Math 5055: Advanced Algebra II

Assignment 2

Solutions

1. **Let $\mathbb{E}$ be the splitting field over $\mathbb{Q}$ of $(x^3-2)(x^2-3)$. Compute $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$, and write down the complete Galois correspondence: list all the subfields of $\mathbb{E}$ and all the subgroups of $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ and how they match.**

   Let us look at the two factors:

   - The splitting field of x^2-3 is $\mathbb{Q}(\sqrt{3})$, with Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \cong S_2 \cong \mathbb{Z}/2$ acting by $\sqrt{3} \mapsto -\sqrt{3}$. (We will write it as S_2 to emphasize that it is acting as the symmetric group on the two roots of x^2-3.)
   - The splitting field of x^3-2 is $\mathbb{F} := \mathbb{Q}(\sqrt[3]{2}, \zeta)$ where $\zeta = \exp(2\pi i/3) = \frac{1}{2}\big(1+\sqrt{-3}\big)$ is a root of x^2+x+1. Indeed, the roots of x^3-2 are $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$. The Galois group is $\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) = S_3$, the symmetric group on three elements (specifically: the symmetric group on the three roots of x^3-2). It can be generated by the order-2 automorphism sending $\zeta \mapsto -\zeta$ while fixing $\sqrt[3]{2}$ and the order-3 automorphism which fixes ζ but sends $\sqrt[3]{2} \mapsto \zeta\sqrt[3]{2}$.

   These two subfields intersect trivially. On the other hand, $\mathbb{E} = \mathbb{F}(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt[3]{2}, \zeta)$. This lets us quickly compute that $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = S_2$ and $\mathrm{Gal}(\mathbb{E}/\mathbb{Q}(\sqrt{3})) = S_3$. The short exact sequences $1 \to \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \to 1$ and $1 \to \mathrm{Gal}(\mathbb{E}/\mathbb{Q}(\sqrt{3})) \to \mathrm{Gal}(\mathbb{E}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \to 1$ together then imply:

$$G \cong S_2 \times S_3.$$

   The S_2 factor exchanges $\pm\sqrt{3}$ while fixing $\sqrt[3]{2}$ and ζ, whereas the S_3 factors fixes $\pm\sqrt{3}$ and permutes the three roots of x^3-2. Indeed, each SES gives a splitting of the other one. One can also see the isomorphism $G \cong S_2 \times S_3$ "directly" by inspecting the permutation action of G on the five-element set $\{\sqrt{3}, -\sqrt{3}, \sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$.

   For future reference, we will write $\sigma \in S_2 \subset G$ for the nontrivial element of the S_2 factor. We'll write $\rho \in S_3 \subset G$ for the 3-cycle $\sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \mapsto \zeta^2\sqrt[3]{2}$, and $\tau \subset G$ for the 2-cycle $\zeta\sqrt[3]{2} \leftrightarrow \zeta^2\sqrt[3]{2}$.

   We now must enumerate the subgroups $H \subset G$, and compute the fields $\mathbb{E}^H$.

   Suppose first that $H \ni \sigma$. Then, for a generic permutation $g \in S_3$, $\sigma g \in H$ if and only if $g \in H$. Thus the subgroups $H \subset G$ containing σ are precisely the groups of the form $H = S_2 \times H'$ for some subgroup $H' \subset S_3$. There are six such groups H': the trivial group (1); the whole group (S^3); three groups of order two ($\langle\tau\rangle$, $\langle\rho\tau\rangle$, and $\langle\rho^2\tau\rangle$); and one group of order three ($\langle\rho\rangle$). The corresponding fields are:

$$\mathbb{E}^{S_2\times S_3} = \mathbb{Q}, \qquad \mathbb{E}^{S_2\times 1} = \mathbb{F} = \mathbb{Q}[\sqrt[3]{2}, \zeta], \qquad \mathbb{E}^{S_2\times\langle\rho\rangle} = \mathbb{Q}[\zeta] = \mathbb{Q}[\sqrt{-3}],$$
$$\mathbb{E}^{S_2\times\langle\tau\rangle} = \mathbb{Q}[\sqrt[3]{2}], \qquad \mathbb{E}^{S_2\times\langle\rho\tau\rangle} = \mathbb{Q}[\zeta^2\sqrt[3]{2}], \qquad \mathbb{E}^{S_2\times\langle\rho^2\tau\rangle} = \mathbb{Q}[\zeta\sqrt[3]{2}].$$

Note that the three fields on the second row are isomorphic, reflecting that they correspond to conjugate groups. They are different as subfields of $\mathbb{E}$ (subgroups of G).

