Math 404 HW 7 Solutions

Problem 7.1

> Show that any field extension $K \subset L$ of degree 2 is normal.

Proof. Let $f \in K[x]$ be an irreducible polynomial with one root $\alpha \in L$. Then we get a chain of fields

$$K \subset K(\alpha) \subset L.$$

The first extension has degree equal to that of f. Then the multiplicative property of the degree yields that $\deg f$ divides 2. So we have that either $\deg f = 1$ or $\deg f = 2$. If f is degree 1 then it already splits in K. If f is of degree 2, then since α is a root in L we have $f = (x - \alpha)g$ for some $g \in L[x]$. Since f is degree 2, then we must have that g is of degree 1, so that f splits in L. In either case, we have that f splits in L. Since f was arbitrary, the result holds. □

Problem 7.2

Show that every element in a finite field can be written as the sum of two squares.

Proof. The result of problem 4 yields that any element in a finite field of characteristic 2 is a square. Thus we only need to consider finite fields $\mathbb{F}_q$ with q odd.

So now let $\alpha \in \mathbb{F}_q$. If $\alpha = \beta^2$, then we may write $\alpha = \beta^2 + 0^2$ as a sum of two squares. So we may assume that α is not a square itself.

We define two relevant functions, the first being$\varphi : \mathbb{F}_q \to \mathbb{F}_q^\times$ given by $\varphi(\beta) = \alpha - \beta^2$. This map has image contained in $\mathbb{F}_q^\times$ precisely because we assumed that α was not a square. The second function to consider is $\psi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ given by $\beta \mapsto \beta^2$. Our goal is to show that the images of these two functions have nonempty intersection, as if $\varphi(\beta) = \psi(\gamma)$ then we will have

$$\alpha - \beta^2 = \gamma^2 \iff \alpha = \beta^2 + \gamma^2.$$

Our strategy is to simply compute the number of elements in the image of each map, and then show that there are too many elements in the images for them to be disjoint.

For φ, we note that

$$\begin{aligned} \varphi(\beta) = \varphi(\gamma) &\iff \\ \alpha - \beta^2 = \alpha - \gamma^2 &\iff \\ \beta^2 - \gamma^2 = 0 &\iff \\ (\beta - \gamma)(\beta + \gamma) = 0 &\iff \\ \beta = \pm\gamma & \end{aligned}$$

This says that every element in the image of this map besides $\varphi(0) = \alpha$ has exactly two preimages (here we are using that the characteristic is not 2, so that $\gamma \neq -\gamma$ for $\gamma \neq 0$). That is, if $\gamma \neq \alpha$ is in the image of φ, there are exactly two elements, both nonzero, that map to it under φ. Thus, if we let $n = \#\text{image}(\varphi)$, then we have $2(n-1) = q - 1$. Rearranging yields

$$\#\text{image}(\varphi) = 1 + \frac{q-1}{2}.$$

Analogous reasoning shows that $\#\mathrm{image}(\psi) = \frac{q-1}{2}$. Suppose towards a contradiction that $\mathrm{image}(\varphi) \cap \mathrm{image}(\psi) = \emptyset$. Then we would have

$$q - 1 = \#\mathbb{F}_{||}{}^{\times} \geq \#\Big(\mathrm{image}(\psi) \cup \mathrm{image}(\varphi)\Big) = 1 + \frac{q-1}{2} + \frac{q-1}{2} = q,$$

a contradiction. Thus, we must have that $\mathrm{image}(\psi) \cap \mathrm{image}(\varphi) \neq \emptyset$, as desired.

□

Problem 7.3

Show that $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ if and only if $a|b$.

We will later have a better proof of this after we learn the fundamental theorem of Galois theory. We will learn that fields K lying in the middle of the Galois extension $\mathbb{F}_p \subset \mathbb{F}_{p^b}$ correspond bijectively with subgroups H of of $\mathrm{Gal}(\mathbb{F}_{p^b}/\mathbb{F}_p)$, with $[\mathbb{F}_{p^b} : K] = |G/H|$. Once we get this result, and we compute the Galois group of $\mathbb{F}_p \subset \mathbb{F}_{p^b}$ as $\mathbb{Z}/b\mathbb{Z}$, then this problem will follow as there is exactly one subgroup of $\mathbb{Z}/b\mathbb{Z}$ of order a for every a dividing b, and no other subgroups.

