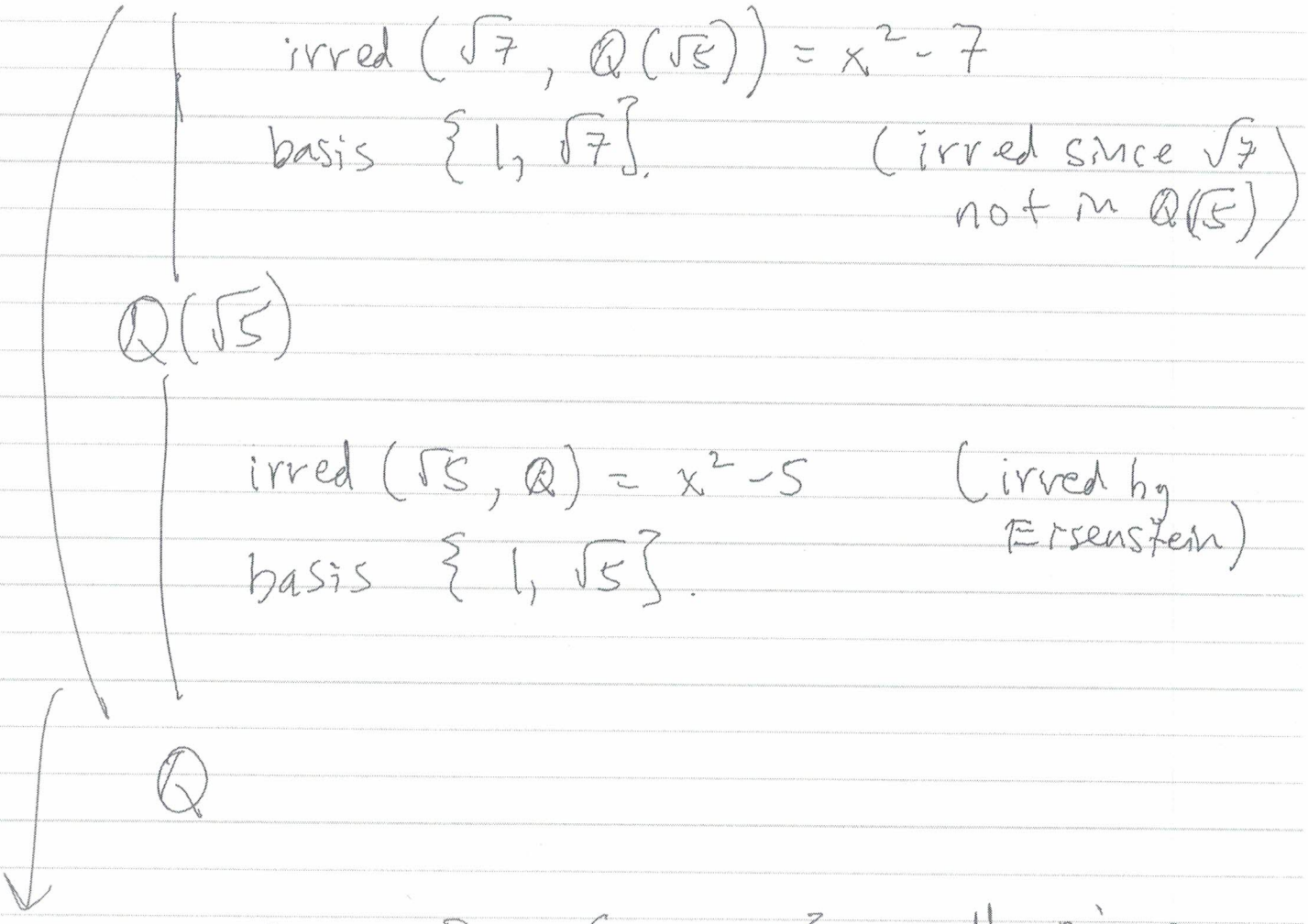
so at least one element in $\mathbb{Z}_p$ is missing from this list.)

H13 Sol

#11a) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$ Summary



basis $\{1, \sqrt{5}\} \cdot \{1, \sqrt{7}\}$ all pairwise products

$= \{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$.

#2b) $\text{irred}(\sqrt{5}-\sqrt{7}, \mathbb{Q})$

$= x^4 - 24x + 4$

(One way to find this:

Let $x = \sqrt{5} - \sqrt{7}$

$x^2 = 5 - 2\sqrt{35} + 7$

$x^2 = 12 - 2\sqrt{35}$

$(x^2 - 12)^2 = (-2\sqrt{35})^2$

$x^4 - 24x + 144 = 140$

$x^2 - 24x + 4 = 0.$)

We need to check it can't factor as i) linear • cubic or ii) quadratic • quadratic. For i), we can use our special case of the Rational Root Thm: the only

possible roots in $\mathbb{Q}$ are $\pm 1, 2, 4$.

None of these work, so $x^4 - 24x^2 + 4$ has no linear root.

For ii) suppose $x^4 - 24x^2 + 4$ factors as $(ax^2 + bx + c)(dx^2 + ex + f)$, with $a, b, c, d, e, f \in \mathbb{Z}$. ($\mathbb{Q}$ is also fine, but we have a result saying an integer poly in $\mathbb{Q}[x]$ factors with integer coefficients if it factors with rationals.)

