A Few Notes on Groups, Rings, and Fields

David Meyer

dmm@{1-4-5.net,uoregon.edu}

Last update: September 10, 2017

1 Introduction

Suppose we want to solve an equation of the form

$$f(x) = x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_1 x + a_0 = 0 \tag{1}$$

where the coefficients[1] $a_i \in \mathbb{Q}$. We can notice quite a few interesting things about $f(x)$. For example, if R is a ring then ring of polynomials in x with coefficients in R, denoted $R[x]$, consists of all formal sums

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

where $a_i = 0$ for all but finitely many values of i.

The fundamental theorem of algebra [1] tells us that for any $n > 0$ and arbitrary complex coefficients $a_{n-1}, \ldots, a_0 \in \mathbb{C}$ there is a complex solution $x = \lambda \in \mathbb{C}$. If we iterate the process we find that

$$f(x) = (x - \lambda_0)(x - \lambda_2) \cdot \ldots \cdot (x - \lambda_{n-1}) = 0 \tag{2}$$

for $\lambda_0, \lambda_2, \ldots \lambda_{n-1} \in \mathbb{C}$. Here $f(x) = 0$ iff $x = \lambda_j$ for some $j \in \{0, 1, \ldots, n-1\}$.

Aside: What is being assumed here? Well, we are assuming that if $r \cdot s = 0$ then either r or s (or both) equal zero. If $r \neq 0$ and $s \neq 0$ but $r \cdot s = 0$ we call r and s *zero divisors.*

[1] Note that the largest degree term (x^{n-1}) has coefficient 1. This is called a *monic* polynomial.

A commutative ring with no zero divisors is called an *intergral domain*[2]. The canonical example of an integral domain is the integers $\mathbb{Z}$.

BTW, why is $\mathbb{Z}$ not a field? Well, consider for example that $2 \in \mathbb{Z}$ but $\frac{1}{2} \notin \mathbb{Z}$ so not every non-zero $n \in \mathbb{Z}$ has an inverse in $\mathbb{Z}$ and so $\mathbb{Z}$ is not a field. Every *finite* integral domain is a field however (Theorem 2.1).

Note that if we have zero divisors then the factorization shown in Equation 2 might not find all of the roots of $f(x)$ (values of x for which $f(x) = 0$). Why? Consider the following example:

$$x^2 + 5x + 6 \equiv 0 \bmod 12 \quad \Rightarrow \quad (x+2) \cdot (x+3) \equiv 0 \bmod 12 \tag{3}$$

Here we can read off the roots $x \equiv -2 \bmod 12 \Rightarrow x = 10 \bmod 12$ and $x \equiv -3 \bmod 12 \Rightarrow x = 9 \bmod 12$. So we have two roots (mod 12) at $x = 9$ and $x = 10$. But are these all of the roots? Well, the answer is no. Consider $f(1) \bmod 12 \equiv (1^2 + 5 + 6) \bmod 12 \equiv 0 \bmod 12$. In addition, $f(6) \bmod 12 \equiv (36 + 30 + 6) \bmod 12 \equiv 72 \bmod 12 \equiv 0 \bmod 12$.

So the roots of Equation 3 are $\{1, 6, 9, 10\}$. Why were we only able to find two of the roots (9 and 10) by factoring? It is because the ring $\mathbb{Z}_{12}$ has zero divisors. What are the zero divisors in $\mathbb{Z}_{12}$? Well

$$\begin{aligned}
2 \cdot 6 &\equiv 12 \bmod 12 \equiv 0 \bmod 12 \\
3 \cdot 4 &\equiv 12 \bmod 12 \equiv 0 \bmod 12 \\
4 \cdot 3 &\equiv 12 \bmod 12 \equiv 0 \bmod 12 \\
6 \cdot 2 &\equiv 12 \bmod 12 \equiv 0 \bmod 12 \\
8 \cdot 3 &\equiv 24 \bmod 12 \equiv 0 \bmod 12 \\
9 \cdot 8 &\equiv 72 \bmod 12 \equiv 0 \bmod 12 \\
10 \cdot 6 &\equiv 60 \bmod 12 \equiv 0 \bmod 12
\end{aligned} \tag{4}$$

Note that if p is a prime then $\mathbb{Z}_p$ is an integral domain (has no zero divisors).

So the condition we need is that the set of coefficients are drawn from an integral domain.

Theorem 1.1. Every field F is an integral domain.

