Galois Theory Exercises

Section 1

1. Show that the discriminant $b^2 - 4ac$ of the general quadratic $ax^2 + bx + c$ can be written as $(r_1 - r_2)^2$, where r_1, r_2 are the roots. (Hint: either use the factorisation $x^2 + \frac{b}{a}x + \frac{c}{a} \equiv (x - r_1)(x - r_2)$ to link r_1, r_2 to a, b, c or check directly from the quadratic formula).

   We will create a similar thing for higher degree polynomials later but the absence of a general formula for the roots will mean you have to do it the first way. Also Galois theory will allow us to check that this generalized discriminant always lies in the same field as the coefficients of the polynomial.

Section 2

1. What is the characteristic of the following fields?
   (a) $\mathbb{C}$
   (b) $\mathbb{F}_p(t)$ - Laurent series in t with coefficients that are integers mod p
   (c) $\mathbb{Q}(\sqrt{2})$

2. Describe bases for the following field extensions:
   (a) $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$
   (b) $\mathbb{R}(\sqrt{7})/\mathbb{R}$
   (c) $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt{18225})/\mathbb{Q}$
   (e) $\mathbb{Q}(\sqrt{3}, \sqrt{11})/\mathbb{Q}$
   (f) $\mathbb{Q}(\sqrt{3}, \sqrt{27})/\mathbb{Q}$
   (g) $\mathbb{C}(t)/\mathbb{C}$, where t is an indeterminate.
   (h) $\mathbb{C}(t)/\mathbb{R}$, where t is an indeterminate.

3. What is the degree of the extension $\mathbb{C}/\mathbb{Q}$? How is this different from the extension $\mathbb{C}/\mathbb{R}$?

4. Prove that there is no field K with $\mathbb{R} \subset K \subset \mathbb{C}$. (Hint: Tower of fields) Generalise your answer to prove that for any extension L/K of prime degree, there is no field M with $K \subset M \subset L$.

5. Prove that any field K with $\mathbb{Q} \subset K \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ satisfies $[K : \mathbb{Q}] = 2$. Find three such subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   Later we will see that the main theorem of Galois theory provides a proof that these three fields are the only ones. It will also give us a way to find the subfields explicitly without having to make educated guesses.

6. The real number π is not algebraic over $\mathbb{Q}$. This is hard to prove. However, show that π is algebraic over $\mathbb{R}$. In fact show that π is algebraic over $\mathbb{Q}(\pi)$.

7. Show that the polynomial $x^2 + x + 4$ is irreducible over $\mathbb{Q}$. (Hint: Eisenstein).

8. Consider the quotient ring $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$. Prove that it is a field by giving consistent addition/multiplication tables. How many elements has it got? Which finite field must it be isomorphic to?

   There is a better way to prove that we have a field here, a method that allows us to construct any finite field using polynomials. The polynomial x^2+x+1 is irreducible over $\mathbb{F}_2$ (it has no roots here, check). Thus the ideal $\langle x^2+x+1\rangle$ of $\mathbb{F}_2[x]$ is maximal, hence the quotient is a field. Clearly $\{[1],[x]\}$ is a basis, so that the field has $2^2=4$ elements.

   Use the same ideas to construct $\mathbb{F}_8$ and $\mathbb{F}_9$ as quotients of polynomial rings (the characteristic will be important).

Section 3

1. Find the Galois groups of the following finite extensions by ad hoc methods:
   (a) $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$.
   (b) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.
   (c) $\mathbb{Q}(\sqrt{2},\sqrt{7})$.

2. Consider a simple finite extension $K(\alpha)/K$, where K is a subfield of $\mathbb{C}$ and α has minimal polynomial f of degree n over K. Show that there are n distinct K-monomorphisms $K(\alpha)\to\mathbb{C}$ defined by $\alpha\mapsto\beta$, where β is any root of f. Which of these K-monomorphisms do you think provide K-automorphisms of $K(\alpha)$? Make a conjecture about the size of the Galois group based on this.

Section 4

1. Compute the action of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ on the roots of the following polynomials over $\mathbb{Q}$ (roots considered in $\mathbb{C}$):
   (a) x^2+1.
   (b) x^2+4.
   (c) $x^2-6x+10$.
   (d) x^3-1.
   (e) $x^4-8x^3+9x^2+24x-60$, (I promise that this factorises!).
   (f) $x^4-8x^3+15x^2-24x+60$ (...this too).

