# A modified version of the proof of Bourbaki–Witt theorem in Lang's Algebra

I give below a slightly cleaned-up version of the proof of Bourbaki–Witt theorem in Lang's Algebra [1], Appendix 2, pages 881–884. What I mean by 'cleaning-up' is that I eliminated some unnecessary invocations of EM (the law of the excluded middle), simply by reformulating the definition of the 'extreme point', so that it is now expressed (without negation) using the relations "$\leqslant$" and "$=$" instead of the relations "$<$"and "$\leqslant$". This streamlines the proof somewhat; among other things, it does away with three impossible situations. Moreover, the two passages where EM is used in a more substantial way (they are marked by "★ . . . ★") now clearly stand out.

A remark about terminology. Lang says that an endomap $f$ on a poset $P$ is 'increasing' if $x \leqslant f(x)$ for all $x \in P$; in this text such an endomap is called ascending, while an order-preserving endomap is called increasing.

**Theorem 1.** (Bourbaki–Witt) *Let $P$ be a chain complete poset, and let $f$ be an ascending endomap on $P$. Then for every $a \in P$ there exists a fixed point of $f$ above $a$.*

*Proof.* Let $a \in P$, and let $\mathcal{A}$ be the set of all subsets of $P$ that contain $a$, are closed under $f$, and are closed under joins (taken in $P$) of nonempty chains. Since $\mathcal{A}$ is defined by closure rules on the set $P$, it is a closure system on the complete lattice $\mathscr{P}P$ (ordered by inclusion), and the intersection $M = \bigcap \mathcal{A}$ is the least element of $\mathcal{A}$.

We will show that $M$ is a chain. Then it will follow that $b = \bigvee M \in M$ because $M$ is closed under joins of nonempty chains, then $f(b) \in M$ because $M$ is closed under $f$, whence $f(b) \leqslant b$, and finally $f(b) = b$ because $f$ is ascending.

First observe that $a$ is the least element of $M$: since the subset $\{x \in M \mid a \leqslant x\}$ of $M$ obeys all required closure rules, it is the whole $M$.

Let $c \in M$. We shall say that $c$ is an **extreme point** of $M$ if whenever $x \in M$ and $x \leqslant c$, then $f(x) \leqslant c$ or $x = c$.[1] For each extreme point $c \in M$ we put

$$M_c := \{x \in M \mid x \leqslant c \text{ or } f(c) \leqslant x\};$$

note that always $a \in M_c$.

◇ *Let $c$ be an extreme point of $M$. Then $M_c = M$.*

We will show that $M_c \in \mathcal{A}$; since $M_c \subseteq M$, it will follow that $M_c = M$.

We have already noticed that $a \in M_c$.

To show that $M_c$ is closed under $f$, take any $x \in M_c$; we have $f(x) \in M$, and $x \leqslant c$ or $f(c) \leqslant x$. If $x \leqslant c$, then $f(x) \leqslant c$ or $x = c$; in both cases $f(x) \in M_c$. If $f(c) \leqslant x$, then $f(c) \leqslant x \leqslant f(x)$, hence $f(x) \in M_c$.

Let $T$ be a nonempty chain in $M_c$; we have $b = \bigvee T \in M$. ★If all elements of $T$ are below $c$, then $b \leqslant c$ and hence $b \in M_c$; otherwise, some element of $T$ is above $f(c)$, hence $f(c) \leqslant b$ and so again $b \in M_c$.★

[1] In Lang's Algebra [1] an extreme point of $M$ is defined as an element $c$ of $M$ such that for every $x \in M$, $x < c$ implies $f(x) \leqslant c$. In classical logic the two definitions are equivalent, while in intuitionistic logic they are not. In intutionistic logic our definition is more demanding; that is, an extreme point by our definition is also an extreme point as defined by Lang.

◇ *Every element of $M$ is an extreme point.*

Let $E$ be the set of all extreme points of $M$. We will prove that $E \in \mathcal{A}$.

First, $a \in E$: if $x \in M$ and $x \leqslant a$, then $x = a$ because $a$ is the least element of $M$.