Proof: Recall that if F is a field then each non-zero $r \in F$ has an inverse r^{-1}. So suppose $r, s \in F$ and $r \neq 0$ such that $r \cdot s = 0$. Then the claim is that $s = 0$. Why? Consider

[2] Saying that F has no zero divisors is equivalent to saying that F has a cancellation law.

$$
\begin{array}{rcll}
r \cdot s & = & 0 & \text{\# assumption with } r \neq 0 \\
& \Rightarrow & r^{-1} \cdot (r \cdot s) = r^{-1} \cdot 0 & \text{\# multiply both sides by } r^{-1} \\
& \Rightarrow & r^{-1} \cdot (r \cdot s) = 0 & \text{\# } x \cdot 0 = 0 \\
& \Rightarrow & (r^{-1} \cdot r) \cdot s = 0 & \text{\# multiplication is associative} \\
& \Rightarrow & s = 0 & \text{\# } r^{-1} \cdot r = 1
\end{array} \tag{5}
$$

So r is not a zero divisor. But every non-zero element r of the field F has an inverse (r is a "unit") so F has no zero divisors and is by definition an integral domain. □

Theorem 2.1 below shows a limited version of this theorem in the other direction: Every finite integral domain is a field.

2 Splitting Fields

Recall that the ring of polynomials over a field F, denoted $F[x]$, is defined as follows[3]

Definition 2.1. Polynomial Ring over F: The polynomial ring over F is defined as

$$F[x] = \{f(x) \mid f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_{n-1}x^{n-1}\}$$

with $a_i \in F$ and with the usual ring properties.

Aside on notation: while $F[x]$ is defined as above, $F(x)$ is defined differently.

$$F(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p(x), q(x) \in F[x] \right\}$$

There doesn't seem to be any standard convention as to the definitions of $F[x]$ vs. $F(x)$. I've seen $F(x)$ used to mean what I defined as $F[x]$ above.

Definition 2.2. Splitting Field: Let $f \in F[x]$. An extension field[4] E of F, written E/F, is called a *splitting field* for f over F if the following two conditions are satisfied:

1. f factors into linear polynomials ("splits" or "splits completely") in $E[x]$
2. f does not split completely in $K[x]$ for any $F \subsetneq K \subsetneq E$

[3] I reversed the order of Equation 1 since its an easier form to work with. In addition, we can assume $a_{n-1} = 1$ since $f(x)$ is monic.

[4] E is an extension field of F if F is a subfield of E.

2.1 The Evaluation Homomorphism: $e : F[x] \to F[\alpha]$

TBD

2.2 Examples

Example 2.1. $\mathbb{Q}[\sqrt{2}]$ is a splitting field for $x^2 - 2$ over $\mathbb{Q}$.

Why? Consider the conditions in Definition 2.2: First, the polynomial $x^2 - 2$ factors into linear polynomials ("splits") in $\mathbb{Q}[\sqrt{2}][x]$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. To see this, consider

$$\begin{aligned}
\mathbb{Q}[\sqrt{2}] &= a_0(\sqrt{2})^0 + a_1(\sqrt{2})^1 + a_2(\sqrt{2})^2 + a_3(\sqrt{2})^3 + a_4(\sqrt{2})^4 + \cdots + a_{n-1}(\sqrt{2})^{n-1} && \# \text{ defn } \mathbb{Q}[\sqrt{2}] \\
&= a_0 + a_1\sqrt{2} + a_2 2 + a_3 2\sqrt{2} + a_4 4 + a_5 4\sqrt{2} + \cdots + a_{n-1} 2^{\frac{n-1}{2}} && \# \text{ simplify} \\
&= (a_0 + a_2 2 + a_4 4 + \cdots) + (a_1 + a_3 2 + a_5 4 + \cdots)\sqrt{2} && \# \text{ group terms} \\
&= a + b\sqrt{2} && \# \; a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]
\end{aligned}$$

Note that here $a = a_0 + a_2 2 + a_4 4 + \cdots$ and $b = a_1 + a_3 2 + a_5 4 + \cdots$ and that $a, b \in \mathbb{Q}$ since $\mathbb{Q}$ is closed under addition and multiplication.