Proof. First we show that any inclusion $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ must fix $\mathbb{F}_p$. That is, we must have a commutative diagram of inclusions

$$\begin{tikzcd}
\mathbb{F}_{p^a} \arrow[r, hook] & \mathbb{F}_{p^b} \\
\mathbb{F}_p \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

To see this, note that by definition any ring homomorphism yielding an inclusion $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ must send $1 \mapsto 1$, by definition of a ring homomorphism. Since the inclusion preserves addition it must send $1 + 1 \mapsto 1 + 1$, and it must send any positive integer $n \mapsto n$ (here we mean 1 in the ring added to itself n times). Since every element of $\mathbb{F}_p$ is 1 added to itself some number of times, this shows that any inclusion $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ must preserve $\mathbb{F}_p$.

So if we have an inclusion $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$, we get a chain of inclusions $\mathbb{F}_p \subset \mathbb{F}_{p^a} \subset \mathbb{F}_{p^a}$, so the multiplicative property of the degree yields

$$b = |\mathbb{F}_{p^b} : \mathbb{F}_p| = |\mathbb{F}_{p^b} : \mathbb{F}_{p^a}| \cdot |\mathbb{F}_{p^a} : \mathbb{F}_p| = |\mathbb{F}_{p^b} : \mathbb{F}_{p^a}| \cdot a,$$

so a divides b.

All that remains to be shown is that if $a|b$, then $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$. One of the main pieces of information that we have about $\mathbb{F}_{p^a}$ is that it is the splitting field of $f(x) = x^{p^a} - x$ over $\mathbb{F}_p$. The universal property of splitting fields yields that there is an inclusion $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ if and only if f splits in $\mathbb{F}_{p^b}$. We will show this in two ways

0.1 Using a generator for the multiplicative group

Let $\alpha \in \mathbb{F}_{p^b}$ be a generator for $\mathbb{F}_{p^b}^\times$. Then $\alpha^{p^b-1} = 1$, and all the elements α^i for $0 \leq i < p^b - 1$ are distinct. Furthermoe if $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$, then we would also have a generator β for the group $\mathbb{F}_{p^a}^\times$. And we would have $\beta = \alpha^i$ for some i. Which i works?

Well we're looking for roots of unity of order $p^a - 1$. In the complex plane for instance, the primitive second root of unity can be obtained from a primitive 4th root of unity i as i^2, and in general if $n = dm$, and ζ is a primitive nth root of unity, then ζ^m is a primitive dth root of unity. Under any isomorphism $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$, this is just saying that m generates a subgroup of order d in $\mathbb{Z}/n$. This same argument would yield that $\alpha^{\frac{p^b-1}{p^a-1}}$ is a root of unity of order $p^a - 1$, provided that this fraction is actually an integer. But since $a|b$, we may write $b = ac$, a factorization into positive integers, so that this fraction equals

$$\frac{(p^a)^c - 1}{p^a - 1}.$$

The geometric series formula (I've heard some of you refer to it as the elephant teacup formula?) yields that this fraction is $\sum_{i=0}^{c-1} (p^a)^i$, which is a positive integer. Thus, we get a root of unity of order $p^a - 1$ in $\mathbb{F}_{p^b}$, and so $x^{p^a} - x$ splits there, and we get the desired field inclusion.

□

0.2 Dividing splitting polynomials

Let $f(x) = x^{p^a} - x$, and let $g(x) = x^{p^b} - x$, so that $\mathbb{F}_{p^a}$ is the splitting field of f over $\mathbb{F}_p$ and $\mathbb{F}_{p^b}$ is the splitting field of g over $\mathbb{F}_p$. If we can show that $f|g$ in $\mathbb{F}_p[x]$, then f will split in $\mathbb{F}_{p^b}[x]$. Indeed, if we have a field K and nonconstant polynomials $f, g \in K[x]$ with $f|g$ and g splitting in $K[x]$, then f also splits in $K[x]$ (prove this yourself, it's a direct consequence of $K[x]$ being a UFD).

