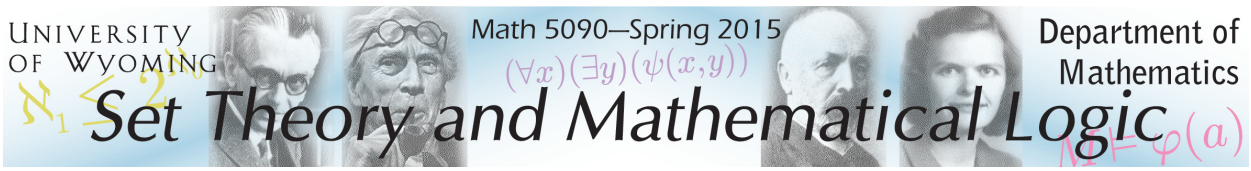

Applications of Logic to Field Theory

The following supplement to Cameron's book is taken largely from *Model Theory: An Introduction* by David Marker.

The language of fields (as the language of rings) includes two constants, 0 and 1; and two binary operations, '+' and '×'. In a nutshell, a field is a commutative ring with multiplicative identity, in which every nonzero element has a multiplicative inverse. Field theory may be defined using first order axioms as follows:

$(\forall x)(\forall y)(x + y = y + x)$
$(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$
$(\forall x)(x + 0 = x)$
$(\forall x)(\exists y)(x + y = 0)$
$(\forall x)(\forall y)(x \times y = y \times x)$
$(\forall x)(\forall y)(\forall z)((x \times y) \times z = x \times (y \times z))$
$(\forall x)(\forall y)(\forall z)((x \times (y + z)) = (x \times y) + (x \times z)))$
$(\forall x)(1 \times x = x)$
$(\neg(0 = 1))$
$(\forall x)((x = 0) \vee ((\exists y)(x \times y = 1)))$

It would be better to write $\alpha(x, y)$ and $\mu(x, y)$ as formal symbols in place of '$x + y$' and '$x \times y$' respectively, to maintain a distinction between the syntax and semantics of field theory; but in the interest of readability, we use '+' and '×', and proceed with caution. We further abbreviate $x \times y$ as xy; also abbreviate xx, $(xx)x$, $((xx)x)x$, ... as x^2, x^3, x^4, etc. (although exponentiation is not strictly part of our formal language). The commutative and associative laws, together with the usual convention that multiplication takes precedence over addition, allows us to suppress many of the usual parentheses; thus for example, $x^2 + a_1x + a_0$ is an abbreviation for $((x \times x) + (a_1 \times x)) + a_0$. From the axioms, we may prove that $0x = 0$ for all x, so there is no need to add an axiom stating this.

A field F is *algebraically closed* if every monic polynomial in a single indeterminate, having coefficients in F, has a zero (i.e. root) in F. The theory of algebraically closed fields is axiomatized using the list of ten field theory axioms above, together with the infinite list of axioms

$(\forall a_0)(\exists x)(x + a_0 = 0)$

$(\forall a_0)(\forall a_1)(\exists x)(x^2 + a_1x + a_0 = 0)$
$(\forall a_0)(\forall a_1)(\forall a_2)(\exists x)(x^3 + a_2x^2 + a_1x + a_0 = 0)$
$(\forall a_0)(\forall a_1)(\forall a_2)(\forall a_3)(\exists x)(x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0)$
etc. ...

By the Fundamental Theorem of Algebra, the field $\mathbb{C}$ of complex numbers is algebraically closed. More generally, start with any field F, and let $\overline{F}$ be the set of all roots of polynomials of the form $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_i \in F$ and $n \geqslant 0$. (These roots exist in some extension of F; we won't worry about the details here.) Then $\overline{F}$ is a field. It is the smallest algebraically closed field containing F, and so is called the *algebraic closure of* F. For example, the algebraic closure of $\mathbb{R}$ is $\overline{\mathbb{R}} = \mathbb{C}$. If F is countable (i.e. finite or countably infinite), then there are only countably many polynomials over F, so the field $\overline{F}$ is countably infinite. In particular, the subfield $\overline{\mathbb{Q}} \subset \mathbb{C}$ is algebraically closed with $|\overline{\mathbb{Q}}| = \aleph_0$. Since $|\mathbb{C}| = 2^{\aleph_0}$, the fields $\overline{\mathbb{Q}}$ and $\mathbb{C}$ are not isomorphic.