Next we need to see what $\mathbb{Q}[\sqrt{2}][x]$ looks like. We saw above that the elements of $\mathbb{Q}[\sqrt{2}]$ have the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. So an element $p(x) \in \mathbb{Q}[\sqrt{2}][x]$ looks like (Definition 2.1)

$$\begin{aligned}
p(x) &= \sum_{i=0}^{n-1} (a_i + b_i\sqrt{2})x^i \\
&= (a_0 + b_0\sqrt{2})x^0 + (a_1 + b_1\sqrt{2})x^1 + (a_2 + b_2\sqrt{2})x^2 + \cdots + (a_{n-1} + b_{n-1}\sqrt{2})x^{n-1}
\end{aligned}$$

for some $a_i, b_i \in \mathbb{Q}$.

Now, if we consider the case in which $a_0 = 0, b_0 = 1, a_1 = 1, b_1 = 0$ and $a_i = b_i = 0$ for $1 < i \leq n - 1$ we get an element $p(x) \in \mathbb{Q}[\sqrt{2}][x]$ that looks like

$$\begin{aligned}
p(x) &= (a_0 + b_0\sqrt{2})x^0 + (a_1 + b_1\sqrt{2})x^1 + \sum_{i=2}^{n-1} (a_i + b_i\sqrt{2})x^i \\
&= (0 + 1\sqrt{2})1 + (1 + 0\sqrt{2})x + \sum_{i=2}^{n-1} 0 \\
&= \sqrt{2} + x \\
&= x + \sqrt{2}
\end{aligned}$$

so we can see that $x^2 - 2$ splits in $\mathbb{Q}[\sqrt{2}][x]$ since $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ (let $b_0 = -1$ to get the $(x - \sqrt{2})$ factor).

So the first criteria of Definition 2.2 is satisfied, but is there a field K that splits $x^2 - 2$ such that $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}[\sqrt{2}]$ (the second criteria in Definition 2.2)? Well, if we consider $\mathbb{Q}[\sqrt{2}][x]$ as a vector space over $\mathbb{Q}[\sqrt{2}]$ we see that it is of order 2 (written $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$), so there is no field K such that $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}[\sqrt{2}]$. So the second criteria is true and so $\mathbb{Q}[\sqrt{2}]$ is a splitting field for $f(x) = x^2 - 2$.

Example 2.2. $\mathbb{Q}[\sqrt[3]{2}]$ is *not* a splitting field for $x^3 - 2$ over $\mathbb{Q}$.

Why? Well, it is because the polynomial $x^3 - 2$ does not split in $\mathbb{Q}[\sqrt[3]{2}][x]$. But still why? After all $x^3 - 2$ does have a root at $\sqrt[3]{2}$ in $\mathbb{Q}[\sqrt[3]{2}][x]$. However, if we divide $x^3 - 2$ by $x - \sqrt[3]{2}$ we see that

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2) \tag{6}$$

and it turns out that $h(x) = x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ is *irreducible*[5] in $\mathbb{Q}[\sqrt[3]{2}]$. This is because the roots of $h(x)$ are complex and but everything in $\mathbb{Q}[\sqrt[3]{2}]$ is real.

So what is a splitting field for $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ over $\mathbb{Q}$? Well, we know $x^3 - 2$ splits into the factors shown in Equation 6 in $\mathbb{Q}[\sqrt[3]{2}]$, so one approach would be to adjoin the (complex) roots of $x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2$ to $\mathbb{Q}[\sqrt[3]{2}]$.

The idea to "keep adding roots of irreducible factors" is the core idea in the proof that every polynomial has a splitting field. This observation leads to the following proposition:

Proposition 2.1. Let $f \in F[x]$ and E be an extension field of F. If E contains the roots $\alpha_1, \cdots, \alpha_n$ of f and f splits in $F[\alpha_1, \cdots, \alpha_n][x]$ then $F[\alpha_1, \cdots, \alpha_n]$ is a splitting field for f over F.

Proof: Because f splits in $F[\alpha_1, \ldots, \alpha_n]$ we only need to show that f doesn't split in a proper subfield containing F. Suppose E is such a proper subfield. Then there is at least one root α_i such that $\alpha_i \notin E$. But this would mean that f would not split in E because if it did then α_i would be a root of one of the linear factors in $E[x]$; this would contradict our assumption that $\alpha_i \notin E$. So such an E does not exist.

This result guarantees that if you can find all the roots of a polynomial in *some* extension field, then you can construct a splitting field easily. This is great for polynomials that are

[5] A polynomial $p(x)$ is irreducible if no polynomials $g(x)$ and $h(x)$ exist such that $p(x) = g(x) \cdot h(x)$.

in, say, $\mathbb{Q}[x]$ because it is often easy to find roots in $\mathbb{C}$. But what about more obscure fields like $\mathbb{Z}_7$, where we don't have a good understanding of its extension fields? It is not obvious (at least to me) that polynomials over these fields have splitting fields, but luckily it turns out they do.

