MODULE 3: EXERCISE SHEET 1

These problems are due Sunday, 12 June, 2016. They must be sent to nap@rnta.eu (copy to nickgill@cantab.net) by 10 pm Nepal time.

(1) Let p be an odd prime, and let ζ be a primitive pth root of 1 in $\mathbb{C}$. Let $E = \mathbb{Q}[\zeta]$ and let $G = \mathrm{Gal}(E/\mathbb{Q})$; thus $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$. Let H be the subgroup of index 2 in G. Put $\alpha = \sum_{i \in H} \zeta^i$ and $\beta = \sum_{i \in G \setminus H} \zeta^i$. Show:

(a) α and β are fixed by H;

(b) if $\sigma \in G \setminus H$, then $\sigma\alpha = \beta$, $\sigma\beta = \alpha$.

Thus α and β are roots of the polynomial $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. Compute $\alpha\beta$ and show that the fixed field of H is $\mathbb{Q}[\sqrt{p}]$ when $p \equiv 1 \pmod 4$, and $\mathbb{Q}[\sqrt{-p}]$ when $p \equiv 3 \pmod 4$.

Answer. *Parts (a) and (b) both follow from the fact that if $a, g \in G$ and H is a subgroup of G, then Ha is a coset of H, as is Hag. In our particular case, if $g \in H$, then $Hag = Ha$, while if $g = \sigma \in G \setminus H$, then $Hag \neq Ha$.*

(a) *Let $h \in H$, and observe that*

$$\alpha^h = \sum_{i \in H} \zeta^{ih} = \sum_{i \in H} \zeta^i = \alpha$$
$$\beta^h = \sum_{i \in G \setminus H} \zeta^{ih} = \sum_{i \in G \setminus H} \zeta^i = \alpha.$$

(b) *Let $h \in H$, and observe that*

$$\alpha^h = \sum_{i \in H} \zeta^{i\sigma} = \sum_{i \in G \setminus H} \zeta^i = \beta$$
$$\beta^h = \sum_{i \in G \setminus H} \zeta^{ih} = \sum_{i \in G \setminus H} \zeta^i = \alpha.$$

Then $f = (X - \alpha)(X - \beta) = X - tX + \alpha\beta$ and, since t is the sum of all the powers of ζ, and elementary number theory asserts that $t = -1$, α and β are the roots of $X^2 + X + \alpha\beta$.

If $p \equiv 3 \pmod 4$, then $\alpha\beta = \frac{p+1}{4}$, and the quadratic formula implies that the roots of f are $\frac{-1 \pm \sqrt{-p}}{2}$, and the result follows.

If $p \equiv 1 \pmod 4$, then $\alpha\beta = \frac{p-1}{4}$, and the quadratic formula implies that the roots of f are $\frac{-1 \pm \sqrt{p}}{2}$, and the result follows.

(2) (a) Prove that if g is a group for which $g^2 = 1$ for all $g \in G$, then G is abelian.

(b) Prove that the only non-abelian groups of order 8 are the quaternion group, Q_8, and D_4.

Answer. (a) *Let $g, h \in G$. Then $ghgh = (gh)^2 = 1$. This implies that $gh = h^{-1}g^{-1}$, but $g = g^{-1}$ and $h = h^{-1}$, hence $gh = hg$.*

(b) *Let G be non-abelian of order 8. By (a), G must have an element g of order 4. Then $N = \langle g \rangle$ is of index 2 in G and hence is normal. Suppose there exists $h \in G \setminus N$ with $h^2 = 1$. Write $H = \langle h \rangle$ and notice that $G = N \rtimes \theta H$. The group H can only act on N in two possible ways: either θ is trivial, $G = N \times H$ and G is abelian, or else θ is non-trivial and $hgh^{-1} = g^{-1}$, in which case G is dihedral.*

Thus we may assume that if $h \in G \setminus N$, then h is of order 4 (note that it cannot be of order 8, else G is abelian). Now $hgh^{-1} \neq g$, else G would be abelian, thus $hgh^{-1} = g^{-1}$. This equation completely specifies the group multiplication table for G (why?), and since Q_8 is non-abelian of order 8 and is not dihedral, we conclude that $G = Q_8$.

(3) Let $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $E = M\left[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right]$.
   (a) Show that M is Galois over $\mathbb{Q}$ with Galois group the 4-group $C_2 \times C_2$.
   (b) Show that E is Galois over $\mathbb{Q}$ with Galois group Q_8.