We note that

$$\frac{x^{p^b} - x}{x^{p^a} - x} = \frac{x^{p^b-1} - 1}{x^{p^a-1} - 1}.$$

This looks similar to the geometric series formula

$$\frac{r^m - 1}{r - 1} = \sum_{i=0}^{m-1} r^i.$$

In order to apply this formula, we would want to set $r = x^{p^a - 1}$, and we would need there to exist a positive integer m so that

$$x^{p^b - 1} = r^m = x^{m(p^a - 1)}.$$

This will hold if and only we have

$$\frac{p^b - 1}{p^a - 1} \in \mathbb{Z}_{>0}.$$

But this is true, as we argued at the end of the previous method of proof. Note that this actually yields $f|g$ in $\mathbb{Z}[x]$, not just $\mathbb{F}_p[x]$.

□

What follows is some motivation for how you might have arrived at this second strategy, but is certainly not essential reading, so feel free to skip it.

The elements of $\mathbb{F}_{p^a}$ are exactly the roots of f. If we let $g(x) = x^{p^b} - x$, then the elements of $\mathbb{F}_{p^b}$ are exactly the roots of g. So if f splits over $\mathbb{F}_{p^b}$ we would have a factorization of g in $\mathbb{F}_{p^b}[x]$ as

$$\begin{aligned} g(x) &= \left(\prod_{\alpha \in \mathbb{F}_{p^a}} (x - \alpha) \right) \cdot \left(\prod_{\beta \in \mathbb{F}_{p^b} \setminus \mathbb{F}_{p^a}} (x - \beta) \right) \\ &= f(x) \cdot h(x), \end{aligned}$$

with $h(x) \in \mathbb{F}_{p^b}[x]$. I claim that actually $h(x) \in \mathbb{F}_p[x]$. To see this, let $\sigma : \mathbb{F}_{p^b} \to \mathbb{F}_{p^b}$ be the map $\alpha \mapsto \alpha^p$ of problem 4 (called the Frobenius homomorphism). We can extend σ to $\widetilde{\sigma} : \mathbb{F}_{p^b}[x] \to \mathbb{F}_{p^b}[x]$ by just applying σ to the coefficients. Then using problem 4 part (d) we have that

$$\begin{aligned} g(x) &= \widetilde{\sigma}(g(x)) \\ &= \widetilde{\sigma}(f(x)) \cdot \widetilde{\sigma}(h(x)) \\ &= f(x) \cdot \widetilde{\sigma}(h(x)). \end{aligned}$$

So then we have

$$g(x) = f(x) \cdot \widetilde{\sigma}(h(x)) = f(x) \cdot h(x).$$

So rearranging we get $f(x)(h(x) - \widetilde{\sigma}(h(x)) = 0$. Since $f(x) \neq 0$, we get that $h(x) = \widetilde{\sigma}(h(x))$. This means that all the coefficients of h are fixed by σ. So problem 4 part (d) yields that $h(x) \in \mathbb{F}_p[x]$. So you might then have tried to compute $\frac{x^{p^b}-x}{x^{p^a}-x}$. Asking a computer to do this for small values of p, a, and b with $a|b$ would yield the geometric series from the second solution above, and then you would be well on your way to getting the general formula. □

Problem 7.4

Let p be a prime and let $q = p^n$. Consider the map, (called the Frobenius homomorphism)

$$\begin{aligned} \sigma : \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto x^p. \end{aligned}$$

(a) Show that σ is a field homomorphism

(b) Show that σ is the identity on the subfield $\mathbb{F}_p \subset \mathbb{F}_q$.

(c) Show that $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is an isomorphism.

