A Note on the Artin–Schreier Theorem

August 9, 2010

The Ultrafilter Theorem has many equivalent forms over the basic axioms ZF for set theory. One of the most useful and versatile is the *Propositional Completeness Theorem*:

(PCT) Every consistent propositional theory is satisfiable.

A lesser known equivalent is the *Artin–Schreier Theorem*.

(AST) Every formally real field is orderable.

The equivalence of the Artin–Schreier Theorem with the Ultrafilter Theorem was established by Berr, Delon, and Schmid in 1999. [1] The proof given there is somewhat involved algebraically. The goal of this note is to give an elementary proof of the following.

Theorem. $\mathsf{ZF} \vdash \mathsf{PCT} \leftrightarrow \mathsf{AST}$.

We will prove each direction separately. Our proof of the forward implication goes through even without the Axiom of Infinity. Our proof of the reverse implication implicitly uses the existence of the real numbers, but we doubt that this assumption is necessary.

$\mathsf{ZF} \vdash \mathsf{PCT} \to \mathsf{AST}$

We will prove that a slightly stronger form of AST follows from PCT. There are two equivalent definition of formally real fields: the first says that -1 is not a sum of squares, the second says that a sum of nonzero squares is nonzero. The latter has the advantage of being meaningful over any ring and

this is the one we will use in what follows. Assuming PCT, we will show that a (commutative) ring is orderable if and only if it is a formally real domain.

Let R be a commutative ring. We associate with each $x \in R$ a propositional variable P_x, which is intended to mean "x is positive." The theory $\mathcal{T}_R$ then consists of the addition and multiplication schemes

$$P_x \wedge P_y \to P_{x+y} \quad \text{and} \quad P_x \wedge P_y \to P_{xy}$$

for $x, y \in R$, together with the zero axiom and the dichotomy scheme

$$\neg P_0, \quad \text{and} \quad P_x \vee P_{-x}$$

for nonzero $x \in R$.

Proposition 1.

(a) *The theory $\mathcal{T}_R$ is consistent if and only if R is a formally real domain.*

(b) *The theory $\mathcal{T}_R$ is satisfiable if and only if R is an orderable domain.*

Since the axioms of $\mathcal{T}_R$ reflect exactly the axioms of order, part (b) is obvious. For part (a), the forward direction is also easy to see. Indeed, if x, y and $z_1, \ldots, z_n$ are nonzero elements of R then $\mathcal{T}_R$ proves that

$$P_{xy} \vee P_{-xy} \quad \text{and} \quad P_{z_1^2+\cdots+z_n^2},$$

which implies that xy and $z_1^2 + \cdots + z_n^2$ are both nonzero, assuming $\mathcal{T}_R$ is consistent.

For the reverse direction of (a), suppose that R is a formally real domain. We will show that $\mathcal{T}_R$ is consistent.

Note that any variable assignment such that $P_0 = \bot$ automatically satisfies all instances of the multiplication scheme which involve P_0, since these are all of the form

$$P_x \wedge P_0 \to P_0 \quad \text{or} \quad P_0 \wedge P_y \to P_0$$

owing to the fact that R is an integral domain. Also, the only nontrivial instances of the addition scheme which involve P_0 are those of the form

$$P_x \wedge P_{-x} \to P_0,$$

which are equivalent to $\neg P_x \vee \neg P_{-x}$ when $P_0 = \bot$. Therefore, any truth assignment such that $P_0 = \bot$ and $P_{-x} = \neg P_x$ for $x \neq 0$ automatically satisfies all axioms of $\mathcal{T}_R$ except for instances of the addition and multiplication schemes that do not involve P_0.

Let $x_1, \ldots, x_n$ be nonzero elements of R such that $x_i \pm x_j \neq 0$ when $i \neq j$. We will find a partial variable assignment that satisfies all axioms of $\mathcal{T}_R$ that mention only propositional variables from $P_0, P_{\pm x_1}, \ldots, P_{\pm x_n}$. For simplicity, we will call such axioms "relevant."

Associate each signature $\sigma \in \{\pm 1\}^n$ to the partial truth assignment where $P_{\sigma_i x_i} = \top$, $P_{-\sigma_i x_i} = \bot$, and $P_0 = \bot$. By the above observations, this partial truth assignment satisfies all relevant axioms, with the possible exception of some instances of the addition and multiplication schemes that do not involve P_0. Note that:

- $\sigma_i x_i + \sigma_j x_j + \sigma_k x_k = 0$ iff this truth assignment fails to satisfy the relevant axiom $P_{\sigma_i x_i} \wedge P_{\sigma_j x_j} \to P_{\sigma_i x_i + \sigma_j x_j}$, and
- $\sigma_i x_i \sigma_j x_j + \sigma_k x_k = 0$ iff this truth assignment fails to satisfy the relevant axiom $P_{\sigma_i x_i} \wedge P_{\sigma_j x_j} \to P_{\sigma_i x_i \sigma_j x_j}$.

