Counterexamples in Algebra

August 3, 2015

We use k, F, K to denote the fields, and R to denote the rings. Denote by $\mathbb{Z}$ the ring of rational integers, $\mathbb{Q}$ the field of rational numbers, $\mathbb{R}$ the field of real numbers, and $\mathbb{C}$ the field of complex numbers. Denote by $\mathbb{A}$ the ring of algebraic integers.

1 Groups

A Noncyclic Group of Order 4. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
A Presentation Gives a Trivial Group. $\langle x, y, z | xyx^{-1}y^{-1} = y,\ yzy^{-1}z^{-1} = z,\ zxz^{-1}x^{-1} = x\rangle$.
Two Nonisomorphic Groups with the Same Character Table. D_4 and Q_8.
A Nonabelian p-Group.

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a, b \in \mathbb{Z}/(p^2),\ a \equiv 1 \bmod p \right\}.$$

This is a nonabelian group of order p^3.

Another example of a nonzbelian group of order p^3 is

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} | a, b, c \in \mathbb{Z}/(p) \right\}.$$

In fact, these are the only nonabelian groups of order p^3. On the other hand, every group of order p^2 is abelian.
Solvable Groups. Every finite group of order < 60, every Abelian group, any p-group.
Finite Simple Groups. Cyclic groups $\mathbb{Z}/p\mathbb{Z}$, alternating groups A_n with $n \geq 5$, groups of Lie type, sporadic groups.
Group Homomorphisms of Additive Group of $\mathbb{R}$.

There are linear functions $f(x) = ax$. There are also nonlinear ones, consider a projection onto one basis element of the vector space $\mathbb{R}$ over $\mathbb{Q}$.
A Paradoxical Decomposition of a Group.

Let F_2 be the free group with two generators a, b. Consider $S(a)$, $S(a^{-1})$, $S(b)$, and $S(b^{-1})$ be the set of elements starting with a, a^{-1}, b, and b^{-1} respectively. Then we have

$$F_2 = \langle e\rangle \cup S(a) \cup S(a^{-1}) \cup S(b) \cup S(b^{-1}).$$

We have also

$$F_2 = aS(a^{-1}) \cup S(a),$$

and

$$F_2 = bS(b^{-1}) \cup S(b).$$

These decompositions are used in the proof of Banach-Tarski Theorem.

2 Rings

A Commutative Ring with Identity that is Not an Integral Domain. $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$.
A Commutative Ring without Identity. $2\mathbb{Z}$, $\{0, 2\}$ in $\mathbb{Z}/4\mathbb{Z}$.
A Noncommutative Ring without Identity. $M_2(2\mathbb{Z})$.
A Noncommutative Division Ring with Identity. The real quarternion $\mathbb{H}$.
A Ring with Cyclic Multiplicative Group.

$R = \mathbb{Z}/n\mathbb{Z}$ with $n = 2, 4, p^k, 2p^k$. Any finite fields. Also $\mathbb{Z}$ has units $\{\pm 1\}$ which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and is cyclic.

A Subring that is Not an Ideal. $\mathbb{Z} \subset \mathbb{Q}$.
An Order of a Ring is Larger than its Characteristic. Any $\mathrm{GF}(p^n)$ for $n \geq 2$.
A Prime Ideal that is Not a Maximal Ideal.

Let $R = \mathbb{Z}[x]$. The ideal $P = (x)$ is a prime ideal since $R/P \cong \mathbb{Z}$ is an integral domain. Since $\mathbb{Z}$ is not a field, P is not a maximal ideal. In PID, every prime ideal is maximal and vice versa. In fact, if R is an integral domain that is not a field, for example $\mathbb{Z}$, then (0) is a prime ideal that is not maximal.

A Homomorphic Image Need Not be an Ideal. $\mathbb{Z} \subset \mathbb{Q}$.
An Additive Group Homomorphism that is Not a Ring Homomorphism.

The derivative map $D : \mathbb{R}[x] \to \mathbb{R}[x]$. We have $D(f + g) = D(f) + D(g)$ but $D(fg) = gD(f) + fD(g)$.