2. Find bounds for the size of the Galois groups of these extensions of $\mathbb{Q}$:
   (a) $\mathbb{Q}(\sqrt{5},\sqrt{11})$.
   (b) $\mathbb{Q}(\sqrt[3]{5},\sqrt{3})$.
   (c) $\mathbb{Q}(\sqrt[53]{13})$.
   (d) $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7},\sqrt{11},...,\sqrt{199})$.

Section 5

1. Return to the previous question and find all of the Galois groups, checking your bounds worked.

2. In this question we will investigate the Kronecker-Weber theorem for the special case of quadratic extensions of $\mathbb{Q}$.
   (a) Show that every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{d})$ for some square free integer d. Are any of these isomorphic?

(b) Consider the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive p-th root of unity for odd prime p. Invent the element:

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^a,$$

where $\left(\frac{a}{p}\right)$ is the Legendre symbol. This sum is an object known as a *Gauss sum*.
Show that:

$$G^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p,$$

and hence that $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \subseteq \mathbb{Q}(\zeta)$. (If you are struggling then just do all of this explicitly for the cases $p = 3, 5$).

(c) Hence show that the fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$ each lie in some cyclotomic field. (this is not as easy as it sounds, you might have to split cases and adjoin something to take account of the minus in the previous part).

(d) Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ each lie in some cyclotomic field (consider adjoining a primitive 8-th root of unity to $\mathbb{Q}$).

(e) Use the previous parts to show that every quadratic extension of $\mathbb{Q}$ lies in some cyclotomic field. (Hint: prime factorisation).

3. We can now prove quadratic reciprocity

(a) Let $q \neq p$ be an odd prime and consider the same setup as in the previous question. Show that:

$$G^q = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G \bmod q.$$

(Hint: use what you know about G^2.)

(b) Show explicitly that:

$$G^q \equiv \left(\frac{q}{p}\right) G \bmod q.$$

(c) Assuming that cancellation of G may occur mod q (which it can here, but is not obvious), prove the main part of the quadratic reciprocity law:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Section 6
Section 7
Section 8

1. Use the main theorem of Galois theory to prove that there are no fields K satisfying $\mathbb{R} \subset K \subset \mathbb{C}$. (You solved this earlier using a tower of fields argument but really it is just a consequence of group theory)

2. Use the main theorem to investigate the correspondence for the following extensions:

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{11})/\mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}$, where ζ is a primitive cube root of unity. (This is the *normal closure* of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$).

(c) $\mathbb{Q}(\zeta)$, where ζ is a primitive 5-th root of unity. Do the same for a primitive 7-th root of unity.

3. Consider $\mathbb{Q}(\zeta)$ for ζ a primitive p-th root of unity (for odd prime p).

(a) Viewing the Galois group as $(\mathbb{Z}/p\mathbb{Z})^\times$, let g be a primitive root mod p (so that g is not a quadratic residue mod p; the quadratic residues form a proper subgroup of even powers of g).
Show that if $h = g^{\frac{p-1}{2}}$ then $H = \{1, h\}$ forms a subgroup of the Galois group.

(b) Show that the element $\zeta + \sigma_h(\zeta)$ of $\mathbb{Q}(\zeta)$ is fixed by H. What is this element explicitly?

(c) Hence show that the fixed field of H is $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos(\frac{2\pi}{p}))$. (This requires a little bit of extra work, part (b) only shows that the fixed field contains $\mathbb{Q}(\zeta + \zeta^{-1})$).

4. Let p be prime. Consider the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ for some primitive p-th root of unity. We will show the existence of a unique quadratic extension using the main theorem of Galois theory. Note that we have done the existence part of this in a previous question explicitly using Gauss sums.

(a) What is the Galois group of this extension?

(b) Is the extension Galois?

(c) Can you find a subgroup H of the Galois group of order $\frac{p-1}{2}$? (Hint: QR)

(d) How does this give the existence of a unique intermediate field making a quadratic extension of $\mathbb{Q}$? (You may assume that the Galois group is cyclic. This is true by the existence of primitive roots mod p).

5. We can use the setup in the previous question to prove quadratic reciprocity in a way that generalizes to higher powers. In this question we will get halfway. The other half requires some algebraic number theory.

