GALOIS THEORY
Solutions to Worksheet 7

A 1. Long division (for example) of $f(X)$ by $X-\alpha$ yields:

$$f(X) = (X-\alpha)\Big(X^2+\alpha X + (-3+\alpha^2)\Big) \in L[X]$$

The quadratic formula for $g(X)$ needs the square root of

$$\Delta = b^2-4ac = \alpha^2 - 4(-3+\alpha^2) = 12-3\alpha^2$$

which is explicitly shown to be a square in the hint.

[*Note*: if $\mathrm{char}(K)=3$, then $f(X)=X^3+1=(X+1)(X^2-X+1)$ is not irreducible.]

A 2. It is easy to see that (ii) implies (i) and here I focus on proving that (i) implies (ii).

The key thing to understand is this: **Claim** If $\mathrm{char}(K)\neq 2$ then every extension $K\subset L$ of degree $[L:K]=2$ is of the form $L=K(\alpha)$ for some $\alpha\in L$ such that $\alpha^2\in K$. I am going to leave out the proof of the Claim (hint: quadratic formula) and I will use it to answer the question.

So assume (i), then by the tower law $[L:E]=2$ and $[E:K]=2$ and by the Claim $L=E(\alpha)$ for some $\alpha\in L$ with $\alpha^2\in E$. Also $E=K(\beta)$ where $\beta^2\in K$. Hence we can write $\alpha^2=u+v\beta$ with $u,v\in K$, so

$$(\alpha^2-u)^2 = v^2\beta^2\in K$$

hence α is a root of the polynomial

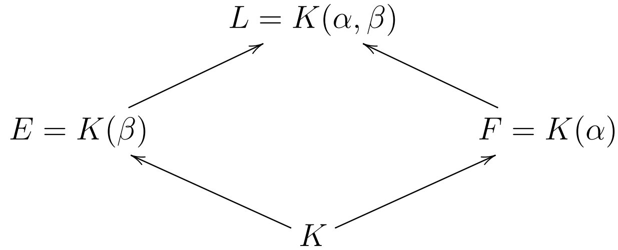
$$f(X) = (X^2-u)^2 - v^2\beta^2 = X^4-2uX^2+(u^2-v^2\beta^2)\in K[X]$$

which is of the required form. If $f(X)\in K[X]$ is irreducible then we are done.

So what if $f(X)$ is not irreducible? This is *really awkward*! In that case by the tower law $[K(\alpha):K]=2$ and the minimal polynomial of α over K is a quadratic polynomial

$$X^2+cX+d\in K[X]$$

and necessarily $c=0$, otherwise $\alpha=\frac{-\alpha^2-d}{c}\in E$, a contradiction. Hence in fact $\alpha^2\in K$ and we have extensions:



where $\beta^2 = b \in K$ and $\alpha^2 = a \in K$ BUT also, clearly, $\alpha \notin K(\beta)$ and $\beta \notin K(\alpha)$.

Remark there is a third field, $G = K(\alpha\beta)$, *distinct* from E, F, and also of degree $[G : K] = 2$. Note also that $(\alpha\beta)^2 = ab \in K$. (I leave all this to you to sort out.)

I now want to work with the element $\alpha + \beta \in L$: I claim that it has degree 4 over K, and then $L = K(\alpha + \beta)$ and, since

$$(\alpha + \beta)^2 = a + b + 2\alpha\beta \in G, \tag{1}$$

the argument above shows that the minimal polynomial of $\alpha + \beta$ has the required form.

Suppose for a contradiction that $\alpha + \beta$ satisfies a quadratic polynomial

$$X^2 + AX + B \in K[X]$$

If $A = 0$ then we have that $(\alpha + \beta)^2 = -B \in K$, and this implies (by Equation 1) that $\alpha\beta \in K$, a contradiction. If $A \neq 0$ then $\alpha + \beta = \frac{-(\alpha+\beta)^2 - B}{A} \in G$ (Equation 1 again) and the polynomial

$$g(X) = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$$

is in $G[X]$. This polynomial is irreducible, otherwise its roots α, β already belong to G, so $L = G$ and we get a contradiction in too many ways (for instance $[L : K] = [G : K] = 2$). But then $g(X)$ equals $X^2 - a$, the minimal polynomial of α over $K[X]$, and this then leads to a contradiction in too many ways (for instance it implies that $\alpha = -\beta$).

A 3. (i) $a > 1$ so a has a prime divisor p; now use Eisenstein. Or use uniqueness of factorization to prove $\sqrt{a} \notin \mathbb{Q}$.

Next, if $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ then write $\sqrt{b} = x + y\sqrt{a}$; square, and use the fact that $\sqrt{a}$ is irrational to deduce that $2xy = 0$. Hence either $y = 0$ (contradiction, as $\sqrt{b} \notin \mathbb{Q}$) or $x = 0$ (contradiction, as we can write $ab = cd^2$ with c squarefree, and $a \neq b$ so $c \neq 1$, and again $\sqrt{c} \notin \mathbb{Q}$).