WLOG, we can take $a = d = 1$

(If $a = d = -1$, just move the unit -1 from one factor to the other.)

So $x^4 - 24x + 4 = (x^2 + bx + c)(x^2 + ex + f)$.

$= x^4 + (b+e)x^3 + (be + c + f)x^2 + (bf + ce)x + cf$.

Thus, matching coefficients,

$b+e = 0$

$be+c+f = -24$

$bf+ce = 0$

$cf = 4$

Thus, $b = -e$, so

$bf+ce = bf - bc = b(f-c) = 0.$

Since we're in an integral domain, either

$b=e=0$ or $f-c=0$ (so $c=f$).

If $b=e=0$, we have $(x^2+c)(x^2+f)$.

By factoring x^4-24x^2+4 using the quadratic formula, you can see this forces c and f to be non-rational

If $c=f$, our condition $cf=4$ implies $c=f=\pm 2$, then $be+c+f = -24$

transforms into $-b^2 \pm 4 = -24$,

i.e. $b^2 = 24 \pm 4 = 20$ or 28.

Either way b is irrational.

Thus, our polynomial $x^4 - 24x^2 + 4$ is irreducible.

The obvious basis for $\mathbb{Q}(\sqrt{5} - \sqrt{7})$ over $\mathbb{Q}$ is

$$\{1, \sqrt{5} - \sqrt{7}, (\sqrt{5} - \sqrt{7})^2, (\sqrt{5} - \sqrt{7})^3\}$$

$$= \{1, \sqrt{5} - \sqrt{7}, 12 - 2\sqrt{35}, 2\sqrt{5} - 22\sqrt{7}\}.$$

#1c) Let $B_1 = \{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$,

$B_2 = \{1, \sqrt{5} - \sqrt{7}, 12 - 2\sqrt{35}, 2\sqrt{5} - 22\sqrt{7}\}$.

It is easy to write each element in B_2 as a $\mathbb{Q}$-linear combination of

basis elements in B, (in fact, they are already written this way) Let check the reverse.

$1 = 1$ ✓ easy

$$\sqrt{5} = \frac{22}{24}\left(\sqrt{5} - \sqrt{7}\right) + \frac{1}{24}\left(2\sqrt{5} - 22\sqrt{7}\right)$$

$$\sqrt{7} = \frac{-2}{-20}\left(\sqrt{5} - \sqrt{7}\right) + \frac{1}{-20}\left(2\sqrt{5} - 22\sqrt{7}\right)$$

$$\sqrt{35} = \frac{-12}{-2}(1) + \frac{1}{-2}\left(12 - 2\sqrt{35}\right).$$

#3) We need to completely factor $x^3 + 2x + 1$ in $\mathbb{Z}_3[x]$, assuming α is a root in an extension field.

First, let's do long division to factor out $x - \alpha$.

#2) Fraleigh Sec 31 #25

If we successively adjoin square roots, we get a tower of fields for which each step is a degree 2 extension.* Thus by our Chain Rule, $[E_n : \mathbb{Q}] = 2^n$.

$\deg 2^n$

E_n
| 2
⋮
E_2
| 2
E_1
| 2
$\mathbb{Q}$

* (since adjoining a square root means our irreducible polynomial is of the form $x^2 - k$ each time, where k is from the current base field).

Now $f(x) = x^{14} - 3x^2 + 12$ is irred. over $\mathbb{Q}$ by Eisenstein with $p = 3$. Thus, if α is a root of $f(x)$, $\deg(\alpha, \mathbb{Q}) = 14$.

Since 14 does not divide any 2^n, for $n \in \mathbb{Z}^+$ $\mathbb{Q}(\alpha)$ cannot be a subfield of any E_n as designed above, ie. α ~~is not the~~

cannot be expressed as a rational function of square roots of rational functions of square roots of ... etc. (If it could, we could build an E_n, adding one such square root at a time.)

#3) Fraleigh Sec 31, # 30. 1) α^2 is alg /F (by prev Thm) and also 2) $F(\alpha^2)$ is the

Since $\alpha^2 \in F(\alpha)$ and

smallest extension field of F which contains α^2, so we have the inclusion $F(\alpha^2) \leq F(\alpha)$, and thus the tower.

$F(\alpha)$
|
$F(\alpha^2)$
|
F

Using our chain rule,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F].$$

Since the LHS is odd, so is each factor on the right hand side.

So far, we know that α^2 is algebraic of odd degree over F.

It remains to show that $F(\alpha^2) = F(\alpha)$,

or equivalently $\left[F(\alpha) : F(\alpha^2)\right] = 1$

Consider $\deg(\alpha, F(\alpha^2))$, which is the same number as $\left[F(\alpha) : F(\alpha^2)\right]$, since throwing (adjoining) α into $F(\alpha^2)$ will yield $F(\alpha)$. Again, by the Chain Rule, this number is odd, since it's an integer factor of an odd integer. However $\deg(\alpha, F(\alpha^2)) \leq 2$, since α is a root of the quadratic $x^2 - \alpha^2 \in F(\alpha^2)[x]$.

this implies it must be 1, so $\left[F(\alpha) : F(\alpha^2)\right] = 1$,

and $F(\alpha^2) = F(\alpha)$.