(d) Show that the set of elements fixed by σ is exactly $\mathbb{F}_p$; In other words, show that

$$\mathbb{F}_p = \{x \in \mathbb{F}_q : \sigma(x) = x\}.$$

(a) We compute first that $\sigma(1) = 1^p = 1$, so sigma sends 1 to 1. So we just need to check that σ preserves addition and multiplication. To do this, fix $x, y \in \mathbb{F}_q$. We compute

$$\sigma(xy) = (xy)^p = x^p y^p = \sigma(x)\sigma(y),$$

where the second equality uses the fact that multiplication in $\mathbb{F}_q$ is commutative. For multiplication, we have

$$\begin{aligned} \sigma(x + y) &= (x + y)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}. \end{aligned}$$

We have previously shown that all the binomial coefficients $\binom{p}{i}$ for $1 \leq i \leq p-1$ are divisible by p. Since $p = 0$ in $\mathbb{F}_q$ we have

$$\begin{aligned}\sigma(x+y) &= \binom{p}{p}x^p + \binom{p}{0}y^p \\ &= x^p + y^p \\ &= \sigma(x) + \sigma(y),\end{aligned}$$

and so σ is a homomorphism, as desired.

□

(b) Since σ is a ring homomorphism, from one ring to itself, it must fix both 0 and 1. Since σ preserves addition, it must preserve any sum $1 + 1 + \cdots + 1$. Since every element of $\mathbb{F}_p$ is the result of adding 1 to itself finitely many times, we get that σ must fix $\mathbb{F}_p$.

Alternately, we could readily compute $0^p = 0$, so we reduce to showing that σ fixes any element $x \in \mathbb{F}_p^\times$. By lagrange's theorem, the multiplicative order d of x divides $p-1$. So we may write $p - 1 = cd$, and compute

$$x^{p-1} = x^{cd} = (x^d)^c = 1^c = 1.$$

Multiplying on both sides of this equality by x yields $x^p = x$, the desired equality.

□

(c) Any ring homomorphism whose domain is a field must be injective (the kernel is an ideal, and there are only two ideals in a field, think about it). So we get that σ is injective. Alternatley we could also have noted that since $\mathbb{F}_p$ is a field, we would have $x^p = 0$ implies $x = 0$, so σ has trivial kernel.

Since σ is an injective map between two finite sets of the same size, it must be bijective, and so an isomorphism.

□

(d) We have already shown that every element in $\mathbb{F}_p$ is fixed by σ, so we must show that there are no other elements fixed by σ. Indeed, an element $\alpha \in \mathbb{F}_q$ being fixed by σ is equivalent to α being a root of $f(x) = x^p - x \in \mathbb{F}_q[x]$. We have already shown that f has p distinct roots, which are the elements of $\mathbb{F}_p$. Then we can just cite a general result that if K is a field, then a nonzero polynomial $f(x) \in K[x]$ of degree n has at most n distinct roots in K (corollary 4.17 in Hungerford). Since f can have no other roots, σ can fix no other elements, and the result holds.

□

Problem 7.5

Let $K \subset L$ be a field extension.

(a) Show that $\mathrm{Gal}(L/K)$ is a group under composition

(b) Let $\alpha \in L$ be a root of a polnomial $f(x) \in K[x]$. Then for all $\sigma \in \mathrm{Gal}(L/K)$ we have that $\sigma(\alpha)$ is also a root of f.

The short version of (a) is just that elements of the Galois group permute L while leaving K fixed and preserving arithmetic. We can do this twice and still permute L, leav K fixed, and preserve arithmetic. This gives the composition law. Associativity follows from associativity of function composition. The identity permutation certainly leaves K fixed and preserves arithmetic, so we have an identity element. And if we permute L and fix K, undoing that amounts to also permuting L and fixing K, so we get inverses, after checking that the inverse also preserves arithmetic. This is enough, but if you want to really sink your teeth in the details behind this, read on.

First just a lemma in case this hasn't come up for you all yet, as on a cursory glance I don't see it in Hungerford. You don't need to prove this, but I wanted to include it here in case you hadn't seen it.

Lemma 1. *Let $\varphi : A \to B$ be a homomorphism between algebraic objects (say groups, rings, fields, vector spaces, etc.). Then the following are equivalent*

(1) φ is an isomorphism as in Hungerford, meaning it is injective and surjective.

