$\frac{48}{50}$

Modern Algebra 2
HW 6

1) Assume for contradiction that $f(x)$ is reducible in $\mathbb{Z}[x]$.

$\exists\ g(x) = b_s x^s + \dots + b_0$ s.t. $b_i, c_j \in \mathbb{Z}$. and $f(x) = g(x)h(x)$

$h(x) = c_t x^t + \dots + c_0$

Consider the functions mod p.

$\bar{f}(x) = \bar{g}(x)\bar{h}(x)$. However $f(x)$ is irreducible modulo $p \Rightarrow \bar{g}(x)$ or $\bar{h}(x)$ is trivial.

WLOG, say $\bar{g}(x)$ is trivial.

5

$\Rightarrow c_t, c_{t-1}, \dots, c_1$ are all multiples of p, $c_0 \equiv 1 \bmod p$

Now consider the leading term of $f(x)$

Because $f(x) = g(x)h(x)$, $a_n = b_s \cdot c_t$.

$p \mid c_t \Rightarrow p \mid b_s c_t \Rightarrow p \mid a_n$.

However contradiction $\Rightarrow f(x)$ is irreducible in $\mathbb{Z}[x]$

$\therefore f(x)$ is irreducible in $\mathbb{Q}[x]$ ∎

Counterexample if $p \mid a_n$: $4x^2 + 4x + 1 = (2x+1)^2$. Reducible in $\mathbb{Q}[x]$.

$4x^2 + 4x + 1 \equiv 1 \bmod 2$. 1 is irreducible modulo 2.

2) Assume for contradiction that $f(x)$ is reducible in $\mathbb{Z}[x]$.

$\exists\ g(x) = b_s x^s + \dots + b_0$ s.t. $b_i, c_j \in \mathbb{Z}$ and $f(x) = g(x)h(x)$

$h(x) = c_t x^t + \dots + c_0$

Consider $f(x)$ modulo p

$\bar{f}(x) = \bar{a}_n x^n$ where $\bar{a}_n \neq \bar{0}$

5

Because $\bar{g}(x)\bar{h}(x) = \bar{f}(x)$, $\bar{g}(x) \mid \bar{f}(x)$ and $\bar{h}(x) \mid \bar{f}(x)$.

$a_n = b_s c_t \Rightarrow \bar{a}_n = \bar{b}_s \bar{c}_t$.

Thus $\bar{g}(x)$ and $\bar{h}(x)$ each have only 1 element ($\bar{b}_s x^s$ and $\bar{c}_t x^t$ respectively).

Thus $b_{s-1}, b_{s-2}, \dots, b_0$ are multiples of P.

Similarly $c_{t-1}, c_{t-2}, \dots, c_0$ are multiples of P.

$a_0 = b_0 c_0$.

$p \mid b_0$ and $p \mid c_0 \Rightarrow p^2 \mid b_0 c_0$.

Contradiction

$f(x)$ irreducible in $\mathbb{Z}[x]$

$\therefore f(x)$ irreducible in $\mathbb{Q}[x]$ ∎

3) $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. If n is prime, then $\frac{n!}{k!(n-k)!}$ is divisible by n unless $k=0$ or $k=n$.
Thus $\binom{p}{k}$ is a multiple of p when $k \neq 0$ and $k \neq p$ for any prime p.
$\binom{p}{0} = \binom{p}{p} = 1$

$(x^p - 1) = (x-1)(x^{p-1} + x^{p-2} + \dots + 1)$
$((x+1)^p - 1) = (x)((x+1)^{p-1} + (x+1)^{p-2} + \dots + 1)$
$((x+1)^p - 1) = (\binom{p}{p}x^p + \binom{p}{p-1}x^{p-1} + \dots + \binom{p}{p} * 1) - 1$
$= \binom{p}{p}x^p + \binom{p}{p-1}x^{p-1} + \dots + \binom{p}{1}x$
$= x[\binom{p}{p}x^{p-1} + \binom{p}{p-1}x^{p-2} + \dots + \binom{p}{1}]$
$\Rightarrow (x+1)^{p-1} + (x+1)^{p-2} + \dots + 1 = \binom{p}{p}x^{p-1} + \binom{p}{p-1}x^{p-2} + \dots + \binom{p}{1}$.
$= x^{p-1} + \underbrace{\binom{p}{p-1}x^{p-2} + \dots + \binom{p}{2}x + p}_{\text{coefficients are multiples of } p}$

$p^2 \nmid p$ and $p \nmid 1$

By eisenstein's criterion, $(x+1)^{p-1} + (x+1)^{p-2} + \dots + 1$ is irreducible in $\mathbb{Z}[x]$
$\Rightarrow x^{p-1} + x^{p-2} + \dots + 1$ is irreducible in $\mathbb{Z}[x]$
$\therefore x^{p-1} + \dots + 1$ is irreducible in $\mathbb{Q}[x]$ ∎