We must now enumerate the subgroups $H \subset G$ such that $H \not\ni \sigma$. Given such a subgroup, consider the composition $H \subset G \to S_3$, where second map is the natural projection. This composition will be an isomorphism onto its image. In other words, and such H does select a subgroup $H' \subset S_3$, and we have already enumerated those subgroups.

Going in the other direction: given a subgroup $H' \subset S_3$, which are the subgroups $H \subset G$ that live over it? The answer is the following: $H \subset G$ will map isomorphically to H' exactly when $H = \{(\phi(g), g) : g \in H'\} \subset S_2 \times S_3$ with ϕ some fixed homomorphism $H \to S_2$.

Inspecting our six subgroups H', we see that two of them (the subgroups of order one and three) have only the trivial homomorphism to S_2, and four of them (the subgroups of order two and six) have one trivial and one nontrivial homomorphism to S_2.

Using the trivial homomorphism produces the subfields

$$\mathbb{E}^{1\times S_3} = \mathbb{Q}[\sqrt{3}], \qquad \mathbb{E}^{1} = \mathbb{E}, \qquad \mathbb{E}^{\langle\rho\rangle} = \mathbb{Q}[\sqrt{-3}, \sqrt{3}] = \mathbb{Q}[\sqrt{3}, \sqrt{-1}],$$
$$\mathbb{E}^{\langle\tau\rangle} = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}], \quad \mathbb{E}^{\langle\rho\tau\rangle} = \mathbb{Q}[\zeta^2\sqrt[3]{2}, \sqrt{3}], \quad \mathbb{E}^{\langle\rho^2\tau\rangle} = \mathbb{Q}[\zeta\sqrt[3]{2}, \sqrt{3}].$$

What do the nontrivial homomorphisms look like? Consider, for example, the subgroup $H' = \langle\tau\rangle \subset S_3 = \langle\tau, \rho\rangle$, mapping nontrivially to $S_2 = \langle\sigma\rangle$. The corresponding lifted group $H \subset G$ is $\langle\sigma\tau\rangle$. The permutation $\sigma\tau$ acts as $\sqrt{3} \leftrightarrow -\sqrt{3}$ and as $\zeta \leftrightarrow \zeta^2$. Note that $\zeta = \frac{1}{2}(1 + \sqrt{-3})$, and so $\zeta \leftrightarrow \zeta^2$ is equivalent to $\sqrt{-3} \leftrightarrow -\sqrt{-3}$. Together with $\sqrt{3} \leftrightarrow -\sqrt{3}$, we learn that $\sigma\tau$ fixes $\sqrt{-1}$. It also fixes $\sqrt[3]{2}$, giving the first of the following three equalities:

$$\mathbb{E}^{\langle\sigma\tau\rangle} = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-1}], \qquad \mathbb{E}^{\langle\sigma\rho\tau\rangle} = \mathbb{Q}[\zeta^2\sqrt[3]{2}, \sqrt{-1}], \qquad \mathbb{E}^{\langle\sigma\rho^2\tau\rangle} = \mathbb{Q}[\zeta\sqrt[3]{2}, \sqrt{-1}].$$

The other two are exactly analogous.

Lastly, we have the subgroup $H' = S_3 \subset S_3$, lifted to a subgroup $H \subset G = S_2 \times S_3$ via the nontrivial homomorphism $S_3 \to S_2$. This subgroup H can be generated by ρ together with $\sigma\tau$, and:

$$\mathbb{E}^{\langle\rho,\sigma\tau\rangle} = \mathbb{Q}[\sqrt{-1}].$$

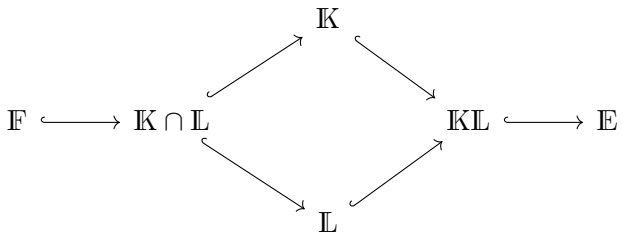
2. (a) **Let $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ be field extensions such that $\mathbb{E}$ is the splitting field over $\mathbb{F}$ of some set S of polynomials. Show that then $\mathbb{E}$ is the splitting field of some set of polynomials over $\mathbb{K}$.**