(2) There exists an $\underline{\text{inverse homomorphism}}$ $\psi = \varphi^{-1}$, which is uniquely defined by the equalities

$$\psi \circ \varphi = \mathrm{id}_A, \ \text{and}\ \varphi \circ \psi = \mathrm{id}_B,$$

with $\mathrm{id}_A : A \to A$ being the identity map, defined by $\mathrm{id}_A(a) = a$ for all $a \in A$, and similar for id_B.

As a remark, the first formulation of this definition is sometimes easier to check, while the second formulation of the definition is sometimes more powerful to use.

Proof. First let's do (2) $\implies$ (1). To show that φ is injective, suppose we have elements $a, a' \in A$ such that $\varphi(a) = \varphi(a')$. Then we have

$$a = \psi \circ \varphi(a) = \psi \circ \varphi(a') = a',$$

so φ is injective. For surjectivity, let $b \in B$. Then we have

$$b = \varphi \circ \psi(b) = \varphi(\psi(b)),$$

which shows that b is in the image of φ. Since $b \in B$ was arbitrary, φ is surjective as desired.

Now let's show (1) $\implies$ (2). Injectivity and surjectivity of φ together show that for any $b \in B$ there is a unique $a \in A$ so that $\varphi(a) = b$. Sending each $b \in B$ to this corresponding $a \in A$ yields a function $\psi : B \to A$ so that $\varphi \circ \psi = \mathrm{id}_B$ (note that we could have gotten a function satisfying this property even if φ was just surjective, using the axiom of choice). To show that $\psi \circ \varphi = \mathrm{id}_A$, note that

$$\varphi\Big((\psi \circ \varphi)(a)\Big) = (\varphi \circ \psi)(\varphi(a)) = \varphi(a).$$

Thus, a and $\psi \circ \varphi(a)$ have the same image under φ. Since φ is injective, we must have that $a = \psi \circ \varphi(a)$. Since $a \in A$ was arbitrary, we have that $\psi \circ \varphi = \mathrm{id}_A$, as desired.

So now all that remains is to show that ψ is also a homomorphism. For the rest of this proof, when we concatenate two elements of A or B we refer to using whatever way of putting elements together is relevant to the algebraic structure at hand. Like multiplying in a group, adding and multiplying in a ring, or adding and multipying by scalars in a vector space.

We wish to show that for any elements $b, b' \in B$ we have that $\psi(bb') = \psi(b)\psi(b')$. Since φ is injective, it suffices to show that $\varphi(\psi(bb') = \varphi(\psi(b)\psi(b'))$. We compute

$$\begin{aligned} \varphi\big(\psi(b)\psi(b')\big) &= \varphi(\psi(b))\varphi(\psi(b')) && \text{(as } \varphi \text{ is a homomorphism)} \\ &= bb' \\ &= \varphi(\psi(bb')), \end{aligned}$$

as desired. □

(a) First we show that composing two elements of the Galois group does in fact yield another element in the Galois group. To do this, let $\sigma, \tau \in \operatorname{Gal}(L/K)$. To see that $\sigma \circ \tau$ is also an isomorphism, note that the lemma yields inverse homomorphisms σ^{-1} and τ^{-1}. Since the composition of homomorphisms is a homomorphisms, the element $\tau^{-1} \circ \sigma^{-1}$ is a field homomorphism $L \to L$. We compute

$$\begin{aligned}(\tau^{-1} \circ \sigma^{-1}) \circ (\sigma \circ \tau) &= \tau^{-1} \circ (\sigma^{-1} \circ \sigma) \circ \tau \\ &= \tau^{-1} \circ \mathrm{id}_L \circ \tau \\ &= \tau^{-1} \circ \tau \\ &= \mathrm{id}_L,\end{aligned}$$

and the other composition works similarly. Thus $\sigma \circ \tau$ also has an inverse, and so $\sigma \circ \tau$ is an automorphism of L as well, so all that needs be shown to see that $\sigma \circ \tau \in \operatorname{Gal}(L/K)$ is that $\sigma \circ \tau$ also fixes K.