(a) Let $q \neq p$ be an odd prime. Show that $\left(\frac{q}{p}\right) = 1$ is the same as the element σ_q of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ belonging the the subgroup H in part (c) above.

(b) Remind yourself what the corresponding fixed field of H must be (return to the Gauss sum question).

(c) Now use the main theorem of Galois theory to show that $\left(\frac{q}{p}\right) = 1$ is the same as σ_q fixing this field.

(d) The element σ_q attatched to the prime q is quite an important element in algebraic number theory called the Frobenius element of q. It has certain nice properties measuring the factorisation of primes in certain bigger rings than $\mathbb{Z}$. Here the fact that the frobenius element fixes $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ tells us that q must factorise in the so called ring of integers of this field. But this is a quadratic extension of $\mathbb{Q}$ and algebraic number theory tells us exactly which primes factorise in such extensions...in this case they are the primes q with Legendre symbol $\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1$.

(e) Thus we have an equality:

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right).$$

This is equivalent to quadratic reciprocity since by Euler's criterion:

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) \equiv ((-1)^{\frac{p-1}{2}})^{\frac{q-1}{2}} \bmod q,$$

so that

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{q}\frac{q-1}{2}}\left(\frac{p}{q}\right) \bmod q,$$

which must provide an equality since both sides take values in $\{\pm 1\}$.

6. Some of the work done in MAS276 (Rings and groups) fits in nicely with Galois theory and algebraic number theory. In this question we see how the norms in the quadratic rings $\mathbb{Z}[\sqrt{d}]$ are really definable in terms of Galois theory.

   (a) Recall in MAS276 that for $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ we were able to define a norm as follows:

   $$N(\alpha) = a^2 - db^2.$$

   Show that this is really $\alpha\sigma(\alpha)$ where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d}))$ is the non-identity element.

   (b) Let K be a number field (finite extension of $\mathbb{Q}$). Show that if $K/\mathbb{Q}$ is a Galois extension then

   $$N(\alpha) := \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha)$$

   lies in $\mathbb{Q}$ for any $\alpha \in K$.

   (c) Show further that if α satisfies a monic polynomial with integer coefficients then $N(\alpha) \in \mathbb{Z}$. This generalises what you did in MAS276, but to certain other "ring extensions" of $\mathbb{Z}$. (Hint: What does the Galois group send such elements to? Which elements of $\mathbb{Q}$ have this property?)

   (d) Each number field contains a special ring that generalises the notion of "integer". Every number field has finite degree over $\mathbb{Q}$, so creates an algebraic extension. Clearing denominators of polynomials we find that every element in a number field satisfies some polynomial over $\mathbb{Z}$. If we take the ones that satisfy a **monic** polynomial over $\mathbb{Z}$ then (non-trivially) we get a ring, called the *ring of integers* of the number field, denoted $\mathfrak{O}_K$ (we describe the elements of this ring as "integers of K").

   Show that if $K = \mathbb{Q}$ then $\mathfrak{O}_K = \mathbb{Z}$ (you used this in the previous part). Also try to prove that for $K = \mathbb{Q}(\sqrt{d})$ we have $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$ otherwise (in other words the elements in $\mathbb{Z}[\sqrt{d}]$ are always integers of K but sometimes there are more).

   (e) Let L be a number field. Show that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ sends integers of L to other integers of L. Thus, given any Galois extension of number fields L/K show that the generalised norm:

   $$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$$

   lies in $\mathfrak{O}_K$ for any $\alpha \in \mathfrak{O}_L$ (Hint: use the fact that $\mathfrak{O}_L \cap K = \mathfrak{O}_K$).

   This is a major generalisation of the fact that the norm of things in $\mathbb{Z}[\sqrt{d}]$ turn out to be in $\mathbb{Z}$ but here this is a general norm that works in arbitrary number fields. We can now study nice properties of integers via relative extensions of number fields. More information is preserved by not working directly in $\mathbb{Z}$.

   (f) Play around with a few of the norms here for cyclotomic extensions and other number fields of your choice. Also resurect your A-level knowledge and investigate how "rationalising the denominator" is really a trick involving the work done in this question.

   constructing fermat prime gons using main theorem (existence of tower of quadratic extensions via existence of subgroups order powers of 2).

Section 9