Exercises to do in a Field

Mike Pierce

From Professor Ran's 2008 Qualifying Exam

Exercise 1 — Let $f(x) = x^5 - x + 1 \in \boldsymbol{F}_5[x]$.

(a) Prove that f has no roots in $\boldsymbol{F}_{25}$. (Hint: What polynomial identity holds for any element of $\boldsymbol{F}_{25}$?).

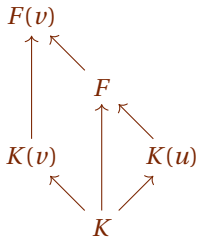
(b) Determine the splitting field and full Galois correspondence for the polynomial $x^5 - x + 1$ over $\boldsymbol{F}_5$, over $\boldsymbol{F}_{25}$, and over $\boldsymbol{F}_{125}$.

See Page 5 in the Galois Theory section of Dusel's notes, and also Proposition 7.8 in Chapter V of Hungerford, and the following Corollary. We can verify $x^5 - x + 1$ has not roots in $\boldsymbol{F}_5$ manually, and so, by that theorem that says this particular polynomial is either irreducible or splits completely over $\boldsymbol{F}_5$, f must be irreducible. If F is the splitting field of f over $\boldsymbol{F}_5$, then $[E : \boldsymbol{F}_5] = 5$. But since $[\boldsymbol{F}_{125} : \boldsymbol{F}_5] = 3$ and $[\boldsymbol{F}_{25} : \boldsymbol{F}_5] = 2$, and neither 2 nor 3 divide 5, they cannot be intermediate fields. In particular their intersection with E is trivial so neither $\boldsymbol{F}_{25}$ nor $\boldsymbol{F}_{125}$ contain any roots of f.

Over each of $\boldsymbol{F}_5$, $\boldsymbol{F}_{25}$, and $\boldsymbol{F}_{125}$, the splitting field of f will be a degree 5 cyclic extension, and so will be the fields $\boldsymbol{F}_5^5$, $\boldsymbol{F}_{25^5}$, and $\boldsymbol{F}_{125^5}$ respectively. These are cyclic extension, each with Galois group $\mathbf{Z}_5$, so there are are no subgroups or intermediate fields to speak of.

Exercise 2 — Let F be the splitting field of $f \in K[x]$ over K. Prove that if an irreducible polynomial $g \in K[x]$ has a root in F, then g splits into linear factors over F. (This result is part of a theorem characterizing normal extensions and you may not, of course, quote this theorem or its corollaries).

Let u be a root of g in F let v be a root of g that is not necessarily in F. Let G denote the splitting field of g over K. Both u and v are roots of the irreducible polynomial g so there is some automorphism $\varphi \in \mathrm{Aut}_K(G)$ that swaps v and u, because the Galois group acts transitively on the roots of the polynomial. So $K(v) \simeq K(u)$ via this isomorphism. Now the heavy lifting thanks to Theorem 3.8 in Chapter V of Hungerford: since F is a splitting field of f over $K(u)$ and $F(v)$ is a splitting field of $\varphi f = f$ over $K(v)$, then φ extends to an isomorphism $F \simeq F(v)$.



But if $F \simeq F(v)$, well then F and $F(v)$ have the same degree over K, so they must be equal. I.e, $v \in F$ all along.

Exercise 3 — Disprove (by example) or prove the following: If $K \to F$ is an extension (not necessarily Galois) with $[F:K] = 6$ and $\mathrm{Aut}_K(F)$ isomorphic to the Symmetric group S_3, then F is the splitting field of an irreducible cubic in $K[x]$.

Let E be the fixed field of $\mathrm{Aut}_K(F)$. So $E \to F$ is Galois and has degree $|\mathrm{Aut}_K(F)| = |S_3| = 6$. But since $[F:K] = 6$ and E is an intermediate field, we must have that $E = K$, so $K \to F$ is Galois. Now look at the subgroup $\langle (1\,2) \rangle$ in S_3, and let L be the intermediate field of $K \to F$ Since $\langle (1\,2) \rangle$ is an index 3 subgroup, $[L:K] = 3$, and so $L = K(a)$ for any $a \in L \setminus K$ (because there's no room for $K(a)$ be an intermediate extension). So a is the root of some irreducible cubic f over K, but since $\langle (1\,2) \rangle$ is not a normal subgroup of S_3, there is some automorphism of $\mathrm{Aut}_K(F)$ that sends a to some other root of f outside of L. In particular, L doesn't contain all the roots of f, so you've got to go up to F to get all the roots, and so F is the splitting field of f.