Answer. (a) *M is the splitting field of $(X^2-2)(X^2-3)$ and so $M : \mathbb{Q}$ is a Galois extension of degree 4. One can verify that the following are the non-trivial maps in* $\mathrm{Gal}(M/\mathbb{Q})$*, and they are all of order 2:*

$$\begin{aligned}\theta_1 :&\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\\ \theta_2 :&\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\ \theta_3 :&\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

Observe that

$$\left(X-\sqrt{(-\sqrt{2}+2)(\sqrt{3}+3)}\right)\left(X-\sqrt{(-\sqrt{2}+2)(-\sqrt{3}+3)}\right)\left(X-\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right)\times$$
$$\left(X-\sqrt{(\sqrt{2}+2)(-\sqrt{3}+3)}\right)\left(X+\sqrt{(-\sqrt{2}+2)(\sqrt{3}+3)}\right)\left(X+\sqrt{(-\sqrt{2}+2)(-\sqrt{3}+3)}\right)\times$$
$$\left(X+\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right)\left(X+\sqrt{(\sqrt{2}+2)(-\sqrt{3}+3)}\right)$$

is equal to

$$f = X^8 - 24X^6 + 144X^4 - 288X^2 + 144.$$

Then E is the splitting field of f over $\mathbb{Q}$ (why?), and so $E : \mathbb{Q}$ is Galois.

Now, to see that $\mathrm{Gal}(E/\mathbb{Q})$ *is the quaternion group, one can check that all but two of its elements are of order 4. (There are various ways of doing this.)*

(4) Let G be the Galois group of $f(X) = X^4 - 2$ over $\mathbb{Q}$. Thus if θ is the positive fourth root of 2, then G is the Galois group of $\mathbb{K} : \mathbb{Q}$ where $\mathbb{K} = \mathbb{Q}(\theta, i)$.
   (a) Describe all 8 automorphisms in G.
   (b) Show that G is isomorphic to the dihedral group D_4.
   (c) The group G has two normal subgroups N_1 and N_2 that are of order 4 and are not cyclic. Write down the elements of N_1 and N_2 and verify that the corresponding fixed fields, $\mathbb{K}^{N_1}$ and $\mathbb{K}^{N_2}$, are normal extensions of $\mathbb{Q}$.

Answer. *We do (a) and (b) in one go, making use of* *http://math.stackexchange.com/questions/1231921/galois-group-of-x4-2.* *Since $L = \mathbb{Q}(\sqrt[4]{2})$ is real of degree 4, we see that K is a proper extension of L, and since* $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ *we see the total degree of the extension is $2 \cdot 4 = 8$. But then we have that* $\mathrm{Gal}\,(K/\mathbb{Q}) \leq S_4$ *is a subgroup of S_4 of order 8. This implies it is a Sylow-2 subgroup of S_4, all of which are isomorphic–by the second Sylow theorem. We know that D_8, the dihedral group of order 8, is such a subgroup, so that gives the isomorphism type.*
But then you know what to look for as explicit representations go, you note that relative to the ordering

$$\alpha_j = i^j \sqrt[4]{2}, 1 \leq j \leq 4$$

we have the 4-cycle (1234) *given by the automorphism*

$$\begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ i \mapsto i \end{cases}$$

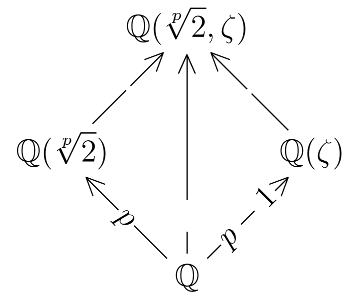
which is enough to totally determine it, since those are generators of the extension. Clearly also

$$\begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases}$$

is represented by the transposition (13)*, and these two generate the group, so give you everything you need for a fully explicit description.*
(Note, by the way, that the four roots of X^4-2 *form a square on the complex plane, and the action of the Galois group on these roots, corresponds exactly to the action of* D_4 *on the plane.)*
For (c), we can take N_1 *to be generated by rotation by* π *in this square, along with reflection in the diagonals. One obtains that* $\mathbb{K}^{N_1}=\mathbb{Q}[\sqrt{2}]$*. On the other hand, we can take* N_2 *to be generated by rotation by* π*, along with reflection in a line connecting two opposite edge mid-points. We obtain that* $\mathbb{K}^{N_2}=\mathbb{Q}[\sqrt{-2}]$*.*

(5) In this question we generalize Example 3.22 from the notes. Let $f=X^p-2\in\mathbb{Q}[x]$ (where p is a prime), and let E be the splitting field of f over $\mathbb{Q}$.
 (a) Prove that f is irreducible.
 (b) Prove that $[E:\mathbb{Q}]=p(p-1)$.
 (c) Prove that $\mathrm{Gal}(E/\mathbb{Q})$ has a normal subgroup N of order p, and calculate E^N.
 (d) Write down a subgroup $H\leq \mathrm{Gal}(E,\mathbb{Q})$ of order $p-1$.
 (e) Prove that $\mathrm{Gal}(E/\mathbb{Q})=N\rtimes H$, and describe the action of H on N.