To see this, let $x \in K$. Then since σ and τ both fix K we have

$$\sigma \circ \tau(x) = \sigma(x) = x.$$

So we've verified that composition makes sense.

The identity map $\mathrm{id}_L : L \to L$ is a field automorphism and fixes K as it fixes everything. Furthermore, for any $\sigma \in \operatorname{Gal}(L/K)$ we have that $\sigma \circ \mathrm{id}_L = \mathrm{id}_L \circ \sigma$, so we have an identity element for the group. Associativity follows as function composition is associative.

For inverses, we showed in the lemma that any $\sigma \in \operatorname{Gal}(L/K)$ has an inverse automorphism $\sigma^{-1} : L \to L$, but we still have to show that σ^{-1} also fixes K. But for any $x \in K$ we have $x = \sigma(x)$, and applying σ^{-1} on both sides yields $\sigma^{-1}(x) = x$, as desired.

□

(b) Let $f = \sum\limits_{i=0}^{n} a_i x^i$, with $a_i \in K$. By assumption, we have

$$0 = \sum_{i=0}^{n} a_i \alpha^i.$$

Applying σ on both sides, and using that $\sigma(0) = 0$ and that σ commutes with addition and multiplication, we get

$$0 = \sum_{i=0}^{n} \sigma(a_i)\sigma(\alpha)^i = \sum_{i=0}^{n} a_i \sigma(\alpha)^i,$$

as by assumption $\sigma(a) = a$ for all $a \in K$. This is exactly the statement that $f(\sigma(\alpha)) = 0$, which is the desired result.

□

Problem 7.6

Compute the Galois groups of the following extensions

(a) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

(c) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)/\mathbb{Q}$

(d) $\mathbb{F}_{p^2}/\mathbb{F}_p$.

(a) The Galois group is $\mathbb{Z}/2\mathbb{Z}$.

To see this, let $f = x^2+2 \in \mathbb{Q}[x]$. Then $\mathbb{Q}(\sqrt{2})$ is the splitting field of f over $\mathbb{Q}$, as the other root of f is $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. So we get an injection $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \hookrightarrow S_2$. Furthermore, this embedding has as its image a transitive subgroup of S_2 (meaning one capable of sending any element in $\{1, 2\}$ to any other element in that same set by a permutation in the subgroup). There is only one such subgroup, namely S_2 itself, so the Galois group is isomorphic to $S_2 \cong \mathbb{Z}/2\mathbb{Z}$.

(b) The Galois group is trivial, the unique group with 1 element.

To see this, note that any element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is uniquely determined by where it sends $\sqrt[3]{2}$, and it must send this element to some root of $f = x^3 - 2$. However, we have $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, and the other two roots of f are in $\mathbb{C} \setminus \mathbb{R}$, so the only possibility is that σ sends $\sqrt[3]{2}$ to itself. Since the identity automorphism does this, the identity automorphism must be the only automorphism.

(c) The Galois group is S_3, the symmetric group on 3 letters.

To see this, let $f = x^3 - 2 \in \mathbb{Q}[x]$. I claim that $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ is the splitting field for f over $\mathbb{Q}$. We will prove this at the end, but first we see how this lets us compute the Galois group.

Let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$, and let $G = \mathrm{Gal}(L/\mathbb{Q})$. Since f is irreducible over $\mathbb{Q}$ (say by Eisenstein at the prime 2) and $\mathbb{Q}$ is of characteristic zero, we have that f is separable (this could also be verified by computing the roots and seeing that they are distinct). Thus, the action G on the roots of f yields an embedding $G \hookrightarrow S_3$. So we just need to show that $|G| = 6$ to get the desired isomorphism. The embedding above yields $|G|$ divides 6, so we just need to show $|G| > 3$. We will do this by building up automorphisms from the two intermediate fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt{3}i)$.