Aside: We saw that every field is an integral domain (Theorem 1.1). Here we observe that any finite integral domain (like $\mathbb{Z}_7$) is a field.

Theorem 2.1. Every finite integral domain is a field.

Proof: The proof is based on the fact that since R is an integral domain it has a cancellation law (or equivalently, R has no zero divisors). Having a cancellation law means that

$$ab = ac \implies b = c \tag{7}$$

To see why any finite integral domain R is a field, consider $R = \{r, r^2, r^3, \ldots, r^n\}$ where $r^k \neq 0$ for $1 \leq k \leq n$. Since R is finite we will have $r^k = r^l$ for some k and l such that $k > l$. Then

$$\begin{array}{rlll}
r^k & = & r^l & \text{\# } R \text{ is a finite integral domain} \\
 & \Rightarrow & r \cdot r^{k-1} = r \cdot r^{l-1} & \text{\# factor out } r \\
 & \Rightarrow & r^{k-1} = r^{l-1} & \text{\# use cancellation law (cancel } r\text{, Equation 7)} \\
 & \Rightarrow & r \cdot r^{k-2} = r \cdot r^{l-2} & \text{\# factor out } r \\
 & \Rightarrow & r^{k-2} = r^{l-2} & \text{\# use cancellation law (cancel } r\text{, Equation 7)} \\
 & \vdots & & \text{\# iterate } l-1 \text{ times} \\
 & \Rightarrow & r^{k-l+1} = r^1 & \text{\# ...} \\
 & \Rightarrow & r \cdot r^{k-l} = r \cdot r^0 & \text{\# factor out } r \\
 & \Rightarrow & r^{k-l} = r^0 & \text{\# use cancellation law (cancel } r\text{, Equation 7)} \\
 & \Rightarrow & r^{k-l} = 1 & \text{\# } r^0 = 1
\end{array}$$

So $r^{k-l} = 1$. If $k - l = 1$ then r is a unit since $r^{k-l} = r^1 = 1$ so r^{-1} is $\frac{1}{r}$. Otherwise $k - l > 1$ and $r^{k-l} = 1 \Rightarrow r^{k-l-1} = \frac{1}{r}$. So $r^{-1} = r^{k-l-1}$ and every $r \neq 0 \in R$ has an inverse. Thus every non-zero $r \in R$ is a unit and so R is a field. $\square$

3 Note: Gauss and the Gaussian Integers $\mathbb{Z}[i]$

First, recall that the Gaussian Integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z} \text{ and } i = \sqrt{-1}\}$. Gauss found that the polynomial $a^2 + b^2$ had a unique factorization (would "split") in $\mathbb{Z}[i]$:

$$a^2 + b^2 = (a - bi)(a + bi)$$

The natural question was are there other values that could be adjoined to $\mathbb{Z}$ to form a new number system in which some polynomial would split. For example

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

Here we can factor say 6 in $\mathbb{Z}[\sqrt{-5}]$ as $6 = 2 \cdot 3 = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$. So the natural question is there other values in which we can factor polynomials into irreducible factors? It turns out there is are precisely nine such numbers, $\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ (Gauss discovered this sequence but couldn't prove that these were the only such numbers). That is, only the negative square root of these numbers can be adjoined to $\mathbb{Z}$ to get a ring with unique factorization. This is the set

$$\{\sqrt{-1}, \sqrt{-2}, \sqrt{-3}, \sqrt{-7}, \sqrt{-11}, \sqrt{-19}, \sqrt{-43}, \sqrt{-67}, \sqrt{-163}\}$$

Interestingly, a Heegner number (so named for the amateur mathematician that proved Gauss's conjecture) is a square-free positive integer d such that the imaginary quadratic field $\mathbb{Q}[\sqrt{-d}]$ has unique factorization.