   If $\mathbb{E}$ is the splitting field over $\mathbb{F}$ of some set $S \subset \mathbb{F}[x]$, then $\mathbb{E}$ is also the splitting field over $\mathbb{K}$ of the same set S. Indeed, "$\mathbb{E}$ is the splitting field over $\mathbb{F}$ of $S \subset \mathbb{F}[x]$" means that $\mathbb{E}$ is generated by the elements of $\mathbb{F}$ together with the roots of elements of S, and all elements of S split completely over $\mathbb{E}$. But if $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$, then $\mathbb{E}$ is also generated by the elements of $\mathbb{K}$ together with the roots of S.

   (b) **Show that the converse does not hold. Specifically, find an example where $\mathbb{F} \subset \mathbb{K}$ is the splitting field of some set of polynomials, and $\mathbb{K} \subset \mathbb{E}$ is the splitting field of some set of polynomials, but $\mathbb{F} \subset \mathbb{E}$ is not a splitting field of some set of polynomials.**

   Take $\mathbb{F} = \mathbb{Q}$, $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$, and $\mathbb{E} = \mathbb{Q}[\sqrt[4]{2}]$.

3. (***Lagrange's Theorem of Natural Irrationalities***)
Suppose given a diagram of field extensions



such that $\mathbb{F} \subset \mathbb{K}$ is finite and Galois. Prove that $\mathbb{L} \subset \mathbb{KL}$ is finite and Galois, and that $\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) = \mathrm{Gal}(\mathbb{K}/(\mathbb{K} \cap \mathbb{L}))$.

Hints: $\mathbb{L} \subset \mathbb{KL}$ is the splitting field of some separable polynomial. (Why? So what?) Any $\mathbb{F}$-linear automorphism of $\mathbb{KL}$ takes $\mathbb{K}$ to itself. (Why? So what?) Compute kernel and image of $\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

Since $\mathbb{F} \subset \mathbb{K}$ is finite and Galois, the $\mathbb{K}$ is the splitting field over $\mathbb{F}$ of some separable polynomial $f(x) \in \mathbb{F}[x]$. In other words, $\mathbb{K}$ is generated by $\mathbb{F}$ together with all the roots of f. Thus $\mathbb{KL}$ is generated by $\mathbb{L}$ together with all the roots of f. In other words, $\mathbb{KL}$ is the splitting field over $\mathbb{L}$ of f. Thus $\mathbb{L} \subset \mathbb{KL}$ is finite and Galois.

Any $\mathbb{F}$-linear automorphism of $\mathbb{KL}$ will permute the roots of f, and so will take $\mathbb{K}$ back to itself. Thus we find a restriction map $\mathrm{Gal}(\mathbb{KL}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Precomposing with the inclusion $\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) \subset \mathrm{Gal}(\mathbb{KL}/\mathbb{F})$ gives a map

$$\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F}).$$

We first claim that this map is an injection. Indeed, $\mathrm{Gal}(\mathbb{KL}/\mathbb{L})$ is a subgroup of the permutation group $S_{\deg f}$ on the $\deg f$-many roots of f. But if some element of $\mathrm{Gal}(\mathbb{KL}/\mathbb{L})$ acts by some permutation of the roots of f, then its image in $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ will act by that same permutation. Said another way: $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is also a subgroup of $S_{\deg f}$, and the map $\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is an inclusion of subgroups (and hence an injection).

