Tutorial sheet 4 - solutions - 1 -

1. We already know: $E^{(n)}$ is an abelian group with n elements. Let $n := \prod_{i=1}^{k} p_i^{e_i}$ be its prime factor decomposition. We want to find an element of order n.

For each i, the polynomial $x^{n/p_i} - 1$ has at most $n/p_i < n$ roots and thus there is an $a_i \in E^{(n)}$ which is not a root. Set $b_i := a_i^{(n/p_i^{e_i})} = a_i^{\left(\frac{n}{p_i^{e_i}}\right)}$. Now $b_i^{(p_i^{e_i})} = 1$ so the order of b_i is a power of p_i but since $b_i^{p_i^{e_i-1}} = a_i^{n/p_i} \neq 1$ the order is exactly $p_i^{e_i}$. Let $b := b_1 \cdot \ldots \cdot b_k$. <u>Claim</u>: b has order n.

Assume, on the contrary, that the order of b is a proper divisor of n. Then it is a divisor of one of the n/p_i, wlog, say n/p_1. Then

$$1 = b^{n/p_1} = b_1^{n/p_1} \cdot \ldots \cdot b_k^{n/p_k}.$$

For $2 \le i \le k$, $p_i^{e_i}$ divides n/p_1 and so $b_i^{n/p_1} = 1$, and so $b_1^{n/p_1} = b^{n/p_1} = 1$.

This is a contradiction. Thus $E^{(n)}$ is a cyclic group of order n.

2. (i) We use $Q_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$

for $n = 8$, divisors of 8 are: $1, 2, 4, 8$ $\Rightarrow$ $\underline{Q_8(x)} = \dfrac{x^8-1}{x^4-1} = \underline{x^4+1}$

μ takes values on n/d: $0, 0, -1, 1$

(ii) For $n = 20$, divisors d of 20 are: $1, 2, 4, 5, 10, 20$

μ takes values on n/d: $0, 1, -1, 0, -1, 1$

$$\Rightarrow \underline{Q_{20}(x)} = \frac{x^{20}-1}{x^{10}-1} \cdot \frac{x^2-1}{x^4-1} = (x^{10}+1)/(x^2+1) = \underline{x^8 - x^6 + x^4 - x^2 + 1}.$$

3. $x^3 + x + 1$ is an irreducible polynomial over $\mathbb{F}_2$ (no roots, degree ≤ 3).

$\Rightarrow \mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3+x+1)$ let $\theta := x + (x^3+x+1)$ be a root.

$\Rightarrow \mathbb{F}_8 = \{0, 1, \theta, \theta+1, \theta^2, \theta^2+1, \theta^2+\theta, \theta^2+\theta+1\}$

$\mathbb{F}_8$ is also the 7th cyclotomic field of $\mathbb{F}_2$, so every element $\neq 0, 1$ has order 7.

i	0	1	2	3	4	5	6
θ^i	1	θ	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1

4. We use:

$$I(q, n; x) = \prod_d Q_d(x)$$

where d runs through the pos. divisors of $q^n - 1$ with $n = \mathrm{ord}_d(q)$.

(i)

For $q=3$, $n=2$, ~~we~~ we have the divisors $1,2,4,8$ of $3^2-1=8$.

We have: $\mathrm{ord}_1(3)=1$, $\mathrm{ord}_2(3)=1$, $\mathrm{ord}_4(3)=2=n$, $\mathrm{ord}_8(3)=2=n$.

$$\Rightarrow I(3,2;x) = Q_4(x)\cdot Q_8(x) = (x^2+1)(x^4+1)$$

(ii) We know that x^4+1 is a product of two irreducible polynomials of degree 2 in $\mathbb{F}_3[x]$. We could guess, but we can also do:

$$x^4+1 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x + bd.$$

$\Rightarrow bd=1$, $a+c=0$, $b+d+ac=0$, $ad+bc=0$ for some $a,b,c,d \in \mathbb{F}_3$.

$\Rightarrow b=d$, $-a=c$

$\Rightarrow 2b-a^2=0$

Choose $a=1$, $\Rightarrow b=2=d=c$ $\Rightarrow x^4+1=(x^2+x+2)(x^2+2x+2)$

Both factors are irreducible.

Thus all irreducible monic polynomials of degree 2 over $\mathbb{F}_3$ are:

$$x^2+1,\ x^2+x+2,\ x^2+2x+2$$