Math 1530: Homework 6

Milan Capoor

31 October 2023

5.9

(a) *Let K/F be an extension of fields. Prove that*

$$[K : F] = 1 \iff K = F.$$

If $K = F$, then for all $k \in K$,

$$k = f \quad \text{for some } f \in F$$

written differently,

$$k = f \cdot 1$$

so $\{1\}$ is a spanning set for K over the F-vector space. But additionally, $\{1\}$ is linearly independent because $a1 = 0 \implies a = 0$. Thus, $\{1\}$ is a basis for F/K and

$$\dim_F(K) = \#\{1\}[K : F] = 1$$

For the other direction, we suppose that $[K : F] = 1$. By definition, $[K : F] = \dim_F(K) = 1$. So the basis for K consists of only one vector. Put differently, every $k \in K$ is a multiple of some element in F and the basis vector $v \in K$:

$$K = \{fv : f \in F\}$$

But since K/F is an extension of fields, $F \subset K$ so $f \in K \implies v = 1$. But this means that

$$K = \{f1 : f \in F\} = \{f : f \in F\} = F \quad \blacksquare$$

(b) *Let L/F be a finite extension of fields, and suppose that $[L : F]$ is prime. Suppose further that K is a field lying between F and L; i.e., $F \subseteq K \subseteq L$. Prove that either $K = F$ or $K = L$.*

Assume that $K \neq F$ and $K \neq L$. Then because $F \subseteq K \subseteq L$, K creates a tower of field extensions $L/K/F$.

By Theorem 5.18,

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

but since $[L : F]$ is prime, we have two cases:

(a) $[L : K] = [L : F], \quad [K : F] = 1$

(b) $[K : F] = [L : F], \quad [L : K] = 1$

From Part (a), if $[K : F] = 1$, $K = F$ and if $[L : K] = 1$, $L = K$ so we have a contradiction and $K \neq F$ or $K \neq L$. ■

5.14

This exercise asks you to prove the uniqueness of the quotient and remainder appearing in Proposition 5.20. Let F be a field, let $f(x), g(x) \in F(x)$ be polynomials with $g(x) \neq 0$, and suppose that there are polynomials $q_1(x), q_2(x), r_1(x), r_2(x) \in F(x)$ satisfying

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x) \quad \text{with } \deg(r_1) < \deg(g), \\ f(x) &= g(x)q_2(x) + r_2(x) \quad \text{with } \deg(r_2) < \deg(g). \end{aligned}$$

Prove that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$.

$$\begin{aligned} g(x)q_1(x) + r_1(x) &= g(x)q_2(x) + r_2(x) \\ g(x)q_1(x) - g(x)q_2(x) &= r_2(x) - r_1(x) \\ g(x)[q_1(x) - q_2(x)] &= r_2(x) - r_1(x) \end{aligned}$$

But $\deg(r_2(x) - r_1(x)) \leq \deg(r_2) < \deg(g)$ so the only way for the LHS and RHS to be equal is if $q_1(x) - q_2(x) = 0 \implies q_1(x) = q_2(x)$. Then, since the LHS is equal, $r_2(x) - r_1(x) = 0 \implies r_2(x) = r_1(x)$. ■

5.15

Let F be a field.

(a) *Prove that every polynomial of degree 1 in $F[x]$ is irreducible.*

Let $ax + b$ $(a \neq 0)$ be any polynomial of degree 1 in $F[x]$. Consider the ideal $(ax + b)F[x]$. Suppose that there is an ideal I such that

$$(ax + b)F[x] \subseteq I \subseteq F[x]$$

From Theorem 5.21, every ideal in $F[x]$ is principal so $\exists g(x) \in F[x] : I = g(x)F[x]$, so

$$(ax + b)F[x] \subseteq g(x)F[x] \subseteq F[x]$$

But this means that $ax + b \in (g(x))$ so

$$ax + b = g(x)h(x) \quad h(x) \in F[x]$$

But $\deg(gh) = \deg(g) + \deg(h)$ (Definition 5.19) and $\deg(ax + b) = 1$ so

$$\deg(g) + \deg(h) = 1$$

Further, $\deg(g) \geq 1$ or else $ax+b \notin g(x)F[x]$ so $\deg(h) = 0$. Thus $h(x) = c \in F$. So $ax + b = cg(x)$ and $\deg(g) = 1$. So $ax + b = g(x)$ up to a constants and the only factorization of $ax + b$ is trivial. Thus, any polynomial of degree 1 is irreducible. ■

(b) *Let $f(x) \in F[x]$ be a polynomial of degree 2. Prove that $f(x)$ is irreducible if and only if it has no roots in F.*

Assume that f has no roots in f. Then it cannot be written in the form

$$(ax + b)(cx + d)$$

with $a, b, c, d \in F$ because then $x = -\frac{b}{a}$ and $x = -\frac{d}{c}$ would be roots. But this means that there are no degree 1 factorizations of f, so it is irreducible.