Since R is an integral domain, the truth assignment associated to σ satisfies all relevant axioms if and only if $p_\sigma q_\sigma \neq 0$, where

$$p_\sigma = \prod_{1 \leq i,j,k \leq n} (\sigma_i x_i + \sigma_j x_j + \sigma_k x_k),$$
$$q_\sigma = \prod_{1 \leq i,j,k \leq n} (\sigma_i x_i \sigma_j x_j + \sigma_k x_k).$$

If we expand the sum

$$\sum_{\sigma \in \{\pm 1\}^k} p_\sigma q_\sigma$$

into monomials of the form

$$(\sigma_1 x_1)^{e_1} \cdots (\sigma_k x_k)^{e_k}$$

we see that only those with all even exponents $e_1, \ldots, e_k$ do not cancel out. Since R is formally real, the remaining terms form a nonempty sum of nonzero squares whose value is therefore nonzero. It follows that $p_\sigma q_\sigma \neq 0$ for some $\sigma \in \{\pm 1\}^n$, which gives a variable assignment satisfying all relevant axioms.

$\mathsf{ZF} \vdash \mathsf{AST} \to \mathsf{PCT}$

We will use $N(X, Y, Z)$ to denote the propositional connective

$$(X \vee Y \vee Z) \wedge (\neg X \vee \neg Y \vee \neg Z).$$

In other words, $N(X, Y, Z)$ holds iff X, Y, Z are not all equal. In 1978, Schaefer observed that this simple connective is suprisingly expressive. [2]

Lemma 2. *Every propositional theory $\mathcal{T}$ is equisatisfiable with a propositional theory $\mathcal{S}$ whose axioms are all of the form $N(X, Y, Z)$, where X, Y, Z are either propositional variables or the propositional constant $\top$.*

Proof. We may suppose that all of the axioms of the theory $\mathcal{T}$ are disjunctions of exactly three propositional literals. For each propositional variable X, introduce a fresh variable symbol X' with the axiom $N(X', X, X)$ (which is equivalent to $X' \leftrightarrow \neg X$). Let $\mathcal{T}'$ be obtained from $\mathcal{T}$ by replacing every occurrence of the negative literal $\neg X$ by the variable X'. Every axiom $X \vee Y \vee Z$ in $\mathcal{T}'$ is equisatisfiable with

$$N(X, Y, U), N(Y, Z, V), N(U, V, \top),$$

where U, V are fresh variable symbols. Thus $\mathcal{T}$ is equisatisfiable with the theory $\mathcal{S}$ whose axioms consist of $N(X', X, X)$ for every propositional variable X, together with $N(X, Y, U), N(Y, Z, V), N(U, V, \top)$ for every axiom $X \vee Y \vee Z$ of $\mathcal{T}'$. □

The reason that we want a theory of this form is that the connective $N(X, Y, Z)$ can be emulated by the order properties of the simple polynomial

$$xy + yz + zx$$

as explained by the following lemma.

Lemma 3. *Let R be an ordered integral domain and let $x, y, z \in R$ be such that $1 \leq x^2, y^2, z^2 \leq 2$.*

- *If $x, y, z > 0$ or $x, y, z < 0$ then $3 \leq xy + yz + zx$.*
- *Otherwise, $xy + yz + zx \leq 0$.*

Proof. The first statement is clear. For the second statement, suppose that $x < 0 < y$. (All other cases are symmetric.) If $z > 0$, then

$$xy + yz + zx = x(y + z) + yx \leq -2 + 2 = 0.$$

If $z < 0$, then

$$xy + yz + xz = y(x + z) + xz \leq -2 + 2 = 0. \qquad \square$$

Let $\mathcal{S}$ be a propositional theory as in Lemma 2. We will successively construct three fields $K \subseteq L \subseteq M$. The first two will be unconditionaly formally real. The last will satisfy the following proposition.

Proposition 4.

(a) *If the theory $\mathcal{S}$ is consistent then the field M is formally real.*

(b) *If the field M is orderable then the theory $\mathcal{S}$ is satisfiable.*

This is not as sharp an equivalence as Proposition 1, but it is enough to give the required implication. While we will not prove this here, we know that the converse of (a) is true. The converse of (b) is consistently false in ZF, but it is true assuming the Ordering Principle.

For each propositional variable X associate a variable symbol x and let K be the field of rational functions in these variables with coefficients in $\mathbb{Q}$. Let L be the field obtained by adjoining the square roots

$$\sqrt{x^2 - 1} \quad \text{and} \quad \sqrt{2 - x^2},$$

where x ranges over the variable symbols. This is not the field that will help us deduce the PCT from the AST, but let us pause for a moment and convince ourselves that L is formally real by finding embeddings of finitely generated subfields of L into the real numbers.

