Homework 2

Friday, January 19, 2018 9:40 PM

1. Prove that the following polynomials are irreducible:

(a) $x^{p-1}+x^{p-2}+\cdots+1$ in $\mathbb{Q}[x]$ where p is a prime number.

(b) $x^{p-1}+y^2x^{p-2}+y^2x^{p-3}+\cdots+y^2$ in $\mathbb{Q}[x,y]$

where p is a prime number.

(c) $1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}$ in $\mathbb{Q}[x]$ (you are allowed to use famous theorems about prime numbers.)

(d) x^n-y in $F[x,y]$.

(e) x^2+y^2-2 in $F[x,y]$ where $\mathrm{char}(F)\neq 2$.

(f) x^4+12x^3-9x+6 in $\mathbb{Q}[i][x]$.

2. Prove that $x^{p^n}-x+a$ does not have a zero in $\mathbb{Q}$ if p is prime, $a\in\mathbb{Z}$, and $p\nmid a$.

3. (a) Prove that in $(\mathbb{Z}/p\mathbb{Z})[x]$ we have

$$x(x-1)\cdots(x-(p-1))=x^p-x,$$ where p is prime.

(b) Deduce that $(p-1)!\equiv -1 \pmod p$.

Homework 2

Friday, January 19, 2018 11:24 PM

4. (a) Let G be a finite group. Suppose for any $n \in \mathbb{Z}^+$, $|\{g \in G \mid g^n = e\}| \leq n$. Prove that G is cyclic.

(b) Let F be a finite field. Prove that $F^\times$ is cyclic.

(Hint for (a). Let $\psi(d) := |\{g \in G \mid o(g) = d\}|$.

Step 1. Show, if $o(g) = d$, then $h^d = e \Leftrightarrow h = g^i$ for some $0 \leq i \leq d-1$.

Step 2. Show, if $\psi(d) \neq 0$, then $\psi(d) = \phi(d)$ where ϕ is the Euler ϕ-function.

Step 3. $G = \bigsqcup_{d \mid |G|} \{g \in G \mid o(g) = d\}$ implies $\sum_{d \mid |G|} \psi(d) = |G|$.

Step 4. Use steps 2, 3, and the fact that $\sum_{d \mid m} \phi(d) = m$, to deduce $\forall d \mid |G|$ we have $\psi(d) = \phi(d)$. In part. $\psi(|G|) \neq 0$.)

5. Let D be a finite division ring. In this problem you will prove D is a field.

(a) For any $a \in D$, let $C_D(a) := \{d \in D \mid ad = da\}$. Prove that $C_D(a)$ is a division ring.

(b) Convince yourself that $Z(D)$ is a field. Suppose $|Z(D)| = q$. Deduce $C_D(a)$ is a power of q.

(b) Use class formula for $D^\times$ to convince yourself.

$$|Z(D)^\times| + \sum_{\substack{a \in \text{Conjug.} \\ \text{class} \\ \text{rep/n.}}} [D^\times : C_D(a)^\times] = |D^\times| \qquad (*)$$

Use the following fact without proof:

$$\Phi_n(x) := \prod_{\substack{(i,n)=1 \\ 1 \le i \le n}} (x - \zeta_n^i) \in \mathbb{Z}[x] \text{ and}$$

for $m \mid n$, $m < n$, $x^n - 1 = (x^m - 1)\, h(x)\, \Phi_n(x)$ for some $h(x) \in \mathbb{Z}[x]$, and $(*)$ to deduce

$\Phi(q) \mid q-1$; and show it is a contradi.