(*January 22, 2024*)

The Small Wedderburn Theorem

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[0.1] Claim: Finite rings R (with 1, but not necessarily commutative) without (proper) zero-divisors are *division rings*, in the sense that every non-zero element has a multiplicative inverse.

Proof: In general, in a ring R without proper zero-divisors, the maps $x \to xb$ and $x \to bx$, for fixed non-zero b, are *injective*: indeed, if $xb = x'b$, then $(x - x')b = 0$, so $x - x' = 0$. The same argument applies on the other side.

In particular, for R *finite*, injectivity implies surjectivity.

Thus, for given $0 \neq b \in R$, there is $x \in R$ such that $bx = 1$. In fact, since $b(xb) = (bx)b = 1 \cdot b = b \cdot 1$, by cancellation we have also $xb = 1$, so x is a two-sided inverse to b. ///

In fact, the same proof mechanism shows:

[0.2] Claim: Finite rings R (not necessarily commutative) *not necessarily* with a 1, *without* proper zero-divisors, *do* have a unit 1.

Proof: Again, for $b \neq 0$, multiplication operators $x \to xb$ and $x \to bx$ are injective, due to absence of zero divisors. Finiteness of R implies surjectivity of these maps. Thus, given b, there is x such that $bx = b$. Then $b(xb) = (bx)b = b \cdot b$. By cancelling, $xb = b$, so x also acts as a unit (for b) on the other side.

For any other $c \in R$, similarly, $(cx)b = c(xb) = c \cdot b$, so $cx = c$. A similar argument shows that $xc = x$. Thus, x is a unit in R, in the sense of behaving like 1. ///

[0.3] Remark: The truth of the latter claim is interesting, but, perhaps, of minor interest. Still, it gives:

[0.4] Example: For integer $m > 1$ and prime p not dividing m, the subring R of $\mathbb{Z}/mp$, consisting of multiples of m, can be verified to satisfy the hypothesis of this last claim, so has a unit, even though it does not contain 1 mod mp. However, as soon as we see this, it's maybe obvious via Sun-Ze's theorem: there is x mod mp with $x = 0$ mod m and $x = 1$ mod p, which is the unit in R.

[0.5] Theorem: (Wedderburn 1905, Dickson, et al) Finite rings R without proper zero divisors are *commutative*, that is, are *fields*.

Proof: Using the orbit-stabilizer theorem, consider the group $R^\times$ acting on the set $R^\times$ by conjugation $x \to bxb^{-1}$. That is,

$$\#R^\times \;=\; \sum_{x_o} \frac{\#R^\times}{\#G_{x_o}}$$

where G_{x_o} is the fixer/isotropy subgroup

$$G_{x_o} \;=\; \{g \in R^\times : gx_og^{-1} = x_o\}$$

Let Z be the center of R. It is a finite commutative ring without zero-divisors, so is a finite *field*, with cardinality q for some prime power q.

Also, $R_{x_o} = G_{x_o} \cup \{0\}$ is a *subring* of R: certainly $R^\times_{x_o}$ is a *subgroup* of $R^\times$, for general reasons, and, for $a, b \in G_{x_o}$,

$$(a+b)x_o \;=\; ax_o + bx_o \;=\; x_oa + x_ob \;=\; x_o(a+b)$$

Since R_{x_o} has no zero-divisors, it is a division ring. If we want to argue by induction, then, for non-central x_o, R_{x_o} is a proper subring of R, so has lesser cardinality, so is a field. As an overfield of Z it has cardinality q^m for some m. Since R is a vectorspace over R_{x_o}, it has cardinality $(q^m)^k$ for some k. That is, $m|n$.

In fact, a basic theory of module/vectorspaces over division rings is an easy extrapolation of vectorspaces over fields, so this induction is not strictly needed.

The orbit-stabilizer identity is

$$q^n - 1 \;=\; \#R^\times \;=\; \underbrace{1 + \ldots + 1}_{q-1} + \sum_{\text{non-central}\, x_o} \frac{q^n-1}{q^m-1}$$

where the first sum is over central elements, and where $m = m_{x_o}$ depends on x_o, and $m|n$, with $m < n$ for non-central x_o.

Because $x^m - 1$ factors into cyclotomic polynomials $x^m - 1 = \prod_{d|m} \Phi_d(x)$ as polynomials *with integer coefficients*. Thus, for $m|n$ and $m < n$, the polynomial $\Phi_n(x)$ divides the polynomial $\frac{x^n-1}{x^m-1}$. Since Φ_n has integer coefficients, $q^m - 1 = \prod_{d|m} \Phi_d(q)$ as *integers*, and $\Phi_n(q)$ divides the integer $\frac{q^n-1}{q^m-1}$.

From the orbit-stabilizer relation, $\Phi_n(q)$ divides $q-1$, if R is not commutative. To see that this is impossible, use the geometry of the complex numbers. Namely,

$$\Phi_n(q) \;=\; \prod_k (q - e^{2\pi ik/n}) \qquad \text{(product over } k \text{ prime to } n)$$

The complex-geometry fact is that, for such k, $|q - e^{2\pi ik/n}| > q - 1$. Thus, the product, which is an integer, is strictly larger than $q - 1$, so cannot divide $q - 1$.

So the center of R must be all of R. ///

[0.6] Example: In a more naive context, one surely might imagine that there'd be a finite-field analogue of the Hamiltonian quaternions

$$\mathbb{H} \;=\; \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

with the coefficients in $\mathbb{F}_p$. Take $p > 2$ to avoid $-1 = +1$. Yes, such a ring exists, and for $p > 2$ is non-commutative. However, since it is non-commutative, and *finite*, it must have 0-divisors, unlike $\mathbb{H}$.
