III.F. Fields

Given a field $\mathbb{F}$, the intersection of all its subfields is called the **prime subfield**. Clearly, this contains the prime ring $\eta(\mathbb{Z})$, which is isomorphic to $\mathbb{Z}_p$ (p prime) or to $\mathbb{Z}$. In the first case, $\mathbb{Z}_p$ *is* the prime subfield; in the latter, we may extend $\eta\colon \mathbb{Z} \hookrightarrow \mathbb{F}$ to $\mathbb{Q}$ by $\eta(\frac{r}{s}) := \eta(r)\eta(s)^{-1}$.

This extension is well-defined since given $\frac{r'}{s'} = \frac{r}{s}$, we have $r's = rs' \implies \eta(r')\eta(s) = \eta(r)\eta(s') \implies \eta(r')\eta(s')^{-1} = \eta(r)\eta(s)^{-1}$. To see that it is injective, recall from III.D.23 that a field has no nontrivial proper ideals. Hence

(III.F.1) all (ring) homomorphisms *from a field* to a ring *are injective.*

We conclude

III.F.2. PROPOSITION. *The prime subfield of a field* $\mathbb{F}$ *is isomorphic to* $\mathbb{Q}$ *or* $\mathbb{Z}_p$.

Also note the following about ring homomorphisms $\varphi\colon \mathbb{F} \to R$ (in addition to (III.F.1)): given $f \in \mathbb{F}$ (with inverse f^{-1}), we have $\varphi(f)\varphi(f^{-1}) = \varphi(ff^{-1}) = \varphi(1) = 1 \implies \varphi(f^{-1}) = \varphi(f)^{-1}$.

One way to construct fields (beyond the usual suspects) is via quotient rings. For the remainder of this section, let R denote a *commutative* ring.

III.F.3. THEOREM. *If* $I \subsetneq R$ *denotes a proper ideal, then*

$$R/I \text{ is a field} \iff I \text{ is maximal.}$$

PROOF. ($\Longleftarrow$): Given a proper ideal $J \subsetneq R/I$, its preimage under $\nu\colon R \twoheadrightarrow R/I$ is a proper ideal containing I (and equal to I iff $J = \{0\}$) by III.E.8. Hence if I is maximal, the only possibility for J is $\{0\}$. By III.D.23, R/I is a field.

($\Longrightarrow$): Assume R/I is a field, and let $J \subset R$ be an ideal with $I \subsetneq J$. We will show that $J = R$ so that I is maximal.

Given any $r \in J\backslash I$, the ideal (I, r) generated by I and r is contained in J. Since $r \notin I$, we have $\nu(r) \neq 0$. As ν is onto, there exists

$r' \in R$ with $\nu(r') = \nu(r)^{-1}$; and then

$$\nu(1 - rr') = \nu(1) - \nu(r)\nu(r') = 1 - 1 = 0 \quad \Longrightarrow \quad a := 1 - rr' \in I.$$

This means $1 = a + rr' \in (I, r)$ hence $(I, r) = J = R$. $\square$

III.F.4. EXAMPLES. (i) Similarly to III.E.6(i), we have (by the Fundamental Theorem III.E.5) $\frac{\mathbb{Q}[x]}{(x^2-10)} \overset{\cong}{\to} \mathbb{Q}[\sqrt{10}]$, which we know is a field. Hence $(x^2 - 10)$ is maximal.

(ii) Given a submanifold $\mathcal{S} \subset \mathcal{M}$, when is $C^0(\mathcal{S})$ a field? It can only consist of one point — otherwise there are obvious zero-divisors. So $\mathcal{I}_{\mathcal{S}}$ is maximal $\iff$ $\mathcal{S}$ is a point.

(iii) Since $\frac{\mathbb{Z}[\sqrt{10}]}{(3,1+\sqrt{10})} \cong \mathbb{Z}_3$, the ideal $(3, 1 + \sqrt{10})$ is maximal. None of the principal ideals $(1 + \sqrt{10})$, $(-1 + \sqrt{10})$, (3) are.

Briefly veering off topic, there is an important variant of III.F.3.