Consider the field extension $\mathbb{Q}(\sqrt[3]{2}) \subset L$. This extension is proper as the former field is contained in $\mathbb{R}$ and the latter field isn't. Furthermore L is obtained from the first field by adjoining a root of $p(x) = x^2 + 3$. Since the extension is proper, p can't split over $\mathbb{Q}(\sqrt[3]{2})$, and since p is of degree 2, it must be irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Note for later that this together with $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ implies $|L : \mathbb{Q}| = 6$. Thus, we have an isomorphism

$$L \cong \frac{\mathbb{Q}(\sqrt[3]{2})[x]}{(x^2+3)}.$$

Thus, we have an automorphism $\tau : L \to L$ fixing $\mathbb{Q}(\sqrt[3]{2})$ with $\tau(\sqrt{3}i) = -\sqrt{3}i$ (this corresponds to $x \mapsto -x$ under the above isomorphism).

Now consider the field extension $\mathbb{Q}(\sqrt{3}i) \subset L$. Since $|L : \mathbb{Q}| = 6$ and $|\mathbb{Q}(\sqrt{3}i) : \mathbb{Q}| = 2$, we have that $|L : \mathbb{Q}(\sqrt{3}i)| = 3$. Furthermore, L is obtained from $\mathbb{Q}(\sqrt{3}i)$ by adjoining a root of $f(x) = x^3 - 2$. Since the degree of the field extension and the degree of this polynomial are the same, we must have that f is irreducible. Thus, we have an isomorphism

$$L \cong \frac{\mathbb{Q}(\sqrt{3}i)[x]}{(x^3-2)}.$$

Since we have already shown that f splits in L with 3 distinct roots, we get three automorphisms of L fixing $\mathbb{Q}(\sqrt{3}i)$ sending $\sqrt[3]{2}$ to each of the three roots of f. Let these three automorphisms be σ_1, σ_2, and σ_3.

So to show that $|G| > 3$, we just need to show that τ and the σ_i are distinct. The σ_i are distinct from each other because they send $\sqrt[3]{2}$ to different elements. The σ_i are distinct from τ because the σ_i all fix $\sqrt{3}i$, but τ does not. Thus, we have 4 distinct elements of the Galois group, and so by previous reasoning the Galois group is S_3.

The only loose end to tie up is to show that L is the splitting field of $f = x^3 - 2$ over $\mathbb{Q}$. To see this, let K be the splitting field of f over $\mathbb{Q}$.

Note that the roots of f are

$$\sqrt[3]{2}, \alpha := \frac{\sqrt[3]{2}}{2}(-1+\sqrt{3}i), \text{ and } \frac{\sqrt[3]{2}}{2}(-1-\sqrt{3}i).$$

This shows that all the roots of f live in L, so the universal property of splitting fields yields $K \subset L$. Furthermore, we have

$$\sqrt{3}i = \frac{2\alpha}{\sqrt[3]{2}} + 1 \in K,$$

so we get that $\sqrt[3]{2}$ and $\sqrt{3}i$ are both elements of K. Minimality yields $L \subset K$, and so equality must hold.

□

(d) The Galois group is $\mathbb{Z}/2\mathbb{Z}$, generated by the Frobenius homomorphism $\sigma(x) = x^p$.

The results of problem 4 yield that σ is a nonidentity element of $G := \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Since the elements of $\mathbb{F}_{p^2}$ are exactly the roots of $x^{p^2} - x$, we have that $\sigma^2 = \mathrm{id}$. So we have an inclusion $\mathbb{Z}/2\mathbb{Z} \hookrightarrow G$, and it just suffices to show that $|G| \leq 2$.

Indeed, let α be any element of $\mathbb{F}_{p^2}$ that's not in $\mathbb{F}_p$. Since $|\mathbb{F}_{p^2} : \mathbb{F}_p| = 2$, we have that $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$. Furthermore, the minimal polynomial f for α has degree equal to the degree of the extension which is 2. Thus f has at most 2 roots. So the action of G on the roots of f yields an embedding $G \hookrightarrow S_n$ for $n \leq 2$, with n the number of distinct roots of f. Thus, we have $|G| \leq 2$, as desired.

□

As a remark, note that the discussion in the last paragraph gets a little funky in characteristic 2 (for instance, it isn't clear that f is separable there), while the discussion of the Frobenius homomorphism remains unchanged.