To prove $E$ closed under $f$, take any $c \in E$; we will show that $f(c) \in E$. Let $x \in M$, $x \leqslant f(c)$; we must show that $f(x) \leqslant f(c)$ or $x = f(c)$. Since $x \in M = M_c$, we have $x \leqslant c$ or $f(c) \leqslant x$. If $x \leqslant c$, then $f(x) \leqslant c$ or $x = c$, thus $f(x) \leqslant c \leqslant f(c)$ or $f(x) = f(c)$; if $f(c) \leqslant x$, then $x = f(c)$.

Let $T$ be a nonempty chain in $E$, and let $b = \bigvee T \in M$; we will show that $b \in E$. Let $x \in M$, $x \leqslant b$; we must show that $f(x) \leqslant b$ or $x = b$. Since $x \in M = M_c$ for all $c \in T$, we have $x \leqslant c$ or $f(c) \leqslant x$ for every $c \in T$. ★There are two possibilities: one is that $f(c) \leqslant x$ for all $c \in T$, the other one is that $x \leqslant d$ for some $d \in T$.★ If the former is the case, then $c \leqslant f(c) \leqslant x$ for all $c \in T$, thus $x$ is an upper bound of $T$, hence $b \leqslant x$, and we have $x = b$. In the other case, since $d$ is an extreme point, we have $f(x) \leqslant d \leqslant b$ or $x = d$; in the latter case, since $b \in M = M_d$, we have $b \leqslant d = x$ hence $x = b$, or $f(x) = f(d) \leqslant b$.

◇ *$M$ is a chain.*

Let $x$, $y \in M$. Since $x \in M = E$ and $y \in M = M_x$, we have $y \leqslant x$ or $x \leqslant f(x) \leqslant y$. □

Both uses of EM in the proof are of the following form:

$$\text{if } T \subseteq A \cup B, \text{ then } T \subseteq A \text{ or } T \cap B \text{ is nonempty,}$$

where a set $X$ is said to be nonempty if it has at least one element, i.e. if $\exists x\colon x \in X$ is true. With the first use of EM we have $A = \{z \in M \mid z \leqslant c\}$ and $B = \{z \in M \mid f(c) \leqslant z\}$, while with the second use we have $A = \{z \in M \mid f(z) \leqslant x\}$ and $B = \{z \in M \mid x \leqslant z\}$. Note that the weaker implication

$$\text{if } T \subseteq A \cup B, \text{ then not not } (T \subseteq A \text{ or } T \cap B \text{ is nonempty})$$

is true, but useless for the purpose of the proof.

Sets that are 'nonempty' as defined above are in intuitionistic set theory said to be 'inhabited'; we will keep calling them 'nonempty'. We must distinguish between nonempty sets and sets that are not empty. A set $O$ is said to be empty if it does not have any elements, i.e. if $\neg(\exists x\colon x \in O)$ is true, or equivalently, if $\forall x\colon \neg(x \in O)$ is true; thus $O$ is empty if and only if it is not nonempty. Since a set is uniquely determined by its elements, and an empty set has none, there is only one empty set $\varnothing$. Now, we say that a set $X$ is not empty if it is not the empty set, that is, if it is not true that there is no element in $X$; formally, $X$ is not empty if $\neg\neg(\exists x\colon x \in X)$ is true. Thus "$X$ is not empty" is equivalent to "not not ($X$ is nonempty)".

Once the proof of Theorem 1 had established that $M$ is a chain, it was through. The chain $M$ is in fact well-ordered, but this was not needed to prove the existence of a fixed point. However, we want to verify that $M$ is well-ordered, so let us prove it; the proof below uses EM.

◇ *$M$ is well-ordered.*

Let $S$ be a subset of $M$ without a least element. Put $V = \{v \in M \mid \exists s \in S\colon s \leqslant v\}$; if $v \in V$, $w \in M$, and $v \leqslant w$, then $w \in V$.

The set $V$ does not have a least element. Indeed, suppose that $u$ is a least element of $V$. There exists $r \in S$ that is below $u$. Then, for any $s \in S$ we have $s \in V$ and hence $r \leqslant u \leqslant s$, which means that $r$ is a least element of $S$, a contradiction.