Answer. (a) *Use Eisenstein.*
 (b) *Observe that* E *contains* $\alpha=\zeta\sqrt[p]{2}$ *where* ζ *is a primitive* p*-th root of unity. By taking powers of* α*, we can conclude that* E *contains* ζ *and* $\sqrt[p]{2}$*. Thus we have the following inclusions, with indexes included.*



Now one knows that $|E:\mathbb{Q}\leq p(p-1)$ *(why?), and the fact that* p *and* $p-1$ *are coprime implies (by multiplicity of degrees) that* $|E:\mathbb{Q}|=p(p-1)$*.*
 (c) *The Fundamental Theorem of Galois Theory implies that it is sufficient to prove that there is an intermediate field* $\mathbb{Q}\subset M\subset E$ *with* M *normal over* $\mathbb{Q}$ *and* $|E:M|=p$*. For this take* $M=\mathbb{Q}(\zeta)$*.*
 (d) *Again, we invoke FTGT: take the field* $M_1=\mathbb{Q}(\sqrt[p]{2})$*. Then* $H=\mathrm{Gal}(E/M_1)$ *is a subgroup of* $\mathrm{Gal}(E,\mathbb{Q})$ *of order* $p-1$*.*
 (e) *Since* $|H|$ *and* $|N|$ *are coprime and* $|H|\cdot|N|=\mathrm{Gal}(E/\mathbb{Q})$*, we see immediately that* $\mathrm{Gal}(E/\mathbb{Q})=N\rtimes H$*. The action of* H *on* N *is isomorphic to the action of* $(\mathbb{Z}/p\mathbb{Z})^\times$ *on* $(\mathbb{Z}/p\mathbb{Z})^+$ *(although I'm not going to prove that here – one can follow the same method as described in lectures).*

(6) Describe the Galois groups of $f=X^6-1$ and X^6+1 over $\mathbb{Q}$. Write down the lattice of fields/ groups for each polynomial, identifying which inclusions are normal.

Answer. *The splitting field of* X^6-1 *is* $\mathbb{Q}[\zeta]$ *where* $\zeta=e^{2\pi i/6}$*. Since* ζ *is a root of* X^2+X+1*, the Galois group of* X^6-1 *is of degree 2, and the lattice of fields is easy.*
 Similarly the splitting field of X^6+1 *is* $\mathbb{Q}[\eta]$ *where* $\zeta=e^{2\pi i/12}$*. Since* ζ *is a root of* X^4-X^2+1*, the Galois group of* X^6-1 *is of degree 4; the Galois group is isomorphic to* $C_2\times C_2$ *(just observe that every non-trivial automorphism has order 2), and so there are three intermediate fields,* $\mathbb{Q}[i]$*,* $\mathbb{Q}[e^{\pi/3}$ *and* $\mathbb{Q}(\zeta+\zeta^{-1})=\mathbb{Q}(\sqrt{3})$*. Since the Galois group is abelian, all inclusions are normal.*

(7) The complex numbers $i\sqrt{3}$ and $1+i\sqrt{3}$ are roots of the quartic $f=X^4-2X^3+7X^2-6X+12$. Does there exist an automorphism σ of the splitting field extension for f over $\mathbb{Q}$ with $\sigma(i\sqrt{3})=1+i\sqrt{3}$?

Answer. *No. You can see this in two different ways. Observe first that* $i\sqrt{3}$ *has minimal polynomial* X^2+3, *while* $1+i\sqrt{3}$ *does not (in particular, the two listed roots are roots of* **different** *irreducible factors of* f*).*

Alternatively, notice that if such an automorphism σ *did exist, then* $\sigma^k(i\sqrt{3}) = k + i\sqrt{3}$, *and so* σ *would be of infinite order, which is impossible.*

(8) Describe the transitive subgroups of S_3, S_4 and S_5.

Answer. S_3*:* A_3 *and* S_3.
S_4*:* A_4, S_4, V *(an elementary abelian group of order 4),* C_4 *(three of these),* D_4 *(three of these).*
S_5*:* A_5, S_5, D_5 *(three of these),* C_5 *(three of these),* $C_5 \rtimes C_4$ *(three of these).*

(9) Find the Galois group of X^4-2 over (a) $\mathbb{F}_3$, (b), $\mathbb{F}_7$. (You calculated the Galois group of X^4-2 over $\mathbb{Q}$ in question (4).)

