Rowan Lochrin
MATH415B - Klaus Lux
1/29/18
Homework 5

12 Determine which of the polynomials are irreducible over Q.

1. $x^5 + 9x^4 + x^2 + 1$ By Eisenstein's criterion $p = 3$

$$3 \nmid, 3 \mid 9, 3 \mid 2, 3 \mid 6, 3^2 \nmid 6$$

2. $x^4 + x + 1$ Suppose
$$x^4 + x + 1 = 0$$
by the mod p irreduciblity test we seek to show that it is irreducible mod 2. Note that because 1 is a term it can have no linear factors so
$$x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$$
and we can no pair of values for $a, b \in 0, 1$ make this true.

3. $x^4 + 3x^2 + 3$ By Eisenstein's criterion $p = 3$
$$3 \nmid 1, 3 \mid 3, 3 \mid 3, 3^2 \nmid 3$$

4. $x^5 + 5x^2 + 1$ by the mod p irreduciblity test we seek to show that it is irreducible mod 5.
$$x^5 + 1 \text{ mod } 5$$
We can see that it has no linear factors

5. $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$
$$\begin{aligned} &14(x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + (3/14)) \\ &= 14x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3 \end{aligned}$$
By Eisenstein's criterion $p = 3$
$$3 \nmid 14, 3 \mid 63, 3 \mid 210, 3 \nmid 6, 3 \mid 84, 3 \mid 3, 3^2 \mid 3$$
So because our original polynomial is a unit times a reducible polynomial it also must be reducible.

20 Prove that, for every positive integer n, there are infinitely many polynomials of degree n in $Z[x]$ that are irreducible over q.

Proof. For any prime p consider the polynomial
$$(p + 1)x^n + px^{n-1} + ... + p$$
We can see that
$$p \nmid (p + 1), p \mid p, p^2 \mid p$$
so Eisenstein's criterion it is irreducible in Q and therefore must be irreducible of Z. Because there are infinitely many primes there must be infinitely many such polynomials. □

24 Given that π is not the zero of a nonzero polynomials with rational coefficients, prove that π^2 cannot be written in the form $a\pi + b$ where a and b are rational.

Proof. Because π is a nonzero polynomial, Deg $\pi \geq 1$ so deg $\pi^2 > 2$ deg deg $a\pi + b =$ deg π. $\square$

27 Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \in Z[x]$$

and $a_n \neq 0$. Prove that if r and s are relatively prime $f(r/s) = 0$, then $r \mid s$ and $s \min a_n$.

Proof.

$$f(r/s) = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + ... + a_0 = 0$$
$$s^n f(r/s) = a_n r^n + a_{n-1}r^{n-1}s + ... + s^n a_0 = 0$$

Implying

$$\begin{aligned} -a_n r^n &= a_{n-1}r^{n-1}s + ... + s^n a_0 \\ &= s(a_{n-1}r^{n-1} + ... + s^{n-1}a_0) \end{aligned}$$

So $s \mid -a_n r^n$ meaning that either $s \mid a_n$ or $s \mid -r^n$ because r and s are relatively prime the latter is impossible. Also note that

$$\begin{aligned} -s^n a_0 &= a_n r^n + a_{n-1}r^{n-1}s + ... + s^{n-1}ra_1 \\ &= r(a_n r^{n-1} + a_{n-1}r^{n-2}s + ... + s^{n-1}a_1) \end{aligned}$$

so $r \mid s^n a_0$ implying $r \mid a_0$ by the same logic. $\square$

28 Let F be a field and let $p(x), a_1(x), a_2(x), ..., a_k(x) \in F[x]$, where $p(x)$ is irreducible over F. If $p(x) \mid a_1(x), a_2(x), ..., a_k(x)$, show that $p(x)$ divides some $a(x)$.
Because p is irreducible we know that if $p(x) \mid a_1(x)$ or $p(x) \mid a_2a_3...a_n$ if p does not divided a_1 then $p(x) \mid a_2$ or $p(x) \mid a_3(x)a_4(x)...a_n(x)$ continuing in this way we can see that either p divides some $a_i(x)$ along the way or p divides $a_n(x)$.

30 If p is a prime, prove that $x^{p-1} - x^{p-2} + x^{p-3} - ... - x + 1$ is irreducible over Q.
If $f(x)$ is irreducible in a field then $f(-x)$ must also be irreducible in that field. Recall the corollary about cyclotomic polynomials, that is $\frac{x^p-1}{x-1}$ irreducible so

$$\frac{(-x)^p - 1}{(-x) - 1} = x^{p-1} - x^{p-2} + x^{p-3} - ... - x + 1$$

Must also be irreducible.

GAP 17.1 Factors of $x^n - 1$

$$\begin{aligned} n = 6 &: x - 1, x + 1, x^2 - x + 1, x^2 + x + 1 \\ n = 8 &: x - 1, x + 1, x^2 + 1, x^4 + 1 \\ n = 12 &: x - 1, x + 1, x^2 - x + 1, x^2 + 1, x^2 + x + 1, x^4 - x^2 + 1 \\ n = 20 &: x - 1, x + 1, x^2 + 1, x^4 - x^3 + x^2 - x + 1, x^4 + x^3 + x^2 + x + 1, x^8 - x^6 + x^4 - x^2 + 1 \\ n = 30 &: x - 1, x + 1, x^2 - x + 1, x^2 + x + 1, x^4 - x^3 + x^2 - x + 1, x^4 + x^3 + x^2 + x + 1, \\ &\quad x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 \end{aligned}$$

Conjecture: All coefficients on factors of $x^n - 1$ will be one or zero. Also the degree of any factor of $x^n - 1$ is a power of two.

$n = 40 : x-1, x+1, x^2-x+1, x^2+x+1, x^4-x^3+x^2-x+1, x^4+x^3+x^2+x+1...$
$n = 50 : x-1, x+1, x^4-x^3+x^2-x+1, x^4+x^3+x^2+x+1, x^{20}-x^{15}+x^{10}-x^5+1...$

We can see we've found a counter example to the second part of our conjecture as 20 is not a power of two.

GAP 17.2

1. $x^5+9x^4+12x^2$ This looks like an example of Eisenstein criterion but it's not.

$$x^5+9x^4+12x^2 = x^2(x^3+9x^2+12)$$

2. x^4+x+1 Is irreducible.
3. x^4+3x^2+1

$$x^4+3x^2+1 = x^4+1 \text{ mod } 3$$

   So it is irreducible in Q.
4. x^5+5x^2+1 Is irreducible.
5. $21x^3-3x^2+2x+9$

$$21x^3-3x^2+2x+9 = x^3+x^2+1 \text{ mod } 2$$

   So it is irreducible in Q.