III.F.5. DEFINITION. An ideal $I \subsetneq R$ is **prime** if

$$ab \in I \quad \Longrightarrow \quad a \in I \text{ or } b \in I.$$

III.F.6. THEOREM. *R/I is a domain $\iff$ I is prime.*

PROOF. I is not prime $\iff$ $\exists a, b \in R \backslash I$ such that $ab \in I$. Equivalently, taking $\bar{a} = a + I$ etc., $\exists \bar{a}, \bar{b} \in (R/I) \backslash \{0\}$ such that $\bar{a}\bar{b} = \bar{0}$; that is to say, R/I is not a domain. $\square$

Since fields are domains . . .

III.F.7. COROLLARY. *Maximal ideals are prime.*

Turning back to the beginning of this section, note that in a sense $\mathbb{Q}$ was the subfield of $\mathbb{F}$ generated by $\mathbb{Z}$ (in the characteristic zero case). We want to generalize this.

III.F.8. PROPOSITION. *Let $\mathcal{R}$ be a subring of a field $\mathbb{F}$. Then the intersection of all subfields containing $\mathcal{R}$ (the "subfield generated by $\mathcal{R}$") is*

$$\{\alpha\beta^{-1} \mid \alpha \in \mathcal{R},\ \beta \in \mathcal{R}\backslash\{0\}\} \cong \frac{\mathcal{R} \times \mathcal{R}\backslash\{0\}}{\equiv}, \tag{III.F.9}$$

where $(\alpha, \beta) \equiv (\gamma, \delta) \iff \alpha\beta^{-1} = \gamma\delta^{-1}$ in $\mathbb{F}$ $\iff$ $\alpha\delta = \beta\gamma$ in $\mathcal{R}$.

PROOF. We only need to check that III.F.9 is a subfield, since any field containing $\mathcal{R}$ clearly contains it. The only remotely nontrivial check is closure under addition: $\alpha\beta^{-1} + \gamma\delta^{-1} = \alpha\delta\beta^{-1}\delta^{-1} + \beta\gamma\beta^{-1}\delta^{-1} = (\alpha\delta + \beta\gamma)(\beta\delta)^{-1}$. $\square$

Going further, we can perform this construction without a "reference field" $\mathbb{F}$.

III.F.10. THEOREM. *Any commutative domain R can be embedded in a field.*

PROOF. Again we define an equivalence relation

$$(a,b) \sim (c,d) \quad \overset{\text{def.}}{\iff} \quad ad = bc \tag{III.F.11}$$

on $R \times R\backslash\{0\}$. This is

- reflexive: $ab = ba$
- symmetric: $ad = bc \iff cb = da$
- transitive: $ad = bc$ and $cf = de \implies adf = bcf = bde \implies d(af - be) = 0$ (and $d \neq 0$) $\implies af = be$ (since R is a domain).

Define (as a set)

$$\mathfrak{F}\{R\} := \frac{R \times R\backslash\{0\}}{\sim},$$

with $1_{\mathfrak{F}\{R\}} := \overline{(1,1)}$, $0_{\mathfrak{F}\{R\}} := \overline{(0,1)}$,

$$\overline{(a,b)} \cdot \overline{(c,d)} := \overline{(ac,bd)}, \quad \text{and} \quad \overline{(a,b)} + \overline{(c,d)} := \overline{(ad+bc,ad)}.$$

These operations are well-defined: for instance, if $(a,b) \sim (a',b')$, i.e. $ab' = ba'$, then $(a'd + b'c)bd = b'd(ad+bc)$ hence

$$\overline{(a',b')} + \overline{(c,d)} = \overline{(a'd+b'c,b'd)} = \overline{(ad+bc,bd)}.$$

(The other checks in this vein are left to you.)

Next, we check the properties of a ring: we have

- $\overline{(0,1)} + \overline{(a,b)} = \overline{(0b+1a,1b)} = \overline{(a,b)}$
- $\overline{(1,1)} \cdot \overline{(a,b)} = \overline{(a,b)}$
- $\overline{(-a,b)} + \overline{(a,b)} = \overline{(-ab+ba,b^2)} = \overline{(0,b^2)} = \overline{(0,1)}$
- $\overline{(a,b)} \cdot (\overline{(c,d)} + \overline{(e,f)}) = \overline{(a(cf+de),b(df))} = \overline{(acbf+abde,b^2df)}$ $= \overline{(ac,bd)} + \overline{(ae,bf)}$

and the other distributive and associative laws can also be checked. Moreover, if $\overline{(a,b)} \neq 0_{\mathfrak{F}\{R\}}$ (i.e. $a \neq 0$), then

$$\overline{(b,a)} \cdot \overline{(a,b)} = \overline{(ba,ab)} = \overline{(1,1)} = 1_{\mathfrak{F}\{R\}}$$

and so $\mathfrak{F}\{R\}$ is a field.

