

## FIELD THEORY PROBLEM SET 2

MATHCAMP 2003

We say that a polynomial  $p(x) = a_n x^n + \cdots + a_1 x + a_0$  is *monic* if  $a_n = 1$ .

1. Compute the greatest common divisor of the two polynomials  $x^7 + 4x^3 + 1$  and  $x^3 + 2x + 2$  in  $\mathbb{F}_7[x]$ .
2. List all irreducible monic polynomials of degree 1 over  $\mathbb{F}_3$ . List all irreducible monic polynomials of degree 2 over  $\mathbb{F}_3$ .
3. Factor  $x^3 - x$  into irreducibles over  $\mathbb{F}_3$ . Factor  $x^9 - x$  into irreducibles over  $\mathbb{F}_3$ .
4. Suppose that  $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  and  $q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$  are monic polynomials over  $\mathbb{Q}$ , and that at least one of the  $a_i$  or  $b_i$  is not an integer. Prove that at least one coefficient of  $p(x)q(x)$  is not an integer. (Hint: suppose that  $p$  is a prime which divides the denominator of some  $a_i$ . Now note that there must exist  $k$  and  $r$  such that  $p^r$  divides the denominator of  $a_k$ ,  $p^r$  divides the denominator of no  $a_i$  for  $i > k$ , and  $p^{r+1}$  divides the denominator of no  $a_i$  for  $i < k$ . Similarly there must exist  $l$  and  $s$  (possibly  $s = 0$ ) such that  $p^s$  divides the denominator of  $b_l$ ,  $p^s$  divides the denominator of no  $b_i$  for  $i > l$ , and  $p^{s+1}$  divides the denominator of no  $b_i$  for  $i < l$ . Consider the coefficient of  $x^{k+l}$  in  $p(x)q(x)$ . Conclude that no prime can divide the denominator of any  $a_i$ .)

**Remark:** The contrapositive of this is usually called **Gauss's Lemma**: if  $f(x)$  is a monic polynomial with integer coefficients, and if  $f(x)$  factors into two monic factors over  $\mathbb{Q}$ , then the factors actually have integer coefficients.

5. Suppose that  $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$  and  $q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$  are monic polynomials with integer coefficients and that at least one of the  $a_i$  or  $b_i$  is not divisible by  $p$ . Prove that at least one coefficient (besides the coefficient of  $x^{m+n}$ ) of  $p(x)q(x)$  is not divisible by  $p$ . Use this fact, plus Gauss's Lemma, to prove **Eisenstein's irreducibility criterion**: if  $f(x)$  is a monic polynomial with integer coefficients all of which (except the leading one) are divisible by  $p$ , and if  $p^2$  does not divide  $f(0)$ , then  $f(x)$  is irreducible. For example, we automatically can conclude that  $x^n + px + p$  is irreducible for any  $n > 1$  and any prime  $p$ .