Let $K_0 = \mathbb{Q}(x_1, \ldots, x_n) \subseteq K$ and let

$$L_0 = K_0 \left[\sqrt{x_1^2 - 1}, \sqrt{2 - x_1^2}, \ldots, \sqrt{x_n^2 - 1}, \sqrt{2 - x_n^2} \right] \subseteq L.$$

In order to faithfully embed K_0 into the real numbers, it suffices to assign algebraically independent transcendental values to each of $x_1, \ldots, x_n$. Such values can be found in any open interval, in particular we can find suitable $\alpha_1, \ldots, \alpha_n \in (1, \sqrt{2})$. Since $1 < \alpha_i^2 < 2$ we can then extend this embedding to

all of L_0. There are 4^n different ways to do this, but we may as well pick the one where $\sqrt{x_i^2 - 1}$ and $\sqrt{2 - x_i^2}$ get mapped to the positive square roots of $\alpha_i^2 - 1$ and $2 - \alpha_i^2$, respectively. There was no reason to pick positive $\alpha_1, \ldots, \alpha_n$, we can replace any number of the α_i by their negatives to obtain the same effect. Given a signature $\sigma \in \{\pm 1\}^n$, let L_0^σ denote the copy of L_0 in $\mathbb{R}$ resulting from the alternate assignment $x_i \mapsto \sigma_i \alpha_i$ (but the same choce of square roots). Abusing notation, we will also use σ for the isomorphism from L_0 to L_0^σ.

The field M we will be interested in is obtained from L by adjoining a square root

$$\sqrt{-xy - yz - zx}$$

for each axiom $N(X, Y, Z)$ of $\mathcal{S}$. Here and elsewhere, we understand that $x = 1$ when X is the constant $\top$, and similarly for y, z and Y, Z. For example, if $N(\top, \top, \top)$ were an axiom of $\mathcal{S}$, M would contain a sqaure root $\sqrt{-3}$. Such M would not be formally real, but this is fine since $N(\top, \top, \top)$ is simply false.

Proof of (a). Let $X_1, \ldots, X_n$ be propositional variables and let $\mathcal{S}_0$ be the finite collection of axioms of $\mathcal{S}$ that only involve variables from $X_1, \ldots, X_n$ or the constant $X_0 = \top$. Let K_0 and L_0 be as above for the associated variables $x_1, \ldots, x_n$. Let $M_0 \subseteq M$ be similarly obtained by adjoining square roots to $-x_i x_j - x_j x_k - x_k x_i$ for each axiom $N(X_i, X_j, X_k)$, where we understand that $x_0 = 1.0$

Since $\mathcal{S}$ is consistent, we can find a variable assignment for $X_1, \ldots, X_n$ that satisfies the finite set $\mathcal{S}_0$. Let $\sigma \in \{\pm 1\}^n$ be such that $\sigma_i = 1$ iff $X_i = \top$ in this assignment. Let L_0 and L_0^σ be as discussed above. By Lemma 3, for each axiom $N(X_i, X_j, X_k) \in \mathcal{S}_0$ we must have

$$\alpha_i \alpha_j + \alpha_j \alpha_k + \alpha_k \alpha_i \leq 0$$

(where we understand that $\alpha_0 = 1$). Therefore, we can extend the embedding σ of L_0 into L_0^σ by assigning

$$\sqrt{-x_i x_j - x_j x_k - x_k x_i}$$

to the positive (say) square root

$$\sqrt{-\alpha_i \alpha_j - \alpha_j \alpha_k - \alpha_k \alpha_i}.$$

This results in a subfield M_0^σ of the reals which is isomorphic to M_0.

It follows immediately that M_0 is formally real. Since every finitely generated subfield of M is contained in some such M_0, it follows that M is formally real. □

Proof of (b). If $<$ is an ordering of M, then $1 \leq x^2 \leq 2$ for every variable x and $xy + yz + zx \leq 0$ for each axiom $N(X, Y, Z)$ of $\mathcal{S}$. It follows from Lemma 3 that the variable assignment

$$X = \begin{cases} \top & \text{when } x > 0 \\ \bot & \text{when } x < 0 \end{cases}$$

satisfies $\mathcal{S}$. □

References

[1] R. Berr, F. Delon, and J. Schmid, *Ordered fields and the ultrafilter theorem*, Fund. Math. **159** (1999), no. 3, 231–241. MR MR1680634 (2000e:03138)

[2] Thomas J. Schaefer, *The complexity of satisfiability problems*, Conference Record of the Tenth Annual ACM Symposium on Theory of Computing (San Diego, Calif., 1978), ACM, New York, 1978, pp. 216–226. MR MR521057 (80d:68058)