Finally, we need to show that

$$\begin{aligned} \phi \colon R &\to \mathfrak{F}\{R\} \\ r &\mapsto \overline{(r,1)} \end{aligned}$$

is an injective homomorphism, embedding R as a subring. We have $\phi(1) = 1_{\mathbb{F}\{R\}}$, $\phi(r_1 + r_2) = \overline{(r_1 + r_2, 1)} = \overline{(r_1,1)} + \overline{(r_2,1)} = \phi(r_1) + \phi(r_2)$, etc.; and if $\phi(r) = 0_{\mathfrak{F}\{R\}}$ then $\overline{(r,1)} = \overline{(0,1)} \implies r \cdot 1 = 1 \cdot 0 \implies r = 0$, done. $\square$

III.F.12. DEFINITION. $\mathfrak{F}\{R\}$ is called the **field of fractions** of R.

We can put together III.F.8 and III.F.10 as follows:

III.F.13. PROPOSITION. *Given a commutative domain R, any injective ring homomorphism $\varphi \colon R \hookrightarrow \mathbb{F}$ factors through R's field of fractions*

$$\begin{tikzcd} R \arrow[rr, hook, "\varphi"] \arrow[dr, hook, "\phi"'] & & \mathbb{F}\,; \\ & \mathfrak{F}\{R\} \arrow[ur, hook, "\tilde{\varphi}"'] & \end{tikzcd}$$

and if the only subfield of $\mathbb{F}$ containing $\varphi(R)$ is $\mathbb{F}$ itself, then $\mathbb{F} \cong \mathfrak{F}\{R\}$.

PROOF. The second statement is obvious (since $\mathfrak{F}\{R\} \cong \tilde{\varphi}(\mathfrak{F}\{R\})$ is a subfield containing $\varphi(R)$), so what we need to do is check that

$$\tilde{\varphi}(\overline{(a,b)}) := \varphi(a)\varphi(b)^{-1}$$

is well-defined and a homomorphism (easy and left to you), as well as injective: if $\varphi(a)\varphi(b)^{-1} = 0$ then $\varphi(a) = 0 \implies a = 0 \implies \overline{(a,b)} = \overline{(0,1)}$. $\square$

III.F.14. EXAMPLES. (i) Consider $\varphi\colon \mathbb{Z}[\sqrt{d}] \hookrightarrow \mathbb{Q}[\sqrt{d}]$. Any subfield containing its image contains $(\forall a,b,c \in \mathbb{Z},\ c \neq 0)$ c^{-1} and $(a+b\sqrt{d})c^{-1}$ hence $\mathbb{Q}[\sqrt{d}]$. So $\mathbb{Q}[\sqrt{d}] \cong \mathfrak{F}\{\mathbb{Z}[\sqrt{d}]\}$.

(ii) Let $\mathbb{F}$ be a field, $R = \mathbb{F}[x]$. Then $\mathbb{F}(x) := \mathfrak{F}\{\mathbb{F}[x]\}$ consists of "rational functions" in x.

Associated to the field of fractions is a different notion of ideal. (We continue to take R a commutative domain.)

III.F.15. DEFINITION. (i) A **fractional ideal** of R is a subset $J \subset \mathfrak{F}\{R\}$ of the form $fI := f \cdot I = \{fa \mid a \in I\}$ for some $f \in \mathfrak{F}\{R\}$ and ideal $I \subset R$.

(ii) J is **principal** if I is.

(iii) J is **invertible** if there exists a fractional ideal J' with $JJ' = R$.

Principal fractional ideals are invertible since they are of the form $fR \subset \mathfrak{F}\{R\}$ and we have $fR \cdot f^{-1}R = R^2 = R$. Denote by

- $\mathcal{J}(R)$:= the set of fractional ideals
- $\mathcal{J}(R)^*$:= the set of invertible fractional ideals
- $\mathcal{PJ}(R)$:= the set of principal fractional ideals.

