Problem 1 [15 pts.]

(a)

[1 pt.] Correct answer: False

[2 pts.] Justification

k^{\times} is cyclic of order 13^2-1=168

5 does not divide 168

Note: [1 pt.] if interpreted in terms of additive order instead

(b)

[1 pt.] Correct answer: True

[1 pt.] Justification

(c)

[1 pt.] Correct answer: False

[1 pt.] Justification

Note that the polynomials being monic rules out nontrivial unit multiples

(d)

[1 pt.] Correct answer: False

[1 pt.] Justification (for the future, please provide a counterexample!)

(e)

[1 pt.] Correct answer: False

[2 pts.] Justification

Explain why 2020 must divide [L:Q] for this to be true

2020 does not divide 1010

(f)

[1 pt.] Correct answer: True

[2 pts.] Justification

Minimal polynomial is defined over Q and so RCF will be in M\_n(Q)

Minimal polynomial splits completely and has no repeated roots

Problem 2 [10 pts.]

Take L to be k[x]/(f(x))

[1 pt.] Statement

[1 pt.] Briefly justify why L is a field -- f(x) is irreducible

[1 pt.] Take \alpha to be the coset of x in L

Show that \alpha is algebraic

[1 pt.] Statement

[2 pts.] Explain why f(\alpha)=0 in L

Show that f(x)=f\_{\alpha}(x) (half of this is already done)

[1 pt.] Choose g(x)\in k[x] such that g(\alpha)=0 in L

[2 pts.] Explain why g(x) is divisible by f(x)

[1 pt.] Conclude the result

Problem 3 [9 pts.]

Perform division algorithm on f(x),g(x) in k[x]

[1 pt.] Write f(x)=q(x)g(x)+r(x)

[1 pt.] Specify that q(x),r(x) are elements of k[x]

[1 pt.] Specify that deg(r)<deg(g)

Show that r(x)=0

[1 pt.] Write r(x)=g(x)(q(x)-h(x))

[1 pt.] g(x)|r(x) in L[x] (must specify L and not k to get pts.)

[1 pt.] Conclude the result (using bound on degree)

Show that h(x)\in k[x]

[1 pt.] Write h(x)g(x)=q(x)g(x) in L[x]

[1 pt.] Use fact that L[x] is integral domain (and g(x) is nonzero) to conclude h(x)=q(x) in L[x]

[1 pt.] Use fact that q(x)\in k[x] to conclude the result

Note: The solution outlined above is only one of many possible approaches

Another common and viable approach is to induct on degree

Problem 4 [7 pts.]

Let f(x) in Q[x] be one of:

(a) x^3-20x+15

(b) x^3+3x^2+3x-1

(c) x^2-x-1

(d) x^6+...+1

(a)

[1 pt.] State that f(x) is Eisenstein at 5

(b)

[2 pts.] Show that a shift of f(x) is Eisenstein at 2

[1 pt.] Conclude that f(x) is irreducible

(c)

[2 pts.] Use one of the following approaches

Rational Root Thm

Quadratic formula

Eisenstein's criterion applied to a shift for the prime 5

x=y-2 gives y^2-5y+5

x=y+3 gives y^2+5y+5

(d)

[1 pt.] Appeal to Lecture 23 Proposition 1

Problem 5 [12 pts.]

Note: all of this assumes \alpha\neq0 (you don't need to worry about the case \alpha=0)

(a)-->(b)

Show that powers of \alpha are linearly dependent

[1 pt.] Write \alpha as the root of a polynomial

[1 pt.] Briefly explain why this gives a (nontrivial) linear dependence relation

[1 pt.] Conclude that k[\alpha] has finite dimension over k

(b)-->(c)

[1 pt.] Explain why it suffices to show \alpha is invertible in k[\alpha]

[1 pt.] Write down linear dependence relation for powers of \alpha

[4 pts.] Solve for \alpha^{-1} as a polynomial in \alpha

(c)-->(a)

[1 pt.] Write \alpha^{-1} as a polynomial in \alpha

[2 pts.] Write \alpha as a root of a (nonzero) polynomial in k[x]