A Multiplicative Group Homomorphism that is Not a Ring Homomorphism.

Let $f : \mathbb{R} \to \mathbb{R}$ be $f(x) = x^2$.

The Unique Ring Homomorphism from $\mathbb{R}$ to $\mathbb{R}$. The identity.
A Commutative Ring with Infinitely Many Units. $\mathbb{Z}[\sqrt{2}]$.
A Noncommutative Ring with Infinitely Many Units. $M_2(\mathbb{Z})$.
A Non-Dedekind Domain.

The ring $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{A} \cap \mathbb{Q}(\sqrt{-3}) = \mathbb{Z}[(1 + \sqrt{-3})/2]$. This is not Dedekind since it is not integrally closed.

A Dedekind Domain which is Not a UFD. $\mathbb{Z}[\sqrt{-5}]$. This is a ring of integers in $\mathbb{Q}(\sqrt{-5})$. We have the non-unique factorization $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
A UFD which is Not Dedekind. $k[x, y]$. The Krull-dimension of this ring is 2.
A UFD which is Not a PID. $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is UFD, $\mathbb{Z}[x]$ is a UFD. However, this is not PID because $(x, 2)$ is not principal.
A PID which is Not a ED.

The ring of integers in $\mathbb{Q}(\sqrt{-19})$. This is $\mathbb{Z}[(1 + \sqrt{-19})/2]$.

A Ring R such that $\mathbf{R \cong R \times R}$.

Let $R = \prod_{i=1}^{\infty} \mathbb{Z}$. Then $R \cong R \times R$ by the following isomorphism:

$$f : R \to R \times R$$

defined by

$$f(x_1, x_2, \cdots) = ((x_1, x_3, \cdots), (x_2, x_4, \cdots)).$$

A Commutative Ring with 4 Elements that is Not Isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The matrices $\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$ over $\mathbb{Z}/2\mathbb{Z} = \mathrm{GF}(2)$. This is isomorphic to $\mathrm{GF}(2)[x]/(x^2)$ by

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto 1 + (x^2),$$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \mapsto x + (x^2).$$

This is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$ since the characteristic is not 4. This is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since this ring has two solutions in $x^2 = 0$.

Another example is the 4-element subring of $\mathbb{Z}/16\mathbb{Z}$, where the multiplication of any pair is zero.

A Commutative Ring with Identity that the Converse of CRT Holds.

Let R be a commutative ring with identity. The converse of CRT is:

If I, J are ideals with $I + J \neq R$, then

$$R/I \cap J \ncong R/I \times R/J.$$

$\mathbb{Z}$, $F[x]$ where F is a field. Further, any Dedekind Domain.

A Commutative Ring with Identity that the Converse of CRT does Not Hold.

$R = \prod_{i=1}^{\infty} \mathbb{Z}$, and $I = J = (0)$. Then $I + J \neq R$ and $R/I \cap J \cong R/I \times R/J$.

A Commutative Ring with Identity that is Noetherian but not Artinian. $\mathbb{Z}$, $k[x]$.

A Commutative Ring with Identity that is neither Noetherian nor Artinian.

$\mathbb{A}$ the ring of algebraic integers, $k[x_1, x_2, \cdots]$ the ring of polynomials in infinitely many variables.

A Local Noetherian Ring. $k[[x]]$ the formal power series ring over a field k.

This has a unique maximal ideal (x), and it is Noetherian by Hilbert's Basis Theorem. Furthermore, this is a DVR.

Integral Domains A, B which Contains a Field F but $\mathbf{A \otimes_F B}$ is Not an Integral Domain.

Let $A = B = \mathrm{GF}(p)(X)$ and $F = \mathrm{GF}(p)(X^p)$. Then A and B are integral domains containing F, but

$$X \otimes 1 - 1 \otimes X \in A \otimes_F B$$

is a nonzero element in $A \otimes_F B$ satisfying

$$(X \otimes 1 - 1 \otimes X)^p = X^p \otimes 1 - 1 \otimes X^p = 0.$$

Hence, $A \otimes_F B$ is not an integral domain.

A Group Ring which is Not Semisimple.