Exercise 4 — If $\boldsymbol{Z}_p \to F$ is a field extension of degree n then the map $x \mapsto x^p$ is a $\boldsymbol{Z}_p$-automorphism of F of order exactly n whose fixed field is $\boldsymbol{Z}_p$.

If $\mathbf{Z}_p \to F$ has degree n, then $F \simeq \mathbf{Z}_{p^n}$ and is the splitting field of the polynomial $x^{p^n} - x$ over $\mathbf{Z}_p$. In particular, every element of $a \in F$ satisfies $a = a^{p^n}$ so the map $x \mapsto x^p$ has order n. Since $(ab)^p = a^p b^p$ and since

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p = x^p + 0 + \cdots + 0 + y^p = x^p + y^p$$

because $\binom{p}{i}$ is divisible by p, the map $x \mapsto x^p$ is a homomorphism of fields. Since $x^p = x \cdot x \cdot \cdots \cdot x = 0$ if and only if $x = 0$ (field are quite integral domains) the map $x \mapsto x^p$ is injective, and hence surjective since $\mathbf{Z}_p$ is finite, so $x \mapsto x^p$ is an honest automorphism of the field $\mathbf{Z}_p$. Furthermore, by Fermat's little theorem (maybe prove this?) $x^p \equiv_p x$ for all $x \in \mathbf{Z}_p$, so $\mathbf{Z}_p$ is fixed by the automorphism $x \mapsto x^p$. (Why is $\mathbf{Z}_p$ *exactly* the fixed field though?)

From Professor Ran's 2006 Qualifying Exam

Exercise 5 — Let $K \subseteq F$ be a finite dimensional extension.

(a) Define what it means for F to be separable over K.

(b) Prove from scratch that if K is a finite field then F is separable over K.

(c) Prove that if K is of characteristic zero then F is separable over K.

(d) Given an example of a non-separable finite dimensional extension.

A field F is *separable* over K if for each $u \in F$ the minimum polynomial f of u has distinct roots in K. Furthermore we say that the polynomial f is separable if it has no multiple roots in some splitting field over K.

By a theorem, f is separable over K if its formal derivative f' is nonzero. ... ◂

EXERCISE 6 — Let K be a field with 9 elements. Prove from scratch that K has an extension of degree 2 and that any two such are isomorphic over K.

◀

EXERCISE 7 — (Note that this exercise isn't correct as stated) Let $u = \sqrt{3+\sqrt{2}}$.

(a) Determine the minimal polynomial f of u over $\mathbf{Q}$.

(b) Prove that $F = \mathbf{Q}(u)$ is a splitting field of f over $\mathbf{Q}$.

(c) Prove that $\sqrt{7} \in F$.

(d) Determine the Galois group of F over $\mathbf{Q}$.

◀

From Professor Ran's 2018 Final

EXERCISE 8 — Let $K \to F$ be an algebraic extension.

(a) Prove that given $u \in F$ there exists an intermediate field E containing u such that $[E : K]$ is finite.

(b) Let $\varphi\colon F \to F$ be a K-monomorphism, i.e. an injective field homomorphism that is the identity on K. Prove that φ is surjective.

(c) Give an example to show that the statement (b) is false without the assumption $K \to F$ algebraic.

◀

EXERCISE 9 —

(a) Let $K \to F$ be a Galois extension with Galois group S_3. Prove or disprove: F is a splitting field over K of a cubic polynomial

(b) Give an example with proof of a splitting field over $\mathbf{Q}$ with Galois group S_3.

Part (a) is just a more chill version of Question 3 above. Then finding an example of such a splitting field is chill too if you remember this theorem.

THEOREM 1 — (4.12 in Hungerford) If p is a prime and f is an irreducible polynomial of of degree p over the field of rational numbers which has precisely two nonreal roots in the field of complex numbers, then the Galois group of f is (isomorphic to) S_p.

So the polynomial $f = x^3 - 2$ will work. I think this might be overkill, but to echo the proof of the theorem, if G is the Galois group of f then since f is irreducible over $\mathbf{Q}$ we can regard G as a subgroup of S_3 and say that 3 divides the order of G, i.e G contains a 3-cycle.

Then since f has complex roots (by inspection, but you can do some calculus if you want to be rigorous) complex conjugation is an automorphism of the splitting field of f over $\mathbf{Q}$, which is a transposition in G, and this 3-cycle and transposition will generate all of S_3.