Under the obvious multiplication $fI \cdot f'I' = ff'II'$, $\mathcal{J}(R)^*$ forms an abelian group with identity element R, and (normal) subgroup $\mathcal{PJ}(R)$.

III.F.16. DEFINITION. $\mathscr{C}\ell(R) := \mathcal{J}(R)^*/\mathcal{PJ}(R)$ is the **ideal class group**.

We shall discuss its relation to uniqueness of factorization later.

III.F.17. EXAMPLE. Assume $d \in \mathbb{Z}\backslash\{0\}$ squarefree, with $d \underset{(4)}{\not\equiv} 1$, and consider an ideal of the form $I = (\alpha, \beta)$ inside $R = \mathbb{Z}[\sqrt{d}]$. Writing $\widetilde{m+n\sqrt{d}} := m - n\sqrt{d}$, and $\tilde{I} = (\tilde{\alpha}, \tilde{\beta})$, we will compute $I\tilde{I}$.

But first, we need a little "lemma". Suppose that $a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ solves an integer equation of the form $x^2 + Bx + C = 0$. Then

$$a + b\sqrt{d} = \tfrac{-B \pm \sqrt{B^2 - 4C}}{2} \implies B^2 - 4C = A^2 d \text{ for some } A \in \mathbb{Z}.$$

Since $d \underset{(4)}{\not\equiv} 1$, we get $B^2 - 4C \underset{(4)}{\not\equiv} 1$, which forces B (and thus A) to be even, whence $a, b \in \mathbb{Z}$. What this shows is that an element of $\mathbb{Q}[\sqrt{d}]$ belongs to R if it solves a monic integral quadratic equation.

Returning to the computation: as the norm map sends $R \to \mathbb{Z}$, and $\alpha, \beta \in R$, we have

$$I\tilde{I} = (\alpha\tilde{\alpha},\, \beta\tilde{\beta},\, \alpha\tilde{\beta},\, \beta\tilde{\alpha}) = (\underbrace{\alpha\tilde{\alpha},\, \beta\tilde{\beta},\, \alpha\tilde{\beta} + \beta\tilde{\alpha}}_{\text{in } \mathbb{Z}, \text{ with gcd } =: g},\, \beta\tilde{\alpha}) = (g,\, \beta\tilde{\alpha}).$$

Since $\frac{\beta\tilde{\alpha}}{g}$ is a root of

$$(x - \tfrac{\beta\tilde{\alpha}}{g})(x - \tfrac{\alpha\tilde{\beta}}{g}) = x^2 - \underbrace{(\tfrac{\beta\tilde{\alpha} + \alpha\tilde{\beta}}{g})}_{\in\mathbb{Z}}x + \underbrace{\tfrac{\alpha\tilde{\alpha}}{g} \cdot \tfrac{\beta\tilde{\beta}}{g}}_{\in\mathbb{Z}},$$

our "lemma" tells us that $\frac{\beta\tilde{\alpha}}{g} \in R$ hence $g \mid \beta\tilde{\alpha}$ in R. So we conclude that

$$I\tilde{I} = (g)\,,$$

a very useful result called **Hurwitz's Theorem** (which also works for $d \underset{(4)}{\equiv} 1$ and $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$). I say it is useful because it comes with the presciption for how to calculate g, as the gcd of three integers.

What this all means for fractional ideals is that

$$\tfrac{1}{g}\tilde{I} \text{ furnishes an inverse to } I.$$

This gives examples of non-principal ideals that have an (explicit!) inverse. Later we will see that all nontrivial ideals in R are invertible.

Our discussion of fraction fields is not complete without mentioning one case where there is nothing to do, a result sometimes called "Wedderburn's little theorem":

III.F.18. THEOREM (Wedderburn). *Let R be a commutative domain, with $|R| < \infty$. Then R is a field.*

PROOF. Let $r \in R\backslash\{0\}$. Since R is finite, there exists a power $n \in \mathbb{Z}_{>0}$ such that $r^n \in \{1, r, \ldots, r^{n-1}\}$, say $r^n = r^k$. Then $r^k(r^{n-k} - 1) = 0$, and since R is a domain, we have $r^{n-k} = 1$ and r is a unit. So $R\backslash\{0\} = R^*$ and R is a field. $\square$