5

4) $\mathbb{F}_p \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Because p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Let $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ be a ~~the~~ generator

$a = c^\alpha \quad 0 < \alpha \le p-1$
$b = c^\beta \quad 0 < \beta \le p-1$

Something wrong w/ having $\Leftrightarrow$ everywhere
You seem to be saying "a and b squares $\Leftrightarrow$ ab square" Not true

Case 1: Both a and b are squares.
a is a square $\Leftrightarrow \exists \alpha_0 \in \mathbb{Z}$ s.t. $2\alpha_0 = \alpha \Leftrightarrow a = (c^{\alpha_0})^2$
b is a square $\Leftrightarrow \exists \beta_0 \in \mathbb{Z}$ s.t. $2\beta_0 = \beta \Leftrightarrow b = (c^{\beta_0})^2$
$\Leftrightarrow ab = (c^{\alpha_0})^2(c^{\beta_0})^2 \Leftrightarrow ab = (c^{\alpha_0+\beta_0})^2 \Leftrightarrow$ ab is a square.

Case 2: a is a square, b is non-square
a is a square $\Leftrightarrow \exists \alpha_0 \in \mathbb{Z}$ s.t. $2\alpha_0 = \alpha \Leftrightarrow a = (c^{\alpha_0})^2$
b is non-square $\Leftrightarrow \beta$ is an odd number $\Leftrightarrow b = c^\beta$
$\Leftrightarrow ab = (c^{\alpha_0})^2 c^\beta \Leftrightarrow ab = c^{2\alpha_0} c^\beta$
$\Leftrightarrow ab = c^{2\alpha_0+\beta} \Leftrightarrow 2\alpha_0$ is even and β is odd $\Leftrightarrow 2\alpha_0 + \beta$ is odd $\Leftrightarrow$ ab is not a square

Case 3: Both a and b are non-squares
a non-square $\Leftrightarrow \alpha$ is odd integer
b non-square $\quad \beta$ is odd integer
$\Leftrightarrow ab = c^\alpha c^\beta = c^{\alpha+\beta} \Leftrightarrow \alpha+\beta$ is even $\Leftrightarrow 2 \mid \alpha+\beta$
$\Leftrightarrow$ ab is a square.

These cases have shown that
ab are a square in $\mathbb{F}_p$ iff a and b are either both square or both non-square ∎

4

If $p=2$ or $p=3$, $24 \equiv 0 \Rightarrow f(x) = (x-\sqrt{5})^2 \Rightarrow f(x)$ is reducible.

5) Case 1: 2 is square modulo P.

4 is square modulo P

$2 \cdot 4 = 8$. Problem (4) implies 8 is a square modulo P

$f(x) = (x^2-1)^2 - 8x^2$ is thus a difference of squares. ✓

$\therefore f(x)$ is reducible modulo P

Case 2: 3 is square modulo P.

4 is square modulo P

$3 \cdot 4 = 12$. Problem (4) implies 12 is a square modulo P ✓

$f(x) = (x^2+1)^2 - 12x^2$ is thus a difference of squares.

$\therefore f(x)$ is reducible modulo P.

Case 3: Both 2 and 3 are non-square modulo P

$2 \cdot 3 = 6$. Problem (4) implies 6 is a square modulo P

4 is a square modulo P ✓

$4 \cdot 6 = 24$. Problem (4) implies 24 is a square modulo P

$f(x) = (x^2+5)^2 - 24$ is thus a difference of squares

$\therefore f(x)$ is reducible modulo P.

In all cases, $f(x)$ is reducible modulo P ∎

5

6) The irreducible polynomial of $\sqrt[3]{2}\, e^{2\pi i/3}$ must be at least degree 3.

x^3-2 is the irreducible polynomial. This also is the irreducible polynomial of $\sqrt[3]{2}$.

Because $\sqrt[3]{2}\, e^{2\pi i/3}$ and $\sqrt[3]{2}$ are algebraic over $\mathbb{Q}[x]$,

$\phi: \mathbb{Q}[x]/x^3-2 \to \mathbb{Q}[\sqrt[3]{2}\, e^{2\pi i/3}]$ and $\psi: \mathbb{Q}[x]/x^3-2 \to \mathbb{Q}[\sqrt[3]{2}]$

are both isomorphisms. (x^3-2 is maximal $\Rightarrow$ it generates the kernel $\Rightarrow \mathbb{Q}[x]/x^3-2$ is iso to images of ϕ and ψ.)

Now one can create $\sigma = \psi\phi^{-1}$ that sends $\mathbb{Q}[\sqrt[3]{2}\, e^{2\pi i/3}] \to \mathbb{Q}[\sqrt[3]{2}]$. ✓

Because ϕ and ψ are isomorphisms, so is σ. Thus the two are isomorphic.

$\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$.

