\ov{}=\overline{}

Problem 1 [18 pts.]

(a)

[1 pt.] Correct answer: True

[1 pt.] Justification - Homework 8 Problem 4 applies since F\_{p^n} is perfect

(b)

[1 pt.] Correct answer: False

Justification - let k=F\_{p^n} and L be a finite extension of k

[1 pt.] L is finite over k hence finite over F\_p

[1 pt.] By Homework 8 Problem 1(e), L is Galois over F\_p iff [L:F\_p]=|Aut\_{F\_p}(L)|

[1 pt.] L is Galois over k since we can "descend from the top"

By Homework 8 Problem 1(e), k is Galois over F\_p iff [k:F\_p]=|Aut\_{F\_p}(k)|

[L:F\_p]=[L:k][k:F\_p]

|Aut\_{F\_p}(L)|=|Aut\_k(L)||Aut\_{F\_p}(k)|

(c)

[1 pt.] Correct answer: False

Justification - let a \in R be irreducible

[2 pts.] a generates a maximal ideal (a)

[1 pt.] The quotient R/(a) is a field

(d)

[1 pt.] Correct answer: True

[1 pt.] Justification - F\_{p^5} is a finite field hence perfect

(e)

[1 pt.] Correct answer: False

[1 pt.] Justification - a polynomial is separable iff it has no repeated roots in any field over which it splits completely

(f)

[1 pt.] Correct answer: True

Justification - let L be a finite extension of a finite field k

[1 pt.] Let \alpha be a generator of the cyclic unit group L^{\times}

[2 pts.] L=k(\alpha)

Problem 2 [7 pts.]

Let R be a PID, f(x) \in R[x] monic, q \in R irreducible

Assume f(x) = x^d (mod q) and f(0) \neq 0 (mod q^2)

For convenience let k = R/(q)

Given a(x) \in R[x], let \ov{a}(x) be its image in k[x]

[1 pt.] Show that k[x] is a UFD - k is a field and so k[x] is a PID

[1 pt.] \ov{f}(x)=x^d

Pick a monic irreducible factor g(x) of f(x) in R[x]

[2 pts.] \ov{g}(x)=x^r for some r \leq d since k[x] is a UFD

[1 pt.] q|g(0)

[1 pt.] Pick another monic irreducible factor h(x) of f(x) in R[x] and deduce q|h(0)

[1 pt.] Conclude that q^2|f(0), a contradiction

Problem 3 [5 pts.]

Note that (F\_p[y])[x]=(F\_p[x])[y]=F\_p[x,y], the polynomial ring over F\_p in the variables x,y

Show that f'(x)=0

[2 pts.] f'(x)=px^{p-1}=0 since the characteristic is p

Show that f(x) is irreducible

y is irreducible in F\_p[y]

[1 pt.] Statement

[1 pt.] Justification

[1 pt.] f(x)=x^p-y is Eisenstein at y hence irreducible by Problem 2

Problem 4 [8 pts.]

Suppose (a) does not hold

\Phi(\zeta\_n^{ip})=0

[1 pt.] Statement

[1 pt.] Justification - Homework 8 Problem 8

g(\zeta\_n^{ip})=0

[1 pt.] Statement

[1 pt.] \Phi(\zeta\_n^{ip})=f(\zeta\_n^{ip})g(\zeta\_n^{ip})

[1 pt.] f(\zeta\_n^{ip}) \neq 0 by assumption

[1 pt.] \zeta\_n^i is a zero of g(x^p)

[1 pt.] f(\zeta\_n^i)=0 by hypothesis

[1 pt.] Explain why g(x^p) and f(x) must share a common factor

Problem 5 [8 pts.]

Let q(x) be a common (monic) factor of f(x) and g(x^p) in Q[x]

Show that q(x) is in Z[x]

[1 pt.] Statement

[1 pt.] Justification - Gauss's Lemma plus the fact that q(x) is monic

[1 pt.] \ov{q}(x) is a common factor of \ov{f}(x) and \ov{g}(x^p)

Show that \ov{g}(x^p)=\ov{g}(x)^p

[1 pt.] Statement

[2 pts.] Justification - Frobenius is a ring homomorphism on F\_p[x] and fixes F\_p

Show that \ov{f}(x) and \ov{g}(x) have a common factor in F\_p[x]

[1 pt.] Take an irreducible hence prime factor of \ov{q}(x)

[1 pt.] Conclude that such a factor divides \ov{g}(x) since it divides \ov{g}(x)^p

Problem 6 [8 pts.]

