BASIC FIELD THEORY

COLTON GRAINGER (MATH 6140 ALGEBRA 2)

[1, No. 13.2.16]. *Given.* Let K/F be an algebraic extension. Let R be a ring such that $K \supset R \supset F$.

To prove. R is a subfield of K containing F.

Proof. We argue first that R is an integral domain, then then R is a field.

The inclusion $F \hookrightarrow R$ is a nontrivial ring homomorphism, that demonstrates in particular $1 \in F \subset R$. So R is a unital ring. Commutativity and the absence of zero divisors follow from the assumption $R \subset K$.

- To verify commutativity: Let $a, b \in R \subset K$. Then $ab = ba$ in K. Therefore $ab = ba$ in R.
- To verify that R has no zero divisors: Suppose $a, b \in R$ such that $ab = 0$. Then $a, b \in K$, which is a field, and so $a = 0$ or $b = 0$.

We have shown R is a commutative unital ring without zero divisors. By definition, R is an integral domain.

We now show that R is a field. It suffices to prove each nonzero element $\alpha \in R$ is invertible in R. So take $\alpha \in R$. Because K is algebraic over F, there is a minimal degree nonzero monic polynomial

$$p_\alpha(x) = x^n + \lambda_{n-1}x^{n-1} + \cdots + \lambda_1 x + \lambda_0 \quad \text{with coefficients } \lambda_k \text{ in } F$$

for which $p_\alpha(\alpha) = 0$. Note $\lambda_0 \neq 0$ by minimality of p_α. Whence

$$\lambda_0 = -\alpha^n - \lambda_{n-1}\alpha^{n-1} - \cdots \lambda_1 \alpha.$$

Therefore

$$1 = \alpha \left(\frac{-\alpha^{n-1} - \lambda_{n-1}\alpha^{n-2} - \lambda_{n-2}\alpha^{n-2} - \cdots - \lambda_1}{\lambda_0} \right) =: \alpha(\alpha^{-1}). \tag{1}$$

(We may divide by λ_0 because $\lambda_0^{-1} \in F \subset R$.) Note the λ_k are in $F \subset R$ and the power α^k are in R. Therefore α^{-1} as defined in (1) is an element of R. Therefore each nonzero element of R is a unit in R.

To summarize: R is an integral domain, $K \supset R \supset F$, and all nonzero elements of R are invertible. We conclude that (by definition of subfield) R is a subfield of K containing F. ☐

[1, No. 13.2.19]. *Given.* Let K/F be a degree n field extension. Let $\mathscr{M}_n(F)$ be the ring of $n \times n$ matrices with entries from F.

To prove.

(a) For any $\alpha \in K$, the action of α on K by left multiplication is an F-linear transformation of K.

(b) K is isomorphic to a subfield of the ring $\mathscr{M}_n(F)$.

(c) $\mathscr{M}_n(F)$ contains an isomorphic copy of every extension E/F of degree at most n.

Proof. (Remark: It's best to make as little reference to the basis for K over F as possible.)

Date: 2019-03-17.

(a) Let $\alpha \in K$ act by left multiplication on K, i.e., $\alpha.\delta = \alpha\delta$ for all $\delta \in K$. To verify that the action is an F-linear transformation, consider $\beta, \gamma \in K$ and $\lambda \in F$. First note α respects scalar multiplication:

$$\begin{aligned} \alpha.(\lambda\beta) &= \alpha\lambda\beta && \text{by definition of the action} \\ &= \lambda\alpha\beta && \text{by commutativity of } K \\ &= \lambda(\alpha.\beta). \end{aligned}$$

Next observe α respects vector addition:

$$\begin{aligned} \alpha.(\beta+\gamma) &= \alpha(\beta+\gamma) && \text{by definition of the action} \\ &= \alpha\beta + \alpha\gamma && \text{by distributivity in } K \\ &= (\alpha.\beta) + (\gamma.\beta). \end{aligned}$$

Therefore the action of α on K is an F-linear transformation of K.

(b) Because K is a degree n extension of F, we may choose a basis $\mathscr{E}$ for K as an n-dimensional vector space over F. Define a ring homomorphism $\varphi\colon K \to \mathscr{M}_n(F)$ by $\varphi(\alpha) = [\alpha]$, where $[\alpha]$ is the matrix representation of the linear transformation $\alpha\colon K \to K$ with respect to the basis $\mathscr{E}$ for K [1, No. 11.10]. To verify that φ is a ring homomorphism, take $\alpha, \beta \in K$. Note for any $\delta \in K$, the actions of α and β satisfy

$$(\alpha+\beta).\delta = \alpha\delta + \beta\delta = \alpha.\delta + \beta.\delta, \tag{2}$$

and

$$(\alpha\beta).\delta = \alpha\beta\delta = \alpha.(\beta.\delta). \tag{3}$$

By inspection of the definition of matrix addition along with the observations in (2),

$$\varphi(\alpha+\beta) = [\alpha+\beta] = [\alpha] + [\beta] = \varphi(\alpha)\varphi(\beta).$$

Because the product of matrices representing linear transformations is the matrix representing the composite of these linear transformations, the observations in (3) imply that

$$\varphi(\alpha\beta) = [\alpha\beta] = [\alpha][\beta] = \varphi(\alpha)\varphi(\beta).$$

Therefore $\varphi\colon K \to \mathscr{M}_n(F)$ is a homomorphism of rings.

We now argue φ is a monomorphism. It is not too hard to see that the image of F under φ is the subring of scalar matrices in $\mathscr{M}_n(F)$, i.e., $\varphi(F) = Z(\mathscr{M}_n(F))$. Whence, knowing K is a field with $\varphi\colon K \to \mathscr{M}_n(F)$ a nontrivial ring homomorphism, it must be that φ is injective. Therefore φ algebraically embeds $\varphi\colon K \xrightarrow{\cong} \varphi(K)$ as a subfield in the ring $\mathscr{M}_n(F)$.

(c) Suppose E is an extension of F of degree $m \leq n$. After choosing a basis $\mathscr{B}$ for E, we may define an algebraic embedding $\varphi_E\colon E \to \mathscr{M}_m(F)$ (in the same fashion as we constructed the homomorphism $\varphi\colon K \to \mathscr{M}_n(F)$ in part b). If one identifies $\mathscr{M}_m(F) \hookrightarrow \mathscr{M}_n(F)$, for example, by way of the inclusion

$$\begin{bmatrix} \mathscr{M}_m(F) & \\ & I_{n-m} \end{bmatrix} \subset \big[\mathscr{M}_n(F)\big],$$

then $\varphi_E(E) \subset \mathscr{M}_n(F)$ is an isomorphic image of the field E. $\square$

References

[1] D. Dummit and R. Foote, *Abstract algebra*. Prentice Hall, 2004.