Announcement: H/W 2 posted, due Tues. 1/24 noon

Recall: α alg. $/F \implies \exists$ irred. monic poly $m_{\alpha,F}(x) \in F[x]$ w/ α as a root & $[F(\alpha):F] = \deg m_{\alpha,F}$

Prop 12: If $[K:F] = n$, $\alpha \in K$, then α is a root of a poly. of deg $\leq n$ over F.

Pf: $\dim_F K = n$, so $1, \alpha, \dots, \alpha^n$ must be linearly dep.

Cor 13: If K/F is finite (i.e. $[K:F] < \infty$), then it is algebraic.

Tower Law (Thm. 14): $F \subseteq K \subseteq L$: fields

$$[L:F] = [L:K][K:F]$$

Pf: If either $[L:K] = \infty$ or $[K:F] = \infty$, then $[L:F] \geq \max([L:K], [K:F]) = \infty$.

Otherwise, let $m = [L:K]$ with basis $\alpha_1, \dots, \alpha_m$ for L/K and $n = [K:F]$ with basis $\beta_1, \dots, \beta_n$ for K/F.

Let $l \in L$. Then l can be written (uniquely) as

$$l = a_1\alpha_1 + \cdots + a_m\alpha_m, \quad a_i \in K$$

Furthermore, each of these a_i can be written (uniquely)

$$a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n,$$

So $$l = \sum_{\substack{1\le i\le m \\ 1\le j\le n}} b_{ij}\alpha_i\beta_j$$ is a linear comb. of

the mn elts. $\alpha_i\beta_j \in L$, so $\{\alpha_i\beta_j\}$ span L, and $[L:F] \le mn$.

On the other hand, if $\sum_{\substack{1\le i\le m \\ 1\le j\le n}} b_{ij}\alpha_i\beta_j = 0$, one can

show by reversing the above process that all the $b_{ij} = 0$, so $\{\alpha_i\beta_j\}$ are linearly independent, and so $[L:F] \ge mn$. $\square$

Examples: 1) Let α be a root of any irred. poly of deg. 3. Then $\sqrt{2} \notin \mathbb{Q}(\alpha)$. To see this, note by Prop. 11 that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. If $\sqrt{2} \in \mathbb{Q}(\alpha)$, then by the Tower Law

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

must be even.

2) Can use Tower Law to prove that $x^3 - \sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{2})$:

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ since $x^2 - 2$ is irred.

$[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}] = 6$ since $x^6 - 2$ is irred.

Tower law:

$$\underbrace{[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}]}_{6} = \underbrace{[\mathbb{Q}(\sqrt[6]{2}):\mathbb{Q}(\sqrt{2})]}_{\text{must be } 3}\underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{2}$$

So $x^3 - \sqrt{2} = m_{\sqrt[6]{2}, \mathbb{Q}(\sqrt{2})}(x)$

Now, we can characterize all finite field ext'ns K/F (i.e. $[K:F]<\infty$).

Thm 17:

K/F finite $\Longleftrightarrow$ K is generated by a finite number of algebraic elts. over F.

Pf: $\Leftarrow$: If $K = F(\underbrace{\alpha_1, \dots, \alpha_n}_{\text{alg.}})$, then

let $F_i = F(\alpha_1, \dots, \alpha_i)$, so

$$F = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n = K$$

Since α_j alg. $/F$, α_j is alg. $/F_i$ for any i

Why? b/c $m_{\alpha_j, F_i} \mid m_{\alpha_j, F}$, so $[F_i(\alpha_j):F_i] \leq [F(\alpha_j):F] < \infty$.

Therefore, if $d_j := [F(\alpha_j):F]$, we have

$$[K:F] = [K:F_{n-1}] \cdots [F_1:F] = [F_{n-1}(\alpha_n):F_{n-1}] \cdots [F(\alpha_1):F]$$
$$\leq d_1 \cdots d_n < \infty$$

Next time: Constructability by straightedge and compass

F