For the other direction, we want to show that if it is irreducible, it has no roots in F. By contraposition, if f is reducible, it *does* have roots in F. This is much easier because if f is reducible, then it can be written as the product of two linear polynomials because it itself is quadratic:

$$f(x) = (ax + b)(cx + d)$$

But this polynomial has roots at $-\frac{b}{a}$ and $-\frac{d}{c}$ which are in F by existence of inverses and closure of F. Thus, if f is reducible, it has roots in F. So we conclude that f is irreducible if and only if it has no roots in F. ■

(c) *Let $f(x) \in F[x]$ be a polynomial of degree 3. Prove that $f(x)$ is irreducible if and only if it has no roots in F.*

In a very similar approach to the above, we will seek to prove the easier contrapositive: f is reducible iff it has roots in F.

If f is reducible, it can be written in the form

$$f(x) = (ax + b)(cx^2 + dx + e)$$

because $\deg(ax + b) + \deg(cx^2 + dx + e) = 3$. But, then $x = -\frac{b}{a} \in F$ would be a root because

$$f(-\frac{b}{a}) = (a \cdot (-\frac{b}{a}) + b)(c(-\frac{b}{a})^2 + d(-\frac{b}{a}) + e) = 0 \cdot (c(-\frac{b}{a})^2 + d(-\frac{b}{a}) + e) = 0$$

Meanwhile, if f has a root a in F then $(x - a)$ is a factor of f by the splitting field. Then, having a degree 1 factor, f is reducible.

Thus f is reducible iff it has roots in F and by the Law of Contraposition, $f(x)$ is irreducible if and only if it has no roots in F. ■

(d) *Let $f(x) = x^4 + 2$. Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

If f is reducible, then it can be written in the form

$$f(x) = (ax^2+bx+c)(dx^2+ex+f) = (ad)x^4+(ae+bd)x^3+(af+be+cd)x^2+(ce+bf)x+cf$$

But we want

$$\begin{cases} ad = 1 \\ ae + bd = 0 \\ af + be + cd = 0 \\ ce + bf = 0 \\ cf = 2 \end{cases}$$

so from the middle three equations,

$$\begin{pmatrix} e & d & 0 \\ f & e & d \\ 0 & f & e \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

which gives the solution

$$\begin{cases} a = 0 \\ b = 0 \\ c = 0 \end{cases}$$

But this leads to contradictions with

$$(0)d = 1$$

and

$$(0)f = 2$$

so f must be irreducible. ■

(e) *Let $f(x) = x^4 + 4$. Prove that $f(x)$ is reducible in $\mathbb{Q}[x]$, despite the fact that it has no roots in $\mathbb{Q}$.*

If f is reducible, it can be written $f(x) = p(x)q(x)$ where $\deg(p) + \deg(q) = 4$. The natural first guess is that both p and q are polynomials of degree 2. Further, we want them both to be monic or to have their leading coefficients be multiplicative inverses. Finally, we want the product of their constant terms to be 4. We will make a first guess of

$$\begin{aligned}(x^2 + ax + 2)(x^2 + bx + 2) &= x^4 + ax^3 + 2x^2 + bx^3 + abx^2 + 2ax + 2x^2 + 2bx + 4 \\ &= x^4 + ax^3 + bx^3 + 4x^2 + abx^2 + 2ax + 2bx + 4 \\ &= x^4 + (a + b)x^3 + (4 + ab)x^2 + (2a + 2b)x + 4\end{aligned}$$

Setting this equal to $x^4 + 4$ gives us a system of equations constraining a and b:

$$\begin{cases} a + b = 0 \\ 4 + ab = 0 \\ 2a + 2b = 0 \end{cases} \implies \begin{cases} a = 2 \\ b = -2 \end{cases}$$

So we have found a factorization

$$x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

and thus f is reducible in $\mathbb{Q}[x]$. ■

5.20

Let F be a field, let $f(x) \in F[x]$ be a possibly reducible non-constant polynomial, and let $d = deg(f)$.

(a) *Prove that there exists a field extension K/F satisfying $[K : F] \leq d$ such that $f(x)$ has a root in K.*

If f is irreducible, then by Theorem 5.27, $K = F[x]/f(x)F[x]$ is a finite extension field of F with degree $[K : F] = \deg(f) = d$ which contains a root of $f(x)$.