If a solution to $x_1^2 + \dots + x_n^2 = -1$ exists in $\mathbb{Q}[\sqrt[3]{2}\, e^{2\pi i/3}]$, then one exists in $\mathbb{Q}[\sqrt[3]{2}]$. This implies that a solution to $x_1^2 + \dots + x_k^2 = -1$ exists in $\mathbb{R}$.

However because $z^2 \geq 0 \;\forall z \in \mathbb{R}$, this cannot be true. ✓

$\therefore x_1^2 + \dots + x_k^2$ has no solution in $\mathbb{Q}[\sqrt[3]{2}\, e^{2\pi i/3}]$ ∎

5

5

7) Because $\alpha^2 \in F(\alpha)$, $F(\alpha^2) \subset F(\alpha)$.

This implies deg of $F(\alpha^2)$ | deg of $F(\alpha)$.

$\Rightarrow$ deg of $F(\alpha^2) | 5$. ✓

$\Rightarrow$ deg of $F(\alpha^2) = 1$ or $= 5$.

The degree cannot be 1 because in that case deg $F(\alpha)$ would be 2.

explain.

Thus deg of $F(\alpha^2)$ is 5.

Because $[F(\alpha) : F(\alpha^2)] = 1$, they are the same field.

$\therefore$ α and α^2 generate the same extension. ✓

4

8) A polynomial with ζ_7 as a solution is $x^7 - 1$.

However $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$

Because ζ_7 is not a solution to $(x-1)$, we can remove it.

From problem 3, $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible. (ζ_7 is still a solution)

ζ_7 thus has degree 6. ✓

$x^5 - 1$ is a polynomial with ζ_5 as a solution.

Similarly $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$

From problem 3, $x^4 + x^3 + x^2 + x + 1$ is irreducible. (ζ_5 is still a solution)

ζ_5 thus has degree 4. ✓

Because $4 \nmid 6$, $\zeta_5 \notin \mathbb{Q}[\zeta_7]$ ∎ explain.

9) $x^4 - a$ is a polynomial that has a as a solution.

$x^4 - a$ could factor into a linear and cubic polynomial.

Solutions to $x^4 - a$ are: $\sqrt[4]{a}$, $-\sqrt[4]{a}$, $-\sqrt[4]{a}\, i$, $\sqrt[4]{a}\, i$

None of these are elements of $\mathbb{Q}$ (If they were, their squares would be elements of $\mathbb{Q}$ and their squares are either $-\sqrt{a}$ or $\sqrt{a}$, which we know are not elements of $\mathbb{Q}$)

Thus $x^4 - a$ cannot factor into a linear and a cubic polynomial. ✓

$x^4 - a$ could factor into two quadratics,

$(x^2 + \alpha x + \beta)(x^2 + \gamma x^2 + \delta)$ where $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$

$= x^4 + (\alpha + \gamma)x^3 + (\beta + \delta + \alpha\gamma)x^2 + (\alpha\delta + \gamma\beta)x + \beta\delta$

$\alpha + \gamma = 0 \Rightarrow \alpha = -\gamma$

$\alpha\delta + \beta\gamma = 0 \Rightarrow \alpha\delta - \beta\alpha = 0 \Rightarrow \alpha\delta = \alpha\beta \Rightarrow \delta = \beta$

$\beta\delta = -a \Rightarrow \beta^2 = -a \Rightarrow \beta = \sqrt{-a}$

5

There is no β in $\mathbb{Q}$ that satisfies this.

Thus $x^4 - a$ cannot be divided into quadratics ✓

$x^4 - a$ is the irreducible for $\sqrt[4]{a}$ over $\mathbb{Q}$.

$\therefore \sqrt[4]{a}$ has degree 4 in $\mathbb{Q}$ ∎

10) L/K algebraic and K/F algebraic.

Let $\alpha \in L$. α is algebraic$/K$

$[K(\alpha):K]$ is finite.

$\exists f(x) = a_n x^n + \dots + a_0$ s.t. $f(\alpha) = 0$ $(a_i \in K)$

Each a_i is algebraic $/F$ ✓

$[F(a_i):F]$ is finite

5

In order to contain α, F must have every a_i

$F \subset F(a_0) \subset F(a_0, a_1) \subset \dots \subset F(a_0, \dots, a_n)$ ✓

$$[F(a_0, \dots, a_n):F] = \underbrace{[F(a_0,\dots,a_n):F(a_0,\dots,a_{n-1})][F(a_0,\dots,a_{n-1}):F(a_0,\dots,a_{n-2})] \dots [F(a_0):F]}_{\text{finite product of finite numbers}}$$

$[F(a_0,\dots,a_n):F]$ is thus finite

$F(a_0 \ \ a_n) \subset K$

$F(a_0,\dots,a_n) \subset F(\alpha) \subset K \subset K(\alpha)$

$[F(\alpha):F(a_0,\dots,a_n)][F(a_0,\dots,a_n):F] = [F(\alpha):F]$. LHS is finite $\Rightarrow$ RHS is finite.

Thus α is algebraic over F. ✓

Thus L/F is an algebraic field extension ∎