Let $G \subset \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ denote the image of $\mathrm{Gal}(\mathbb{KL}/\mathbb{L}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. What is the fixed subfield $\mathbb{K}^G$? In other words, suppose that $g \in \mathrm{Gal}(\mathbb{KL}/\mathbb{L})$ and $u \in \mathbb{K}$; when does $gu = u$? Well, if u is also in $\mathbb{L}$, then certainly $gu = u$, and so $\mathbb{K}^G \supset \mathbb{K} \cap \mathbb{L}$. Conversely, suppose that $u \in \mathbb{K}$ is fixed by all $g \in \mathrm{Gal}(\mathbb{KL}/\mathbb{L})$. But just since $\mathbb{K} \subset \mathbb{KL}$ and since $\mathbb{L} \subset \mathbb{KL}$ is Galois, we see that u must live in $\mathbb{L}$.

This shows that $\mathbb{K}^G = \mathbb{K} \cap \mathbb{L}$. From the Galois correspondence, we learn that $G = \mathrm{Gal}(\mathbb{K}/\mathbb{K} \cap \mathbb{L})$. But G was the isomorphic image of $\mathrm{Gal}(\mathbb{KL}/\mathbb{L})$, completing the proof.

4. (a) **Suppose that $f(x) \in \mathbb{F}_3[x]$ is a monic irreducible cubic. Show that f must divide $x^{27} - x$. Conversely, show that if f is irreducible and divides $x^{27} - x$ then f is either linear or cubic.**

Let $f(x) \in \mathbb{F}_3[x]$ be irreducible, and let α a root of f so that we can consider the field $\mathbb{K} := \mathbb{F}_3(\alpha) = \mathbb{F}_3[x]/(f(x))$. If f is cubic, then $\mathbb{K}$ is a field of order $3^3 = 27$ and hence isomorphic to $\mathbb{F}_{27}$. But every element of $\mathbb{F}_{27}$ is a root of $x^{27} - x$, so in particular α is such a root; since f is the minimal polynomial of α, we discover that f divides $x^{27} - x$. On the other hand, suppose that f divides $x^{27} - x$. Since $\mathbb{F}_{27}$ is the splitting field of $x^{27} - x$, there must be an injection of fields $\mathbb{K} \subset \mathbb{F}_{27}$. So $[\mathbb{K} : \mathbb{F}_3] = \deg f$ must divide $[\mathbb{F}_{27} : \mathbb{F}_3] = 3$, so f must be either linear or cubic.

(b) **Use part (a) to (quickly!) count the number of monic irreducible cubics over $\mathbb{F}_3$.**

From inspecting $\mathbb{F}_{27}$, we see that $x^{27} - x$ is separable, and so it has no multiplicity in its factorization. There are three linear factors, corresponding to the three elements of $\mathbb{F}_3 \subset \mathbb{F}_{27}$:

$$x^{27} - x = x(x-1)(x+1)(x^{24} + x^{22} + \cdots + x^2 + 1).$$

All that matters for us is that the last factor has degree 24. We know from part (a) that all of its irreducible factors are cubic, so it must have exactly eight irreducible factors. But every monic irreducible cubic appears among its factors. In conclusion, there are exactly eight monic irreducible cubics over $\mathbb{F}_3$.

(c) **List all the irreducible monic cubics over $\mathbb{F}_3$.**

A cubic is irreducible as soon as it has no roots. Note that $x^3 - x$ always vanishes on $\mathbb{F}_3$ whereas 1 and $x^2 + 1$ never vanish. Thus the following four cubics never vanish (and hence are irreducible):

$$x^3 - x \pm 1, \qquad x^3 - x \pm (x^2 + 1).$$

On the other hand, $x^2 - 1$ vanishes at $x = \pm 1$ whereas x^3 and $x^3 + x$ vanish only when $x = 0$. Thus the following four cubics never vanish (and hence are irreducible):

$$x^3 \pm (x^2 - 1), \qquad x^3 + x \pm (x^2 - 1).$$

We just wrote down eight distinct irreducible monic cubics. According to part (b), there are no more.