Let F be a field. If there exists a positive integer n such that

$$\underbrace{1 + 1 + \cdots + 1}_{n} = 0$$

in F, then the smallest such n is the *characteristic* of F. (If no such n exists, then we say that the characteristic of F is zero.) If F has characteristic $n > 0$, then it is easy to see that the characteristic of F is prime. (For example, if $1 + 1 + 1 + 1 + 1 + 1 = 0$ then $(1 + 1)(1 + 1 + 1) = 0$ so either $1 + 1 = 0$ or $1 + 1 + 1 = 0$.) If p is prime, then the integers mod p form a field $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ forms a field of characteristic p. The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\overline{\mathbb{Q}}$ have characteristic 0. The algebraic closure $\overline{\mathbb{F}_p}$ is algebraically closed of characteristic p. Note that in a field of prime characteristic p,

$$\underbrace{x + x + \cdots + x}_{p} = (\underbrace{1 + 1 + \cdots + 1}_{p})x = 0x = 0$$

for all x.

The theory of algebraically closed fields of characteristic p has a countable set of first order axioms ACF$\cup\{\psi_p\}$ where ACF consists of the axioms of field theory plus the axioms for 'algebraically closed'; and ψ_p is the statement

$$(\underbrace{1 + 1 + \cdots + 1}_{p} = 0).$$

The theory of algebraically closed fields of characteristic 0 has a countable set of first order axioms ACF $\cup\, \Psi_0$ where

$$\Psi_0 = \{(\neg\psi_2), (\neg\psi_3), (\neg\psi_5), (\neg\psi_7), (\neg\psi_{11}), \ldots\}.$$

The following categoricity theorem (see Marker) will not be required here.

Theorem. ACF$\cup\Psi_0$ *is uncountably categorical. That is, if* κ *is uncountable, then any two algebraically closed fields of characteristic zero and cardinality* κ *are isomorphic. Similarly, for each prime* p, ACF $\cup \{\psi_p\}$ *is uncountably categorical.*

Thus, for example, $\mathbb{C}$ is the unique (up to isomorphism) algebraically closed field of characteristic zero having cardinality $2^{\aleph_0}$. To see that ACF $\cup\, \Psi_0$ is not countably categorical, note that $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}(x)}$ are nonisomorphic countable algebraically closed fields of characteristic zero. Here $\mathbb{Q}(x)$ is the field consisting of all rational functions in x with rational coefficients, i.e. the set of all expressions $f(x)/g(x)$ where $f(x)$ and $g(x)$ are polynomials with rational coefficients, and $g(x)$ has at least one nonzero coefficient. Recall that $\overline{\mathbb{Q}(x)}$ is the algebraic closure of $\mathbb{Q}(x)$.

Let us briefly review some notation. If M is a structure, then $M \vDash \phi$ says that the statement ϕ is true in M. If Σ is a set of sentences, then $\Sigma \vDash \phi$ says that ϕ is true in *every* model of Σ, whereas $\Sigma \vdash \phi$ says that ϕ is provable from Σ. By the Soundness and Completeness Theorem for First Order Logic, the latter two conditions are equivalent: $\Sigma \vDash \phi$ iff $\Sigma \vdash \phi$.

Let ϕ be a statement in the language of fields. Then

$$\mathbb{C} \vDash \phi \quad \text{iff} \quad \text{ACF} \cup \Psi_0 \vDash \phi \quad \text{iff} \quad \text{ACF} \cup \Psi_0 \vdash \phi.$$

That is, ϕ holds in $\mathbb{C}$, iff ϕ holds in every algebraically closed field of characteristic zero, iff ϕ is provable from the axioms ACF $\cup\, \Psi_0$. Similar statements hold for each prime p:

$$\overline{\mathbb{F}_p} \vDash \phi \quad \text{iff} \quad \text{ACF} \cup \{\psi_p\} \vDash \phi \quad \text{iff} \quad \text{ACF} \cup \{\psi_p\} \vdash \phi.$$

That is, ϕ holds in $\overline{\mathbb{F}_p}$, iff ϕ holds in every algebraically closed field of characteristic p, iff ϕ is provable from the axioms ACF $\cup \{\psi_p\}$. See Marker's book for details and proofs. The connection between the characteristic zero case and the case of positive characteristic, is provided by the following.