$k[x]/(x^p - 1)$ with $k = \mathrm{GF}(p)$. This is a group ring kG with a cyclic group G or order p. This is not semisimple by Maschke's theorem. This is a local ring with maximal ideal $I := \ker(kG \xrightarrow{\epsilon} k) = \mathrm{Rad}(kG)$.

3 Fields

An Algebraically Closed Field of Finite Characteristic. $\overline{\mathrm{GF}(p)}$.

An Infinite Field of Finite Characteristic. $\overline{\mathrm{GF}(p)}$, $\mathrm{GF}(p)(x)$ the field of rational functions over $\mathrm{GF}(p)$.

A Real Transcendental Extension. $\mathbb{Q} \subset \mathbb{Q}(\pi)$.

A Real Field which is Not Totally Real. $\mathbb{Q}(2^{\frac{1}{3}})$.

A Totally Real Field. $\mathbb{Q}(\sqrt{2})$.

A Normal Extension of a Normal Extension may Not be Normal. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{\sqrt{2}})$.

An Algebraic Extension of Infinite Degree. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \cdots)$ over $\mathbb{Q}$, $\overline{\mathbb{Q}}$ over $\mathbb{Q}$, $\overline{\mathrm{GF}(p)}$ over $\mathrm{GF}(p)$.

A Nontrivial Finite Extension that is Isomorphic to the Ground Field.

Let $F = \mathbb{Q}(x)$ and $k = \mathbb{Q}(\sqrt{x})$. Then k is a degree-2 extension of F. However, they are isomorphic.

A Finite Extension which Contains Infinitely Many Subextensions.

Let p be a prime. Let $F = \mathrm{GF}(p)(x, y)$ and $k = \mathrm{GF}(p)(x^{\frac{1}{p}}, y^{\frac{1}{p}})$. For any $f(y) \in \mathrm{GF}(p)(y)$,

$$K = F(x^{\frac{1}{p}} f(y) + y^{\frac{1}{p}})$$

is a nontrivial subextension of k.

An Irreducible Polynomial $\mathbf{f \in \mathbb{Q}[x]}$ with Reducible $\mathbf{\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]}$ for Every p.

Let $x^4 + 1 \in \mathbb{Q}[x]$. If $p = 2$, then $x^4 + 1 = (x^2 + 1)^2$. If $p \neq 2$, then $x^4 + 1 | x^8 - 1 | x^{p^2 - 1} - 1$.

4 Modules

A Noetherian Module which is Not Artinian. $\mathbb{Z}$-module $\mathbb{Z}$.
An Artinian Module which is Not Noetherian. $\mathbb{Z}$-module $M = \cup_{i=1}^{\infty}(p^{-i}\mathbb{Z}/\mathbb{Z})$.
A Free Module with Infinite Basis. $\mathbb{Q}$-vector space $\mathbb{R}$.
An Injective Module which is Not Torsion-Free. $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$
A Torsion-Free Module which is Not Flat.

Let $R = k[x, y]$ and $I = (x, y)$. Then I is a torsion-free R-module. This is not flat because

$$I \otimes I \to I \otimes R$$

is not injective. In fact, $0 \neq x \otimes y - y \otimes x \in \operatorname{Ker}(I \otimes I \to I \otimes R)$.
A Projective Module which is Not Free.

Let $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and consider $\mathbb{Z}/2\mathbb{Z} \times (0)$ a submodule of R-module R. This is projective since it is a direct summand of free module but it is too small to be free.
A Flat Module which is Not Projective. $\mathbb{Z}$-module $\mathbb{Q}$.
A Flat Module which is Neither Projective Nor Injective.

The $\mathbb{Z}$-module $\mathbb{Q} \oplus \mathbb{Z}$. This is flat because it is a direct sum of flat modules. This is not projective because of $\mathbb{Q}$, not injective because of $\mathbb{Z}$.
A Semisimple Module which is Not Simple. $\mathbb{C}S_3 \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.
A Module which is Faithful and Flat, but Not Faithfully Flat. $\mathbb{Z}$-module $\mathbb{Q}$.