

## AN IRREDUCIBLE POLYNOMIAL THAT FACTORS MOD $p$ FOR ALL $p$

Let  $\alpha = \sqrt{2} + \sqrt{3}$ . To find a monic polynomial in  $\mathbf{Q}[T]$  with  $\alpha$  as a root, we proceed as follows:

$$\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \implies \alpha^2 - 5 = 2\sqrt{6} \implies (\alpha^2 - 5)^2 = 24 \implies \alpha^4 - 10\alpha^2 + 25 = 24.$$

Thus  $\alpha^4 - 10\alpha^2 + 1 = 0$ , so  $\sqrt{2} + \sqrt{3}$  is a root of

$$T^4 - 10T^2 + 1.$$

This polynomial is irreducible in  $\mathbf{Q}[T]$ ; see the textbook on page 272. It is a really intriguing example of an irreducible polynomial because neither of the two standard irreducibility tests in  $\mathbf{Q}[T]$  (reduction mod  $p$  and the Eisenstein criterion) can be applied: for every prime  $p$ ,  $T^4 - 10T^2 + 1 \pmod{p}$  is reducible, and for no  $c \in \mathbf{Z}$  is  $(T + c)^4 - 10(T + c)^2 + 1$  Eisenstein at some prime.

We will see later in the course why this polynomial is reducible mod  $p$  for all  $p$ . That this polynomial doesn't have an Eisenstein translate is a homework problem. The evidence below, taken over all primes  $p < 50$ , supports the claim that the polynomial is always reducible mod  $p$ . It is not a proof of anything, but is interesting data.

$p$	$T^4 - 10T^2 + 1 \pmod{p}$
2	$(T + 1)^4$
3	$(T^2 + 1)^2$
5	$(T^2 + 2)(T^2 - 2)$
7	$(T^2 + T - 1)(T^2 - T - 1)$
11	$(T^2 + T + 1)(T^2 - T + 1)$
13	$(T^2 + 5T + 1)(T^2 - 5T + 1)$
17	$(T^2 + 5T - 1)(T^2 - 5T - 1)$
19	$(T^2 + 4)(T^2 + 5)$
23	$(T + 2)(T - 2)(T + 11)(T - 11)$
29	$(T^2 + 8)(T^2 + 11)$
31	$(T^2 + 15T - 1)(T^2 - 15T - 1)$
37	$(T^2 + 7T + 1)(T^2 - 7T + 1)$
41	$(T^2 + 7T - 1)(T^2 - 7T - 1)$
43	$(T^2 + 9)(T^2 + 24)$
47	$(T + 5)(T - 5)(T + 19)(T - 19)$

Is it some freakish property that the polynomial  $T^4 - 10T^2 + 1$  is irreducible in  $\mathbf{Q}[T]$  but factors modulo  $p$  for all  $p$ ? No! Using concepts that will be developed later in this course, we will see why this kind of example (a polynomial that is irreducible over  $\mathbf{Q}$  but reducible mod  $p$  for all  $p$ ) is actually very common. It's about as common as a "random" group not being a cyclic group, and surely you would believe that a "random" group is usually not cyclic.