Theorem (Lefschetz Principle). *Let* ϕ *be a statement in the language of fields. Then* ACF $\cup\, \Psi_0 \vdash \phi$ *iff* ACF $\cup \{\psi_q\} \vdash \phi$ *for all sufficiently large primes* q.

Proof. Suppose ACF $\cup\, \Psi_0 \vdash \phi$, and consider a proof of ϕ from ACF $\cup\, \Psi_0$ = ACF $\cup$ $\{(\neg\psi_2), (\neg\psi_3), (\neg\psi_5), \ldots\}$. Only finitely many of the statements $(\neg\psi_p)$ are used in such a proof; so there exists a positive integer N such that ACF $\cup \{(\neg\psi_p) : p < N\} \vdash \phi$. For all primes p, q satisfying $p < N \leqslant q$, we have $\psi_q \vdash (\neg\psi_p)$ and so

$$\text{ACF} \cup \{\psi_q\} \vdash \phi.$$

Conversely, suppose $\mathrm{ACF} \cup \{\psi_q\} \vdash \phi$ for all primes $q \geqslant N$. Suppose further that

$$\mathrm{ACF} \cup \Psi_0 \nvdash \phi\,;$$

we seek a contradiction. By the remarks above, ϕ does not hold in $\mathbb{C}$, so $(\neg\phi)$ holds in $\mathbb{C}$, which means that $(\neg\phi)$ is provable from

$$\mathrm{ACF} \cup \Psi_0 = \mathrm{ACF} \cup \{(\neg\psi_2), (\neg\psi_3), (\neg\psi_5), \ldots\}.$$

A proof of ϕ from $\mathrm{ACF} \cup \{(\neg\psi_2), (\neg\psi_3), (\neg\psi_5), \ldots\}$ uses only finitely many of the axioms $(\neg\psi_p)$, so there exists N such that

$$\mathrm{ACF} \cup \{(\neg\psi_p) \,:\, p < N\} \vdash \phi.$$

For any primes p, q satisfying $p < N \leqslant q$, we have $\psi_q \vdash (\neg\psi_p)$, and so $\mathrm{ACF} \cup \{\psi_q\} \vdash \phi$. $\square$

We have the following remarkable application, first proved using mathematical logic (although an analytic proof was later found by Rudin). A function $f : \mathbb{C}^n \to \mathbb{C}^n$ is a *polynomial map* if it is expressible as an n-tuple of polynomials in n variables with complex coefficients, i.e.

$$f(z_1, z_2, \ldots, z_n) = (f_1(z_1, \ldots, z_n),\, f_2(z_1, \ldots, z_n),\, \ldots,\, f_n(z_1, \ldots, z_n))$$

where each $f_i(z_1, \ldots, z_n)$ is a polynomial in $z_1, z_2, \ldots, z_n$ with complex coefficients.

Theorem (Ax, 1968; Grothendieck, 1966**).** *If a polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is one-to-one, then f is onto.*

Proof. Suppose that, to the contrary, a polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is one-to-one but not onto; we will obtain a contradiction. Here n is fixed. We will illustrate the case $n = 2$; for any larger fixed values of n, the proof is similar. We have $f(z, w) = (f_1(z, w), f_2(z, w))$ where each f_i is a polynomial of degree at most d, say. Again we will illustrate here the case $d = 2$, although the same idea works for each fixed positive value of d. In the special case under consideration,

$$f_1(z, w) = az^2 + bzw + cw^2 + dz + ew + g$$
$$f_2(z, w) = hz^2 + izw + jw^2 + kz + \ell w + m$$

for some constants $a, b, \ldots, m \in \mathbb{C}$. Consider the following statement ϕ in the language of fields:

$$
\begin{aligned}
&(\exists a)(\exists b)\cdots(\exists m) \\
&\quad \left.\begin{aligned}
&(((\forall z_1)(\forall w_1)(\forall z_2)(\forall w_2) \\
&(((az_1^2{+}bz_1w_1{+}cw_1^2{+}dz_1{+}ew_1{+}g = az_2^2{+}bz_2w_2{+}cw_2^2{+}dz_2{+}ew_2{+}g) \\
&\quad \wedge (hz_1^2{+}iz_1w_1{+}jw_1^2{+}kz_1{+}\ell w_1{+}m = hz_2^2{+}iz_2w_2{+}jw_2^2{+}kz_2{+}\ell w_2{+}m)) \\
&\rightarrow ((z_1 = z_2) \wedge (w_1 = w_2)))
\end{aligned}\right\} \text{“}f\text{ is one-to-one”} \\
&\wedge \\
&\quad \left.\begin{aligned}
&(\exists u_1)(\exists u_2)(\forall z)(\forall w) \\
&\quad (\neg((az^2{+}bzw{+}cw^2{+}dz{+}ew{+}g = u_1) \\
&\quad \wedge (hz^2{+}izw{+}jw^2{+}kz{+}\ell w{+}m = u_2)))
\end{aligned}\right\} \text{“}f\text{ is not onto”}
\end{aligned}
$$

By hypothesis, ϕ holds in $\mathbb{C}$, so $\mathrm{ACF} \cup \Psi_0 \vdash \phi$. By the Lefschetz Principle, for all sufficiently large primes q, we have $\mathrm{ACF} \cup \{\psi_q\} \vdash \phi$, and so ϕ holds in $\overline{\mathbb{F}_q}$. Let $a, b, \ldots, m \in \overline{\mathbb{F}_q}$ such that the polynomial map $f : \overline{\mathbb{F}_q}^2 \rightarrow \overline{\mathbb{F}_q}^2$, as above, is one-to-one but not onto. Also let $u_1, u_2 \in \overline{\mathbb{F}_q}$, as above, such that (u_1, u_2) is not in the image of f. All values $a, b, \ldots, m, u_1, u_2 \in \overline{\mathbb{F}_q}$ are roots of polynomials with coefficients in $\mathbb{F}_q$ and so lie in some finite extension $\mathbb{F}_{q^r} \supseteq \mathbb{F}_q$ where $r \geqslant 1$. Restricting f to the finite field $\mathbb{F}_{q^r}$ gives a map $\mathbb{F}_{q^r}^2 \rightarrow \mathbb{F}_{q^r}^2$ which is one-to-one but not onto. This is impossible for a map from a finite set (of cardinality q^{2r}) to itself. This gives the required contradiction. □

A more elementary application of the Lefschetz Principle is the following. Consider a large linear system with integer coefficients:

$$Ax = b$$

where A is an $m \times n$ integer matrix, $b \in \mathbb{Z}^m$. We ask whether there is a solution $x \in \mathbb{Q}^n$. In certain cases, solving this system over $\mathbb{Q}$ can lead to exceedingly ugly fractions; the intermediate steps in such a computation may actually place such demands on our computational resources as to exceed the available memory. In such cases, we may instead look for a ‘mod p’ solution $x \in \mathbb{F}_p^n$ for a suitable large prime p, where arbitrary precision arithmetic is no longer required. The connection between solvability over $\mathbb{Q}$, and solvability over $\mathbb{F}_p$, is expressed as follows.

Theorem. *Let A be an $m \times n$ integer matrix, and let $b \in \mathbb{Z}^m$.*

(i) If the system $Ax = b$ has a solution $x \in \mathbb{Q}^n$, then the system has a 'mod p' solution $x \in \mathbb{F}_p^n$ for every sufficiently large prime p.

(ii) If the system $Ax = b$ has no solution $x \in \mathbb{Q}^n$, then for every sufficiently large prime p, there is no 'mod p' solution $x \in \mathbb{F}_p^n$.

This result asserts that it is impossible for the system $Ax = b$ to be solvable for an infinite set of primes p, and also insolvable for a (complementary) infinite set of primes p. By taking the prime p large enough, checking for solutions over $\mathbb{F}_p$ (which is easier, since only bounded precision arithmetic is required) allows us to determine whether the solution is solvable over $\mathbb{Q}$. A proof of this result is not hard, using available tools from linear algebra (using, for example, the theory of Smith normal forms). However, a quick proof follows from the Lefschetz Principle. Namely, if the system has a solution in characteristic zero, then for all sufficiently large p, it has a solution over $\overline{\mathbb{F}_p}$; and from this it is easy to see that there is a solution over $\mathbb{F}_p$. The converse follows similarly.