These numbers turn up in all kinds of interesting places, including Ramanujan's constant $e^{\pi\sqrt{163}}$. For example

$$\begin{aligned}
e^{\pi\sqrt{19}} &\approx 96^3 + 744 - 0.22 \\
e^{\pi\sqrt{43}} &\approx 960^3 + 744 - 0.000\,22 \\
e^{\pi\sqrt{67}} &\approx 5\,280^3 + 744 - 0.000\,0013 \\
e^{\pi\sqrt{163}} &\approx 640\,320^3 + 744 - 0.000\,000\,000\,000\,75
\end{aligned}$$

or alternatively

$$\begin{aligned}
e^{\pi\sqrt{19}} &\approx 12^3(3^2 - 1)^3 + 744 - 0.22 \\
e^{\pi\sqrt{43}} &\approx 12^3(9^2 - 1)^3 + 744 - 0.000\,22 \\
e^{\pi\sqrt{67}} &\approx 12^3(21^2 - 1)^3 + 744 - 0.000\,0013 \\
e^{\pi\sqrt{163}} &\approx 12^3(231^2 - 1)^3 + 744 - 0.000\,000\,000\,000\,75
\end{aligned}$$

Theorem 3.1. If m is an integer then either $m^2 \equiv 0 \pmod 4$ or $m^2 \equiv 1 \pmod 4$.

Proof: Let $m \in \mathbb{Z}$. Then m is either even or m is odd.

Case I: Assume m is even.
If m is even then there exists $k \in \mathbb{Z}$ such that $m = 2k$.
Then $m^2 = 4k^2$, and so $4|m^2$ and hence $m^2 \equiv 0 \pmod 4$.

Case II: Assume m is odd.
If m is odd then there exists $k \in \mathbb{Z}$ such that $m = 2k + 1$.
Then $m^2 = 4k^2 + 4k + 1 \Rightarrow m^2 - 1 = 4(k^2 + k)$ so
$4|(m^2 - 1)$. Therefore $(m^2 - 1) \equiv 0 \pmod 4$ and
$m^2 \equiv 1 \pmod 4$.

Thus if m is an integer then either $m^2 \equiv 0 \pmod 4$ or $m^2 \equiv 1 \pmod 4$. $\square$

Recall that a *unit* in a ring R is an element which has a multiplicative inverse.

Proposition 3.1. Let F be a field and let $F[x]$ be the polynomial ring over F. Then units in $F[x]$ are exactly the nonzero elements of F.

Proof: First, observe that the nonzero elements of F are invertible in F since F is a field. These elements are also invertible in $F[x]$ since, as we just saw, they are invertible in F.

Suppose, OTOH that $f(x) \in F[x]$ is invertible. That is, $f(x)g(x) = 1$ for some $g(x) \in F[x]$. Then $\deg f \cdot g = \deg f + \deg g = \deg 1 = 0$, which requires that both f and g to have degree 0. In particular, f must have degree 0. So f is a nonzero constant, i.e. f is an element of F. $\square$

Proposition 3.2. Let R be a commutative ring and let a be a unit in R. Then a divides r for all $r \in R$.

Proof: First assume $1 \in R$ (R is a ring rather than a rng). Then a a unit in R means that there exists $b \in R$ such that $ab = 1$. Note that $ab \in R$ since R is closed under multiplication.

Now let r be an arbitrary element of R. Then

$$\begin{array}{rcll} r & = & 1 \cdot r & \text{\# 1 is the multiplicative identity} \\ & = & (ab) \cdot r & \text{\# } a \text{ a unit} \Rightarrow 1 = ab \text{ with } ab \in R \\ & = & a \cdot (br) & \text{\# multiplication is associative} \\ & \Rightarrow & a|r & \text{\# } a|r \Rightarrow r = a \cdot m. \text{ Here } m = br. \ \square \end{array}$$

Proposition 3.3. Let R be a commutative ring and let a and b be units in R. Then ab is a unit in R.

Proof: Let $a, b \in R$ be units. Then there exists $c, d \in R$ such that $ac = 1$ and $bd = 1$. To show that ab is a unit in R consider

$$\begin{aligned}
ac &= a(1c) && \# \ c = 1c \\
&= a(1)c && \# \text{ multiplication is associative} \\
&= a(bd)c && \# \ b \text{ a unit so } 1 = bd \\
&= abdc && \# \text{ multiplication is still associative} \\
&= (ab)(dc) && \# \text{ multiplication is associative} \\
&= 1 && \# \ ac = 1
\end{aligned}$$

So $(ab)(dc) = 1$ which implies that ab is a unit in R with inverse dc. $\square$

4 Acknowledgements

References

[1] Matthew Steed. Proofs of the Fundamental Theorem of Algebra. http://math.uchicago.edu/~may/REU2014/REUPapers/Steed.pdf, 2014. [Online; accessed 29-Mar-2019].