

## Algebra II (2008)

### Exercise 6/week 47

1. Show that  $g(x) := x^5 + x^2 + 1$  is irreducible over  $\mathbb{F}_2$ . Is it primitive? Let  $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$  where  $\alpha^5 = \alpha^2 + 1$ . Find the minimal polynomial of  $\alpha^3$  over  $\mathbb{F}_2$ .
2. Prove: if  $p$  is a prime and  $n$  a positive integer, then  $n$  divides  $\phi(p^n - 1)$  where  $\phi$  is the Euler function.
3. Let  $\mathbb{F}_q$  be a finite field and assume that  $H \cup \{0\}$  is a subfield of  $\mathbb{F}_q$  for every subgroup  $H$  of  $\mathbb{F}_q^*$ . Show that either  $q = 2$  or  $q = 2^r$  for some prime  $r$  for which  $2^r - 1$  is a prime as well.
4. Let  $q$  be a prime power and let  $n$  be a positive integer with  $\gcd(n, q) = 1$ . Let  $m$  be the least positive integer such that  $q^m \equiv 1 \pmod{n}$ . Show that  $\mathbb{F}_{q^m}$  is the splitting field of  $x^n - 1$  over  $\mathbb{F}_q$ .
5. Let  $\zeta_n$  be an element of order  $n$  in the splitting field of  $x^n - 1$  over  $\mathbb{F}_q$ . Then, the polynomial

$$Q_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^n (x - \zeta_n^s)$$

is called the  $n$ th cyclotomic polynomial over  $\mathbb{F}_q$ . Prove:

- (a)  $x^n - 1 = \prod_{d|n} Q_d(x)$ .
  - (b)  $Q_n(x)$  factors into  $\phi(n)/m$  distinct monic irreducible polynomials in  $\mathbb{F}_q[x]$  of the same degree  $m$ , where  $m$  is the least positive integer such that  $q^m \equiv 1 \pmod{n}$ .
6. (a) Let  $r$  be a prime and  $k$  a positive integer. Show that

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}}.$$

- (b) Show that  $1 + x + x^2 + \cdots + x^{100}$  is irreducible over  $\mathbb{F}_2$ .