinearAlgebra[Dimension](inb):

    # cleaning up
    A:=map(rem,inA,m,e):
    L:=ilcm(seq(seq(denom(A[i,j]),i=1..n),j=1..n)):
    A:=A*L:
    b:=inb*L:

    # p:=2^30:
    p:=2^60:
    P:=1:
    x:=Vector(1..n,0):

    while true do

        p:=nextprime(p):

        while not(1 = p mod k) do
            p:=nextprime(p):
        end do:

        printf("p=%d \n", p);

        badprime:=false:

        betas:=map(x->x[1],Roots(m) mod p):

        xpbs:=NULL:

        for beta in betas do
            Apb:=eval(A,e=beta) mod p:
            bpb:=eval(b,e=beta) mod p:
            xpb:=Linsolve(Apb,bpb) mod p:

            #a bad prime/eval point is one that makes A go singluar.
            if type(xpb,function) then
                badprime:=true:
                break:
            end if:

            xpbs:=xpbs,xpb:
        end do:

        if not(badprime) then
            xp:=Vector(1..n,0):

            for i from 1 to n do
```

```
            xp[i]:=Interp(betas,[seq(v[i],v in xpbs)],e) mod p:
        end do:

        x:=chrem([x,xp],[P,p]):
        P:=P*p:

        xx:=Vector(1..n,0):
        pass:=true:

        for i from 1 to n do
            xx[i]:=iratrecon(x[i],P):

            if xx[i]=FAIL then
                pass:=false:
                break:
            end if:
        end do:

        if pass and convert(map(rem,A.xx-b,m,e),set)={0} then
            return xx:
        end if:

    end if:

  end do:

end proc:
```

Output

```
> read "MGE.mpl":

> read "systems/sys49.txt":
> k:=5:
> st:=time():
> x:=MGE(A,b,M,k):
p=1152921504606847081

> time()-st;
                                      2.572

> c:=map(rem,(A.x-b),M,e):
> convert(c,set);
                                       {0}

> read "systems/sys100.txt":
> k:=24:
> st:=time():
> x:=MGE(A,b,M,k):
p=1152921504606847009

> time()-st;
                                      31.929
```

```
> c:=map(rem,(A.x-b),M,e):
> convert(c,set);
                                      {0}

> read "systems/sys196.txt":
> k:=3:
> st:=time():
> x:=MGE(A,b,M,k):
p=1152921504606847009
p=1152921504606847081
p=1152921504606847123
p=1152921504606847189

> time()-st;
                                    326.183

> c:=map(rem,(A.x-b),M,e):
> convert(c,set);
                                      {0}

> quit:
```