Answer. *For this answer and the next it is convenient to know how to check if a polynomial of form* X^4+e *is irreducible. If it is divisible by a linear factor, then there is a root, so this can be checked directly. To check for quadratic factors, we suppose that*

$$(X^2+aX+b)(X^2+cX+d) = X^4+e.$$

Multiplying out and equating coefficients, we obtain that one of the following holds (provided the field characteristic is not 2):

- $a=c=0$ *and* $b=-d$;
- $a=-c$ *and* $b=-d=\frac{a^2}{2}$.

With this in mind, we proceed to the question itself:

(a) *Over* $\mathbb{F}_3$, *and using the calculations above, we find that*

$$X^4-2 = (X^2+X+2)(X^2+2X+2).$$

Note that both of the quadratic factors are irreducible. Let α *be a root of* X^2+X+2. *Now observe that* 2α *is a root of* X^2+2X+2. *Thus* $\mathbb{F}_3[\alpha]$ *is the splitting field of* X^4-2, *and since* α *has a minimum polynomial of degree 2, we have* $|\mathbb{F}_3[\alpha]:F_3| = 2$. *Thus the Galois group of* f *over* $\mathbb{F}_3$ *is of order 2: it is* C_2.

(b) *Over* $\mathbb{F}_7$, *we have the following factorization into irreducibles:*

$$X^4-2 = (X-2)(X+2)(X^2+4).$$

Thus to get a splitting field we need only adjoin a root of X^2+4. *As before, the Galois group is* C_2.

(10) Find the Galois group of X^4+2 over (a) $\mathbb{Q}$, (b) $\mathbb{F}_3$, (c), $\mathbb{F}_5$.

Answer. (a) *The roots of* X^4+2 *are* $\zeta^i\sqrt[4]{2}$ *where* ζ *is a primitive 8-th root of unity, and* $i=1,3,5,7$. *Thus the splitting field of* X^4+2 *over* $\mathbb{Q}$ *is* $\mathbb{Q}(\zeta, i)$, *and the analysis now proceeds very similarly to question (4), so I will not repeat it. Note that the roots of* f *are, again, a square in the complex plane (but this time edges are at an angle of* $\pi/4$ *with the axes) and, unsurprisingly, one obtains that the Galois group is* D_4.

(b) *Over* $\mathbb{F}_3$, *we have the following factorization into irreducibles:*

$$X^4+2 = (X-1)(X+1)(X^2+1).$$

We need only adjoin a root of X^2+1 *thus the Galois group is* C_2.

(c) *Over* $\mathbb{F}_5$, *we find that* $f = X^4+2$ *does not have a root and (using the calculations from the previous answer), it also fails to factorize into quadratics. Hence it is irreducible. Let* α *be a root of* f. *Then* α, 2α, 3α *and* 4α *are all roots and we have*

$$f = (X-\alpha)(X-2\alpha)(X-3\alpha)(X-4\alpha).$$

Thus the splitting field of f *is* $\mathbb{F}_3[\alpha]$, *which has degree 4 over* $\mathbb{F}_5$. *What is more the map*

$$\theta : \mathbb{F}_3[\alpha] \to \mathbb{F}_3[\alpha], \quad \alpha \mapsto 2\alpha$$

generates the whole Galois group, and so the Galois group is cyclic: it is C_4.

Remark*: It turns out that Galois groups of polynomials over finite fields are always cyclic. This will be proved later on.*

(11) **(Optional extra)** Suppose that $L : K$ is an extension with $[L : K] = 2$, that every element of L has a square root in L, that every polynomial of odd degree in $K[X]$ has a root in K and that $\text{char}K \neq 2$. Let f be an irreducible polynomial in $K[X]$, let $M : L$ be a splitting field extension for f over L, Let $G = \text{Gal}(M : K)$ and let $H = \text{Gal}(M : L)$.

- (a) By considering the fixed field of a Sylow 2-subgroup of G, show that $|G| = 2^n$.
- (b) By considering a subgroup of index 2 in H, show that if $n > 1$ then there is an irreducible quadratic in $L[X]$.
- (c) Show that L is algebraically closed.
- (d) Show that the complex numbers are algebraically closed.

Answer not supplied for this.

(12) **(Optional extra)** By considering the splitting field of all polynomials of odd degree over $\mathbb{F}_2$, show that the condition $\text{char}K \neq 2$ cannot be dropped from the previous question.

Answer not supplied for this.