(*September 7, 2023*)

Examples 01

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

[01.1] Let D be an integer that is not the square of an integer. Prove that there is no $\sqrt{D}$ in $\mathbb{Q}$.

[01.2] Let p be prime, $n > 1$ an integer. Show (directly) that the equation $x^n - px + p = 0$ has no rational root (where $n > 1$).

[01.3] Let p be prime, b an integer not divisible by p. Show (directly) that the equation $x^p - x + b = 0$ has no rational root.

[01.4] Let r be a positive integer, and p a prime such that $\gcd(r, p-1) = 1$. Show that every b in $\mathbb{Z}/p$ has a unique r^{th} root c, given by the formula

$$c = b^s \mathrm{mod}\, p$$

where $rs = 1 \mathrm{mod}\, (p-1)$.

[01.5] Show that $R = \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean.

[01.6] Let $f : X \to Y$ be a function from a set X to a set Y. Show that f has a left inverse if and only if it is injective. Show that f has a right inverse if and only if it is surjective. (Note where, if anywhere, the Axiom of Choice is needed.)

[01.7] Let $h : A \to B$, $g : B \to C$, $f : C \to D$. Prove the associativity

$$(f \circ g) \circ h = f \circ (g \circ h)$$

[01.8] Show that a set is infinite if and only if there is an injection of it to a proper subset of itself. Do not set this up so as to trivialize the question.

[01.9] Let G, H be finite groups with relatively prime orders. Show that any group homomorphism $f : G \to H$ is necessarily trivial (that is, sends every element of G to the identity in H.)

[01.10] Let m and n be integers. Give a formula for an isomorphism of abelian groups

$$\frac{\mathbb{Z}}{m} \oplus \frac{\mathbb{Z}}{n} \to \frac{\mathbb{Z}}{\gcd(m,n)} \oplus \frac{\mathbb{Z}}{\mathrm{lcm}(m,n)}$$

[01.11] Show that every group of order $5 \cdot 13$ is cyclic.

[01.12] Show that every group of order $5 \cdot 7^2$ is abelian.

[01.13] Exhibit a non-abelian group of order $3 \cdot 7$.

[01.14] Exhibit a non-abelian group of order $5 \cdot 19^2$.

[01.15] Show that every group of order $3 \cdot 5 \cdot 17$ is cyclic.

[01.16] Do there exist 4 primes p, q, r, s such that every group of order $pqrs$ is necessarily abelian?

[01.17] Let $R = \mathbb{Z}/13$ and $S = \mathbb{Z}/221$. Show that the map

$$f : R \to S$$

defined by $f(n) = 170 \cdot n$ is *well-defined* and is a ring homomorphism. (Observe that it does not map $1 \in R$ to $1 \in S$.)

[01.18] Let p and q be distinct prime numbers. Show directly that there is no field with pq elements.

[01.19] Find all the idempotent elements in $\mathbb{Z}/n$.

[01.20] Find all the nilpotent elements in $\mathbb{Z}/n$.

[01.21] Let $R = \mathbb{Q}[x]/(x^2 - 1)$. Find e and f in R, neither one 0, such that

$$e^2 = e \quad f^2 = f \quad ef = 0 \quad e + f = 1$$

(Such e and f are **orthogonal** idempotents.) Show that the maps $p_e(r) = re$ and $p_f(r) = rf$ are ring homomorphisms of R to itself.

[01.22] Prove that in $(\mathbb{Z}/p)[x]$ we have the factorization

$$x^p - x = \prod_{a \in \mathbb{Z}/p} (x - a)$$

[01.23] Show that $\mathbb{Z}[x]$ has non-maximal non-zero prime ideals.

[01.24] Show that $\mathbb{C}[x, y]$ has non-maximal non-zero prime ideals.

[01.25] Let $\omega = (-1 + \sqrt{-3})/2$. Prove that

$$\mathbb{Z}[\omega]/p\mathbb{Z}[\omega] \approx (\mathbb{Z}/p)[x]/(x^2 + x + 1)(\mathbb{Z}/p)[x]$$

and, as a consequence, that a prime p in $\mathbb{Z}$ is expressible as $x^2 + xy + y^2$ with integers x, y if and only if $p = 1 \bmod 3$ (apart from the single anomalous case $p = 3$).