5. **(*Artin–Schreier extensions*) Let p be a positive prime and $a \neq 0 \in \mathbb{F}_p$. Let $\mathbb{E} = \mathbb{F}_p[\alpha]$ where α is a root of $x^p - x - a$ over $\mathbb{F}_p$. Show that $\alpha \mapsto \alpha + 1$ extends to an automorphism of $\mathbb{E}$. Conclude that $x^p - x - a$ is irreducible and that $\mathbb{E}$ is its splitting field. How does $\alpha \mapsto \alpha + 1$ relate to the Frobenius endomorphism of $\mathbb{E}$?**

If we knew that $f(x) := x^p - x - a$ were irreducible over $\mathbb{F}_p$, then to show that $\alpha \mapsto \alpha + 1$ extends to an automorphism of $\mathbb{E}$, it would suffice to show that $\alpha + 1$ is also a root of f. But $f(\alpha + 1) = (\alpha + 1)^p - (\alpha + 1) - a = \alpha^p + 1^p - \alpha - 1 - a = f(\alpha) = 0$. Then we would further know that $[\mathbb{E} : \mathbb{F}] = p$ and so $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is cyclic of order p generated by the Frobenius. We will henceforth write ϕ for the Frobenius automoprhism.

Let us therefore try to find some power of ϕ which sends $\alpha \mapsto \alpha + 1$. Well, $\phi(\alpha) = \alpha^p = \alpha + a$. Since $a \in \mathbb{F}_p$, $\phi(a) = a$. Then, given $b \in \mathbb{Z}$, we see that $\phi^b(\alpha) = \alpha + ba$. Since $a \in \mathbb{F}_p \cong \mathbb{Z}/(p)$ is nonzero, we can find b such that $ba = 1 \in \mathbb{F}_p$. ($b = a^{p-2}$ works.) But for this choice of b, the automorphism $\phi^b : \mathbb{E} \to \mathbb{E}$ does the trick: it acts by $\alpha \mapsto \alpha + 1$.

The Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{F}_p)$ is cyclic of order $[\mathbb{E} : \mathbb{F}] \leq p$. But it contains an automorphism, namely ϕ^b, of order greater at least p. So $[\mathbb{E} : \mathbb{F}] = p$, and so $x^p - x - a$ is irreducible over $\mathbb{F}_p$.

6. **Show that -1 has a square root in the ring $\mathbb{Z}_5 = \varprojlim \mathbb{Z}/(5^n)$ of 5-adic integers.**

Let us suppose that there is such a square root, and try to solve for it. By succeeding, we will have shown that such a square root exists.

An element of $\mathbb{Z}_5$ can be written as a sequence $\ldots b_3 b_2 b_1 b_0$ where each "digit" b_i is in $\{0, 1, 2, 3, 4\}$. Given any such sequence, we can look at the finite quotient $[b_{n-1} \ldots b_1 b_0] \in \mathbb{Z}/5^n$, where we read the finite-length sequence $b_{n-1} \ldots b_1 b_0$ as an integer written in base 5.

Said more abstractly: to write down an element of $\mathbb{Z}_5$ is to write down an element $b_0 \in \mathbb{Z}/5$, a lift of that element to an element $b_1 b_0 \in \mathbb{Z}/25$, a lift of that element to an element of $\mathbb{Z}/125$, etc.

To write down a square root of -1 in $\mathbb{Z}_5$, we first choose a square root of $-1 \equiv 4$ in $\mathbb{Z}/(5)$. There are two choices: 2 and 3. Pick either one to call b_0.

Now we must lift this choice to a square root of -1 in $\mathbb{Z}/25$. In other words, we must find a number $b_1 \in \mathbb{Z}/5$ such that $(5b_1 + b_0)^2 = -1 \in \mathbb{Z}/25$. But

$$(5b_1 + b_0)^2 \equiv 10 b_1 b_0 + b_0^2 \pmod{25}$$

and $b_0^2 = -1 + 5k$ for some k. So we need to solve

$$10 b_1 b_0 + 5k \stackrel{?}{\equiv} 0 \pmod{25}$$

or equivalently

$$2 b_1 b_0 + k \stackrel{?}{\equiv} 0 \pmod{5},$$

where b_0 and k are already chosen and we are solving for $b_1 \in \mathbb{Z}/5$. But $b_0 \neq 0$ is invertible mod 5, and 5 is odd so 2 is also invertible. Thus there is a unique solution b_1.