Alternative approach for (b)-->(c)

Show that k(\alpha) contains k[\alpha]

[1 pt.] Statement

[1 pt.] Justification

Show that the minimal polynomial f\_{\alpha}(x) generates a maximal ideal

[1 pt.] Statement

[1 pt.] Justification

[1 pt.] Show that k[\alpha] is a field

k[\alpha] \iso k[x]/(f\_{\alpha}(x))

[1 pt.] Explain why k[\alpha] contains k(\alpha) and so the two are equal

Note: Some of this stuff appears as part of Lecture 20 Proposition 1 but is not really proven there

Problem 6 [10 pts.]

Let \alpha:=\sqrt{2}+\sqrt{3}

Show that \alpha is a root of x^4-10x^2+1

[1 pt.] Statement

[1 pt.] Justification -- computation

Show that Q(\alpha) is contained in Q(\sqrt{2},\sqrt{3})

[1 pt.] Statement

[2 pts.] Justification

\alpha is Q-rational function of \sqrt{2},\sqrt{3}

Q(\alpha) is minimal field extension of Q containing \alpha

Show that Q(\alpha) contains Q(\sqrt{2},\sqrt{3})

[1 pt.] Show that Q(\alpha) contains \sqrt{6}

[1 pt.] Show that Q(\alpha) contains \sqrt{2} iff it contains \sqrt{3}

[2 pts.] Show that Q(\alpha) contains one of \sqrt{2},\sqrt{3}

[1 pt.] Appeal to fact that Q(\sqrt{2},\sqrt{3}) is minimal field extension of Q containing \sqrt{2},\sqrt{3}

Note: The solution outlined above is only one of many possible approaches

Problem 7 [12 pts.]

(a)

Construct suitable map from \Emb\_k(L,M) to {\beta\in M : f\_{\alpha}(\beta)=0}

[1 pt.] Send \sigma to \sigma(\alpha)

[2 pts.] Show that \sigma(\alpha) is a root of f\_{\alpha}(x)

Construct suitable inverse map from {\beta\in M : f\_{\alpha}(\beta)=0} to \Emb\_k(L,M)

[1 pt.] Send \beta to the map \sigma: L\to M that sends \alpha to \beta

[3 pts.] Explain why \alpha\mapsto\beta uniquely extends to an element of \Emb\_k(L,M)

[2 pts.] Check that both maps are indeed inverses -- check that both compositions give identity

(b)

[1 pt.] State that \Aut\_k(L)=\Emb\_k(L,L) (this is Lecture 25 Observation 1)

[1 pt.] Bound #{\beta\in L : f\_{\alpha}(\beta)=0} above by deg(f\_{\alpha})

[1 pt.] State that deg(f\_{\alpha})=[L:k]

Note: The solution given for (a) is one of many possible approaches

Problem 8 [25 pts.]

Let \phi: R\to R be the map a\mapsto a^p

(a)

[1 pt.] \phi(1)=1^p=1

[1 pt.] \phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b) by commutativity

Show that \phi(a+b)=\phi(a)+\phi(b)

[1 pt.] Statement

[1 pt.] Expand (x+y)^p using Binomial Formula

[1 pt.] Identify edge terms as x^p and y^p

[1 pt.] Identify ith middle term as \binom{p}{i}a^{p-i}b^i

Show that \binom{p}{i} is divisible by p for 0<i<p

[1 pt.] Statement

[1 pt.] Justification

[1 pt.] Conclude the result -- middle terms vanish in R because of the characteristic

(b)

[1 pt.] Reduce k-linearity of \phi to checking \phi fixes F\_p pointwise

[4 pts.] Show that \phi fixes F\_p pointwise

F\_p^{\times} has order p-1

a^{p-1}=1 for every a\in F\_p^{\times} by Lagrange's Thm

0^p=0

a^p=a for every a\in F\_p

[1 pt.] Use (a) to conclude that \phi is an F\_p-embedding of k into k hence an F\_p-automorphism

(c)

Reduce to showing that \phi has order d

[1 pt.] Appeal to Problem 7(b) to get |\Aut\_{F\_p}(k)|\leq[k:F\_p]=d

[2 pts.] Explain why \Aut\_{F\_p}(k) is cyclic if \phi has order d

Show that \phi has order \leq d

[1 pt.] k^{\times} has order p^d-1

[1 pt.] a^{p^d}=a for every a\in k

[2 pts.] Explain why \phi^d=\id

[1 pt.] Conclude that \phi has order \leq d

[2 pts.] Show that \phi has order d -- k^{\times} is cyclic of order p^d-1

Problem 9 [25 pts.]