Now let $V'$ be the complement of $V$ in $M$, that is, $V' = \{x \in M \mid \neg(x \in V)\}$. If $x \in V'$ and $y \in M$, $y \leqslant x$, then $y \in V'$, since $y \in V$ implies $x \in V$, a contradiction.

We will show that $V' \in \mathcal{A}$, and consequetly, that $V' = M$.

First, were $a \in V$, then $a$ would be a least element of $V$, a contradiction; thus $\neg(a \in V)$ and hence $a \in V'$.

Next, let $x \in V'$. Assume that $f(x) \in V$. Take any $v \in V$. Since $v \in M = M_x$, we have $v \leqslant x$ or $f(x) \leqslant v$; but $\neg(v \leqslant x)$ because $v \in V$ and $x \in V'$ and $v \leqslant x$ lead to contradiction, so we have $f(x) \leqslant v$.[2] It follows that $f(x)$ is a least element of $V$, a contradiction which proves that $f(x) \in V'$.

Finally, let $T$ be a nonempty chain in $V'$, and suppose that $b = \bigvee T \in V$. Let $t \in T$ and $v \in V$. Since $M$ is a chain, we have $t \leqslant v$ or $v \leqslant t$; but $\neg(v \leqslant t)$, so we have $t \leqslant v$. Thus $v$ is an upper bound of $T$, hence $b \leqslant v$. It follows that $b$ is a least element of $V$, a contradiction which proves that $b \in V'$.

We see that $V' = M$, thus $V = \varnothing$ and hence $S = \varnothing$.

We have shown that the only subset of $M$ that has no least element is the empty set. ★ Therefore, every nonempty subset of $M$ has a least element. ★

The conclusion ★ . . . ★ uses EM. We have proved, intuitionistically (while using the results $E = M$, and $M_x = M$ for every $x \in E = M$, which were obtained using EM), that

$$\text{if } S \subseteq M \text{ has no least element, then } S \text{ is empty,}$$

which, still intuitionistically, implies that

$$\text{if } S \subseteq M \text{ is not empty, then not } (S \text{ has no least element}),$$

or formally, that

$$(S \subseteq M) \wedge \neg(S = \varnothing) \implies \neg\neg\big(\exists r \in S\colon (\forall s \in S\colon r \leqslant s)\big)$$

is true. Since "$S$ is nonempty" implies "$S$ is not empty", the following is also true:

$$(S \subseteq M) \wedge (\exists s\colon s \in S) \implies \neg\neg\big(\exists r \in S\colon (\forall s \in S\colon r \leqslant s)\big)\,.$$

If we admit EM, then $\neg\neg p \iff p$ for every proposition $p$, and we have the desired result.

In the course of proving that $M$ is well-ordered we have used *reductio ad absurdum* (RA) quite a few times; does not this mean that we have used EM all over the proof, not only in its final conclusion? Funnily enough, all uses of RA in the proof are intuitionistically correct. RA is a legitimate reasoning tool of intuitionistic logic. Suppose that a proposition $p$ describes a 'contextual situation' in which a proposition $q$ makes sense; then, if we show that $p \wedge q$ implies $\bot$ (i.e. that $p \wedge q$ leads to contradiction), we can conclude that $p$ implies $\neg q$; the converse also holds: if $p$ implies $\neg q$, then $p \wedge q$ implies $\bot$. However, there are incorrect uses of RA which involve EM; namely, if we know that $p \wedge \neg q$ implies $\bot$, and then conclude that $p$ implies $q$, we have used EM, since what we can really conclude, intuitionistically, is that $p$ implies $\neg\neg q$, which is weaker; if we then read $\neg\neg q$ as $q$, we have used EM.

[2] We can eliminate an impossible case in intitionistic logic, because for any propositions $p$ and $q$, the chain of equivalences and an implication $\neg p \wedge (p \vee q) \iff (\neg p \wedge p) \vee (\neg p \wedge q) \iff \bot \vee (\neg p \wedge q) \iff \neg p \wedge q \implies q$ is valid in intuitionistic logic.

## References

[1] Serge Lang, *Algebra*, Revised Third Edition. Springer-Verlag, New York, 2002.