Midterm exam: tonight 7-9 pm here (Rm 200-205)
Handwritten reference sheet allowed (9.4, 13.1 - 13.6, 14.1)
Next h/w due week after next

Today: exam review

A partial list of somethings we know how to do:

- Prove (ir)reducibility
  Eisenstein, rational root thm., reduction mod p
- Computations in ext'n fields
  e.g. $F(\theta)$; compute powers of θ, use fact that $m_\theta(\theta) = 0$
- Determine constructability
  degree must be a power of 2
- Compute field ext'ns & degrees
  e.g cyclotomic ext'ns, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, splitting field of x^3-2
- Compute field automorphisms & determine if ext'n is Galois
  roots of poly must map to each other
- Determine whether a poly/extn is separable, compute sep, insep degrees
  check whether $\gcd(f, Df) = 1$
- Computations w/ roots of unity, cyclotomic polys

Isomorphisms involving ext'n fields:

Thm 6: Let $f(x) \in F[x]$ be irred. Let α be a root of f

Then,

$$F[x]/(f(x)) \to F(\alpha)$$

$$x \longmapsto \alpha$$

Thm 8: Let $\varphi : F \xrightarrow{\sim} F'$ be an isom. of fields, $f(x) \in F[x]$ irred.

Let $f' = \varphi(f)$. Let α be a root of f, β a root of f'.

Then $\exists$ isom.

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$

$$\alpha \longmapsto \beta$$

$$a \longmapsto \varphi(a), \quad a \in F$$

$$\begin{array}{ccc} \sigma : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ | & & | \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

Can add roots in inductively: σ becomes φ when we add the next root e.g.

$$\begin{tikzcd}[row sep=small]
\sigma : F(\alpha,\gamma) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta,\delta) \arrow[d, dash] \\
\sigma' : F(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & F'(\beta) \arrow[d, dash] \\
\varphi : F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

γ root of g
δ root of g'

α root of f
β root of f'

Thm 27: Let $\varphi : F \xrightarrow{\sim} F'$ be an isom. of fields, $f(x) \in F[x]$ irred. Let $f' = \varphi(f)$. Let K be a splitting field for f/F and K' be a splitting field for f'/F'.

Then $\exists$ isom.

$$\sigma : K \xrightarrow{\sim} K'$$

$$a \longmapsto \varphi(a), \quad a \in F$$

$$\begin{tikzcd}
\sigma : K \arrow[r, "\sim"] \arrow[d, dash] & K' \arrow[d, dash] \\
\varphi : F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

To use together (as we did in Prop 14.5):

$$\begin{array}{lcccc}
 & \sigma: & K & \xrightarrow{\sim} & K' \\
\text{Thm 13.27} & & | & & | \\
 & \tau: & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\
\text{Thm 13.8} & & | & & | \\
 & \varphi: & F & \xrightarrow{\sim} & F'
\end{array}$$

K: splitting field of f
K': splitting field of f'
α: root of f
β: root of f'

Similar ideas for alg. closures

13.5.11: Let $F \subseteq K$. If f is perfect and $f \in F[x]$ has no repeated irred. factors in $F[x]$, prove that $f(x)$ has no repeated irred. factors in $K[x]$

Pf: Write $f = f_1 \cdots f_n$, f_i irred.
Since F is perfect each of $f_1, \ldots, f_n$ are sep., so split into distinct irred. factors$/K$. If f_i, f_j share an irred factor$/K$, they share a root $\alpha \in K$.
Therefore, $(x-\alpha) \mid \gcd(f_i, f_j)$ in K, but since $\gcd(f_i, f_j) \in F$,

$f_i \mid \gcd(f_i, f_j)$ & $f_i \mid \gcd(f_i, f_j)$, so $f_i = f_j$.

Ex 14.1.4: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}$

Galois since splitting field of $(x^2-2)(x^2-3)$

$$[K:F] = [K:\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$

$$\leq [\mathbb{Q}(\sqrt{3}):\mathbb{Q}][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 4$$

and $[K:F] > 2$ since $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

So $\mathrm{Gal}(K/F) = [K:F] = 4$

$\sqrt{2}$ must be mapped to a root of $x^2 - 2$

$\sqrt{3}$ must be mapped to a root of $x^2 - 3$

4 possibilities: $\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$ $\begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$

Must all give automs.

$\begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$ $\begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$

Ex: Let $\zeta := \zeta_8$. Compute $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$

Then $(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^6 = 2 \in \mathbb{Q}$,

so $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] \leq 2$

but $\zeta + \zeta^{-1} \notin \mathbb{Q}$, so $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2$

Also, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$, so by the Tower Law,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$$

Minimal poly.: $x^2 - (\zeta + \zeta^{-1})x - 1$