(a)

Let f(x)=a\_nx^n+...+a\_0 and d=gcd(a\_0,...,a\_n)

[3 pts.] Show that f(x) mod p is zero iff p|d

f(x) mod p is zero

iff p|f(x) in Z[x]

iff p|a\_i for every i

iff p|d (by definition of gcd)

[2 pts.] f(x) mod p is nonzero iff d has no prime divisors iff d=1

(b)

Let f(x),g(x)\in Z[x] be primitive and p prime

Show that f(x)g(x) mod p is nonzero

[1 pt.] Statement

[1 pt.] f(x) mod p and g(x) mod p are nonzero by (a)

[1 pt.] F\_p[x] is an integral domain

[1 pt.] Conclude that f(x)g(x) is primitive using (a)

(c)

Let f(x)=(a\_n/b\_n)x^n+...+(a\_0/b\_0)

[1 pt.] Take L:=lcm(b\_0,...,b\_n)

[1 pt.] Take G:=gcd(La\_0/b\_0,...,La\_n/b\_n)

[2 pts.] Show that (L/G)f(x) is a primitive element of Z[x]

[1 pt.] State that L/G is a positive rational number

(d)

[1 pt.] Choose r\_1,r\_2 positive rational such that r\_1h(x),r\_2g(x) are primitive elements of Z[x] (using (c))

[5 pts.] Show that r\_1r\_2=1

r\_1r\_2f(x)=r\_1h(x)r\_2g(x)\in Z[x] is primitive by (b)

f(x)\in Z[x] is monic by assumption

r\_1r\_2=1 since anything else violates primitivity

[3 pts.] Show that r\_1\in Z (or equivalently r\_2\in Z by symmetry)

h(x) is monic

r\_1h(x) is in Z[x]

Leading term of r\_1h(x) is r\_1

[2 pts.] Show that h(x),g(x)\in Z[x]

r\_1=1=r\_2 since r\_1,r\_2\in Z positive with r\_1r\_2=1

r\_1h(x),r\_2g(x)\in Z[x] by assumption

Problem 10 [23 pts.]

(a) [10 pts.]

(b)

Show that \Phi\_p(x)=x^{p-1}+...+1

[1 pt.] By (a) we have x^p-1=\Phi\_1(x)\Phi\_p(x)

[1 pt.] \Phi\_1(x)=x-1

[1 pt.] \Phi\_p(x)=(x^p-1)/(x-1)=x^{p-1}+...+1

Show that \Phi\_p(x) is the minimal polynomial of \zeta\_p over Q

[1 pt.] \Phi\_p(x) is irreducible since a shift by 1 is Eisenstein at p

[1 pt.] \Phi\_p(x) is monic and kills \zeta\_p

(c)

[1 pt.] Check base case (n=1)

[1 pt.] State inductive hypothesis - assume \Phi\_m(x)\in Z[x] for all m<n

[1 pt.] Separate off factors - let \Psi\_n(x) be the product of \Phi\_d(x) over d|n proper

[1 pt.] Use (a) to write x^n-1=\Phi\_n(x)\Psi\_n(x)

[1 pt.] Use inductive hypothesis to get \Psi\_n(x)\in Z[x] (hence also in Q[x])

[1 pt.] State that \Psi\_n(x) is monic

[1 pt.] Use Problem 3 to get \Phi\_n(x)\in Q[x]

[1 pt.] Use Gauss's Lemma (Problem 9(d)) to get \Phi\_n(x)\in Q[x]