If f is reducible, then we can say $f(x) = g(x)h(x)$ with $\deg(g) < d$ and $\deg(h) < d$. If either g or h is irreducible, then by the case above, the extension field $F[x]/g(x)F[x]$ (or $F[x]/h(x)F[x]$) contains a root of g (or h). Then since that polynomial is a factor of f, the root is also a root of f and the degree of the extension field will be less than d.

If neither g nor h is irreducible, then each can be written as the product of two more polynomials of lesser degree. Again, these polynomials will either be irreducible and contain a root of f or we can find yet smaller factors of f. Eventually, f will have an irreducible polynomial as a factor because all degree 1 polynomials are irreducible (5.15a).

Thus, any $f(x) \in F[x]$ has a root in some extension field of degree less than or equal to $\deg(f)$. ■

(b) *Prove that there exists a field extension L/F and elements $c \in F$ and $a_1, \ldots, a_d \in L$ such that $f(x)$ factors in $L[x]$ as*

$$f(x) = c(x - a_1)(x - a_2) \ldots (x - a_d)$$

(Note that $a_1, \ldots, a_d$ need not be distinct.) Prove that it is always possible to find such an L that also satisfies

$$[L : F] \leq d!$$

The field L is called a splitting field for the polynomial $f(x)$ over the field F

If $\deg(f) = d = 1$, then $f(x) = ax + b$ and we can factor out the leading coefficient such that it has a monic linear polynomial as a factor.

For $d \geq 1$, we note that from part (a), we have an extension G/F where $G = F[x]/g(x)F[x]$ which contains a root of $g(x)$, one of the factors of f. We

call this root $a_1 \in G$ and note that g must be of the form $g(x) = x - a_1$ because it is irreducible. Thus,

$$f(x) = c(x - a_1)h(x)$$

where $c \in F$, $h(x) \in F[x]$ and $\deg h = d - 1$.

Our approach to finding g and the root a_1 in part (a) depended on a tower of reducible polynomials factoring into irreducible polynomials:

$$f(x) = g(x) \cdot \prod_i h_i(x)$$

where each $h_i(x)$ is an irreducible polynomial of the form

$$h_i(x) = x - a_i$$

and each a_i is a root of h_i in the extension field $H_i = F[x]/h_i(x)F[x]$.

By proposition 5.15, the smallest field that contains $F[x]$ and all the roots $a_1, \ldots, a_d$ is $L = F(a_1, a_2, \ldots, a_d)$ so L/F is a field extension such that f factors in $L[x]$ as

$$f(x) = c(x - a_1)(x - a_2)\ldots(x - a_d)$$

$(c \in F)$.

Now consider the degree of this field. In part (a), we found the first root in $[G : F] \leq d$. But the order of roots does not matter because of commutativity in the polynomial ring so equivalently, any root can be found in an extension field of degree at most d. But again by Proposition 5.15, to have two roots (say in extensions H_1 and H_2), we need to construct the larger extension $H_2/H_1/F$.

By theorem 5.18,

$$[H_2 : F] = [H_2 : H_1][H_1 : F] \leq (d - 1) \cdot d$$

so, generalizing,

$$[L : F] = [L : H_d][H_d : H_{d-1}]\ldots[H_1 : F] \leq d \cdot (d - 1) \cdot (d - 2) \cdot 2 \cdot 1 = d! \quad \blacksquare$$

5.21ab

Let F be a finite field with q elements.

(a) *Prove that every non-zero element of F is a root of the polynomial $x^{q-1} - 1$. (Hint. Apply the corollary of Lagrange's Theorem, Corollary 2.50, to the group of units F^* .)*

Because F is a field, the set of non-zero elements of F is the group of units F^*. By Corollary 2.50, the order of every element of this group must divide the order of the group, $q - 1$. i.e., for any $x \in F^*$

$$o(x) \cdot m = q - 1 \quad (m \in \mathbb{Z})$$

so

$$x^{q-1} = x^{o(x)\cdot m} = (x^{o(x)})^m = 1^m = 1$$

This means that every element in the group of units of F satisfies the equation

$$x^{q-1} - 1 = 0$$

so every non-zero element of F is a root of $x^{q-1} - 1$. ■

(b) *Prove that every element of F is a root of the polynomial $x^q - x$.*

Trivially, $x = 0$ is a root.

Now we consider the non-zero elements. By part (a), every non-zero element $x \in F$ satisfies $x^{q-1} - 1 = 0$. Because F is a field, multiplication is closed so we can take the product

$$x(x^{q-1}) - x = 0 \implies x^q - x = 0 \quad \forall x \in F^*$$

so every $x \in F^*$ is a root of $x^q - x$.

Since every non-zero element and the zero element of f are roots of $x^q - q$, every element of F is a root. ■