[1 pt.] Let p be prime not dividing n and i such that f(\zeta\_n^i)=0

[1 pt.] Assume gcd(g(x^p),f(x)) \neq 1

Show that gcd(\ov{g}(x),\ov{f}(x)) \neq 1

[1 pt.] Statement

[1 pt.] Justification - Problem 5

[1 pt.] Obtain a contradiction by appealing to Homework 8 Problem 7

Show that f(\zeta\_n^{ip})=0

[1 pt.] Statement

[1 pt.] Justification - Problem 4(a)

[1 pt.] Appeal to Homework 8 Problem 8 to conclude that \Phi\_n(x)=f(x)

Problem 7 [10 pts.]

Identify Aut\_Q(Q(\zeta\_n)) with {\zeta\_n^i : i \in (Z/nZ)^{\times}}

Conclude that Q(\zeta\_n)/Q is Galois

Construct a suitable function from (Z/nZ)^{\times} to Aut\_Q(Q(\zeta\_n))

Show that this is an isomorphism

Problem 8 [10 pts.]

Let \alpha\in C denote the positive real 4th root of 2

Let L:=Q(\alpha,i)

Show that L/Q is Galois

Argue that L is the splitting field of the irreducible polynomial x^4-2 over Q

Work specifically with embedding results from class

Show that Gal(L/Q) is isomorphic to D\_8

Identify the eight Galois automorphisms of L over Q

Show that Gal(L/Q) is not abelian

Show that Gal(L/Q) does not satisfy the relations to be Q\_8

Problem 9 [17 pts.]

Let n \geq 3, p a prime not dividing n, and d the order of p mod n

(a)

Show that zeros of \ov{\Phi}\_n(x) are primitive nth roots of unity (which live in some extension of F\_p)

[1 pt.] Statement

[1 pt.] Justification - the factorization in Z[x] of x^n-1 into cyclotomic polynomials can be reduced mod p

Check for zeros

[1 pt.] F\_{p^m}^{\times} is cyclic of order p^m-1

[1 pt.] F\_{p^m}^{\times} admits element of order n iff n|(p^m-1)

[1 pt.] iff p^m = 1 mod n

[1 pt.] Conclusion

(b)

Show that group of nth roots of unity in F\_{p^d} is cyclic

[1 pt.] Statement

[1 pt.] Justification - subgroups of cyclic groups are cyclic

[1 pt.] Conclude that every generator of this group is a power of any other generator of this group

(c)

Let f(x) \in F\_p[x] be an irreducible factor of \ov{\Phi}\_n(x)

Show that minimal extension of F\_p in which f(x) admits a root has degree equal to deg(f(x))

[1 pt.] Statement

[1 pt.] Justification - f(x) is irreducible

Show that d=deg(f(x))

[1 pt.] Zeros of f(x) are zeros of \ov{\Phi}\_n(x)

[1 pt.] Appeal to part (a)

(d)

\ov{\Phi}\_n(x) is irreducible iff d = deg(\ov{\Phi}\_n(x)) = |(Z/nZ)^{\times}|

[1 pt.] Statement

[1 pt.] Justification - part (c)

d = |(Z/nZ)^{\times}| iff p generates (Z/nZ)^{\times}

[1 pt.] Statement

[1 pt.] Justification - d = order of p mod n

Problem 10 [10 pts.]

For convenience, denote the image of \Phi\_8(x) in F\_p[x] by f\_p(x) (p in Z a positive prime)

Show that (Z/8Z)^{\times} is not cyclic

[1 pt.] Statement

[1 pt.] Justification - (Z/8Z)^{\times} \iso Z/2Z \times Z/2Z

Show that f\_p(x) is reducible for p odd

[1 pt.] Appeal to Problem 9(d)

[1 pt.] p does not divide 8 iff p \neq 2 iff p is odd

Show that \Phi\_8(x)=x^4+1

[1 pt.] Statement

Justification

[1 pt.] \Phi\_8(x) divides x^8-1=(x^4-1)(x^4+1) in Z[x]

[1 pt.] \Phi\_8(x) is irreducible monic in Z[x] of degree 4 with roots of order 8

[1 pt.] Roots of x^4-1 have order at most 4

Show that f\_2(x) is reducible

[2 pts.] f\_2(x)=x^4+1=(x^2+1)^2=(x+1)^4 since the characteristic is 2