EXERCISE 10 — Let p be a prime and n be any natural number.

(a) Prove that there exists an irreducible polynomial f of degree n in $\mathbf{Z}_p[x]$.

(b) Let $f \in \mathbf{Z}_p[x]$ be an irreducible polynomial of degree n. Determine with proof the degree of the splitting field of f over $\mathbf{Z}_p$.

(c) Exhibit with proof irreducible polynomials of degree 2, 3, and 4 over $\mathbf{Z}_2$.

(a) If a monic polynomial f of degree n is reducible then it must have a monic irreducible factor of degree i for some $i \in \{1, \ldots, m\}$, where $m = \lfloor n/2 \rfloor$. We can simply count the possible number of polynomials f and the possible number of irreducible factors, and note that the former number is greater than the latter to conclude that some f must be irreducible. There are p^n ways to choose the coefficients of f and, again choosing coefficients, there are $p + p^2 + \cdots + p^m$ possibilities of irreducible factor. Then we're good since

$$p + p^2 + \cdots + p^m = \frac{p^{m+1} - p}{p - 1} < p^{m+1} \leq p^n .$$

For part (b), let F be a splitting field of f over $\mathbf{Z}_p$. Recall that the multiplicative group of units of F must be cyclic*. Letting u be a generator of that cyclic group, note that $u \notin \mathbf{Z}_p$, else it couldn't generate all of F. So $F = \mathbf{Z}_p(u)$, and since u is a root of f and f is irreducible, u has degree n over $\mathbf{Z}_p$, so $[F : \mathbf{Z}_p] = n$.

(*) If you really want to prove that $F^\times$, the group of units of F, must be a cyclic group, notice first that it must be a finite abelian group, so $F^\times$ decomposes as $\mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_k}$ where the m_i are the *invariant factors* of the multiplicative group. So $m_1 | m_2 | \cdots | m_k$, and all the elements of $F^\times$ have order dividing m_k. In particular every element of $F^\times$ is a root of $x^{m_k} - 1$ which has exactly m_k distinct roots, so $|G| = m_k$ and $G \simeq \mathbf{Z}_{m_k}$

There are many answers to part (c). Since $\mathbf{Z}_2$ has characteristic 2 though, it's probably smart to guess polynomials with an odd number of terms that have non-zero constant term to ensure that neither 0 or 1 is a root.

$$x^2 + x + 1 \qquad x^3 + x + 1 \qquad x^3 + x + 1 \qquad x^4 + x + 1$$

None of these have 0 or 1 as a root. Then since a reducible polynomial of degree ≤ 3 must have a linear factor, the first three polynomials must be irreducible. Now we've just got to check that $x^4 + x^3 + 1$ doesn't factor into quadratics. If it did, its factorization would look something like $x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$. Cranking out the right-hand-side we see that the coefficients of the x^3 term and the x term both have to be $(a + b)$, so such a factorization can't exist.

EXERCISE 11 — Let $K \to F$ be a field extension such that $[F : K] = n$ and let $G = \mathrm{Aut}_K(F)$.

(a) Prove that $|G| \leq n$. For extra credit prove $|G|$ divides n.

(b) Prove that if $n = 2$ then $|G| = 2$ and for every $n > 2$, give an example where $|G| < n$.

(c) Prove that if $|G| = n$, then $K \to F$ is Galois, i.e. the fixed field of G is K.

Let E be the fixed field of G. So we have a tower of fields $K \to E \to F$, where $E \to F$ is a Galois extension of degree $|G|$. Then by all the stuff we know about towers of fields (stuff we need to prove here?), $|G|$ has to divide $[F : K]$ which is n.

The next part is true just because 2 is prime and small, so $E = F$. In particular $F = K(u)$ for some $u \notin K$ such that $u^2 \in K$. So u is a root of $x^2 - u^2 \in K[x]$, which is irreducible because otherwise u would be a product of the constant terms of the factors and so it would be in K.

For the example, I think $\mathbf{Q} \to \mathbf{Q}\left(\sqrt[n]{2}\right)$ works. ... now I'm not so sure ◄

Here's TeX/TikZ code for a tower diagram of fields, if anyone needs it. In particular this one is for the splitting field of the polynomial $(x^2-2)(x^2-3)(x^2-5)$, but it's not quite right: I forgot $\mathbf{Q}[\sqrt{30}]$.