We now repeat the trick to see how it will generalize. We have chosen a number $5b_1 + b_0 \in \mathbb{Z}/25$ and we wish to lift it to some number $25b_2 + 5b_1 + b_0 \in \mathbb{Z}/125$ such that

$$(25b_2 + 5b_1 + b_0)^2 \stackrel{?}{\equiv} -1 \pmod{125}.$$

But the left-hand side is

$$50 b_2 b_0 + (5b_1 + b_0)^2 \pmod{125}.$$

And we've already chosen b_0, b_1 such that $(5b_1 + b_0)^2 = -1 + 25k$ for some specific $k \in \mathbb{Z}$ (whose value we will only care about mod 5). So we want to solve

$$50 b_2 b_0 + 25k \stackrel{?}{\equiv} 0 \pmod{1)25}$$

or equivalently

$$2 b_2 b_0 + k \stackrel{?}{\equiv} 0 \pmod{5},$$

where b_0 and k are already chosen and we are solving for $b_2 \in \mathbb{Z}/5$. There is a unique solution since $2b_0$ is invertible mod 5.

In general, at the nth step we want to find some $b_n \in \mathbb{Z}/5$ such that

$$\left(5^n b_n + (5^{n-1} b_{n-1} + \cdots + b_0)\right)^2 \stackrel{?}{\equiv} -1 \pmod{5^{n+1}}.$$

But the left-hand side is

$$2 \cdot 5^n \cdot b_n \cdot b_0 + (5^{n-1} b_{n-1} + \cdots + b_0)^2 \pmod{5^{n+1}},$$

and $(5^{n-1} b_{n-1} + \cdots + b_0)^2 = -1 + 5^n k$ for some k. So we are left with finding a b_n such that

$$2 \cdot 5^n \cdot b_n \cdot b_0 + 5^n k \stackrel{?}{\equiv} 0 \pmod{5^{n+1}}$$

or equivalently

$$2b_n b_0 + k \pmod 5,$$

where b_0 and k are already chosen and we are solving for b_n. Since $2b_0$ is invertible mod 5, there is a unique solution.

Remark: Exactly the same argument shows the following. Suppose p is an odd prime and that $a \in \mathbb{Z}$ is not divisible by p. Then a is a square in the ring $\mathbb{Z}_p$ of p-adic integers if and only if a is a square mod p.

The prime $p = 2$ is slightly more complicated because, in the above squarings, we kept meeting a factor of 2. A variation on the proof shows that an odd number $a \in \mathbb{Z}$ is a square in $\mathbb{Z}_2$ if and only if a is a square mod 8, which happens if and only if $a \equiv 1 \pmod 8$.

Remark: Newton observed that the binomial theorem formally gives

$$\sqrt{a+x} = \sqrt{a}\left(1 + \left(\frac{1}{2}\right)\left(\frac{x}{a}\right) + \frac{1}{2}\left(\frac{1}{2}\cdot\frac{-1}{2}\right)\left(\frac{x}{a}\right)^2 + \frac{1}{3!}\left(\frac{1}{2}\cdot\frac{-1}{2}\cdot\frac{-3}{2}\right)\left(\frac{x}{a}\right)^3 + \frac{1}{4!}\left(\frac{1}{2}\cdot\frac{-1}{2}\cdot\frac{-3}{2}\cdot\frac{-5}{2}\right)\left(\frac{x}{a}\right)^4 + \dots\right)$$

with convergence provided $|x| < |a|$. Note that the coefficient on $(\frac{x}{a})^n$ is always a rational number with denominator just some power of 2. (Indeed, the nth coefficient is $(-1)^{n-1}2^{1-2n}\frac{(2n-2)!}{n!(n-1)!}$, and the ratio of factorials is nothing but the $(n-1)$th Catalan number.) So the partial sums, where you just go up to the nth terms, make sense provided 2 is invertible.

Let us therefore work in $\mathbb{Z}_5$ and take $a = 4$ and $x = -5$. Then $\sqrt{a} = 2$ is fine, and the fractions are fine since $\frac{1}{2} = \dots 2223 \in \mathbb{Z}_5$. Does the sum converge? Yes: when you pass from the nth partial sum to the $(n+1)$th, you add a term of the form $m5^{n+1}$, where $m \in \mathbb{Q}$ has no 5s in its denominator. In other words, you are adding a term like $\dots b000\dots0$ where $n+1$ zeros. So the image of the sum in $\mathbb{Z}/5^n$ eventually stabilizes for each n, and so the full sum is valid in $\mathbb{Z}_5$.