(ii) $F = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ and the preceding part, plus the tower law, shows that $[F : \mathbb{Q}] = 4$. Now F is a splitting field in characteristic zero, so it's finite, normal and separable. By the fundamental theorem, the Galois group G of $\mathbb{Q} \subset F$ must be a finite group of order 4, so it's either C_4 or $C_2 \times C_2$. There are lots of ways of seeing that it is actually $C_2 \times C_2$. Here are two that spring to mind: firstly, C_4 only has one subgroup of order 2, whereas F has at least two subfields of degree 2 over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, so by the correspondence in the fundamental theorem, C_4 is ruled out. And another way: if we set $K = \mathbb{Q}(\sqrt{a})$ then F/K is normal and separable and $[F : K] = 2$, so $K \subset F$ is cyclic of order 2 by the fundamental theorem, and the Galois group permutes the roots of $X^2 - b$. We deduce that there must be an element of this Galois group, and thus a field automorphism g_a of F, that sends $+\sqrt{b}$ to $-\sqrt{b}$ and fixes $\sqrt{a}$ (as it fixes K). Similarly there's an automorphism g_b of F that sends $+\sqrt{a}$ to $-\sqrt{a}$ and fixes $\sqrt{b}$. This gives us two elements of order 2 in G, which must then be $C_2 \times C_2$. Of course their product, $g_a g_b$, sends $\sqrt{a}$ to $-\sqrt{a}$ and $\sqrt{b}$ to $-\sqrt{b}$, so it fixes $\sqrt{ab}$ and is the third non-trivial element of G.

The subgroups of $C_2 \times C_2$ are: the subgroup of order 1 (corresponding to F), the group itself, of order 4 (corresponding to $\mathbb{Q}$) (both of these because the Galois correspondence is order-reversing, so i.e. sends the biggest things to the smallest things and vice-versa), and then there are three subgroups of order 2, corresponding to $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. One way to see this for sure is, for example, that g_a fixes $\sqrt{a}$, so the subfield corresponding to $\langle g_a \rangle$ definitely contains $\sqrt{a}$, but has degree 2 over $\mathbb{Q}$ by the tower law and so must be $\mathbb{Q}(\sqrt{a})$. Arguing like this will show everything rigorously.

Finally, all of the subfields are normal over $\mathbb{Q}$, because all subgroups of the Galois group are normal (as it's abelian).

(iii) Every element of G sends $\sqrt{a}+\sqrt{b}$ to something else! (for example g_a sends it to $\sqrt{a}-\sqrt{b}$). So the subgroup of G corresponding to $\mathbb{Q}(\sqrt{a}+\sqrt{b})$ must be the identity, which corresponds to F, and so $F=\mathbb{Q}(\sqrt{a}+\sqrt{b})$.

(iv) If $\sqrt{r}\in\mathbb{Q}(\sqrt{p},\sqrt{q})$ then $\mathbb{Q}(\sqrt{r})$ must be one of the quadratic subfields of $\mathbb{Q}(\sqrt{p},\sqrt{q})$, and hence it must be either $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ or $\mathbb{Q}(\sqrt{pq})$ by part (ii). But by part (i) $\sqrt{r}$ is not in any of these fields!

(v) $[F:\mathbb{Q}(\sqrt{p},\sqrt{q})]$ must be 2 (as it isn't 1) and now use the tower law. To determine the Galois group G, note first that any element of the G will be determined by what it does to $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$, and of course for all $n\in\mathbb{Q}$ $\sqrt{n}$ must be sent to $\pm\sqrt{n}$, so there are at most eight possibilities for G, corresponding to the $8=2^3$ choices we have for the signs. However we know the size of G is eight, so all eight possibilities must occur and the group must be $C_2\times C_2\times C_2$.

Let me stress here, for want of a better place, that you *cannot* just say "clearly $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$ are "independent" so we can move them around as we please" – one really has to come up with some sort of an argument to prove that there really is a field automorphism of F sending, for example, $\sqrt{p}$ to $-\sqrt{p}$, $\sqrt{q}$ to $+\sqrt{q}$ and $\sqrt{r}$ to $-\sqrt{r}$. You can build it explicitly from explicit elements you can write down in the Galois group using degree 4 subfields, or you can get it via the counting argument I just explained, but you *can't* just say "it's obvious" because Galois theory is offering you precisely the framework to make the arguments rigorous and I don't think it is obvious without this framework.

(vi) Think of the Galois group as a 3-dimensional vector space over the field with two elements. There are seven 1-dimensional subspaces (each cyclic of order 2 and generated by the seven non-trivial elements), and there are also seven 2-dimensional subspaces, by arguing for example on the dual vector space – or by arguing that any subgroup of order 4 of $C_2\times C_2\times C_2$ is the kernel of a group homomorphism to C_2 and such a homomorphism is determined by where the three generators go; there are eight choices, one of which gives the trivial homomorphism and the other seven of which give order 4 subgroups.

Hence other than F and $\mathbb{Q}$ there are 14 fields; seven have degree 2 and seven have degree 4. The degree 2 ones are $\mathbb{Q}(\sqrt{p^aq^br^c})$ as a,b,c each run through 0 and 1, but not all zero. The degree 4 ones are $\mathbb{Q}(\sqrt{p^aq^br^c},\sqrt{p^dq^er^f})$ as $(a,b,c),(d,e,f)$ run through bases of the seven 2-dimensional subspaces of the Galois group considered as a vector space of dimension 3 over the field with 2 elements.

(vii) We know all seven non-trivial elements of the Galois group, and none of them fix $\sqrt{p}+\sqrt{q}+\sqrt{r}$ (because if you think of it as a real number, they all send it to something strictly smaller), so the subgroup corresponding to $\mathbb{Q}(\sqrt{p}+\sqrt{q}+\sqrt{r})$ is trivial and we're home.

(viii) Induction and the argument in (v) gives the degree; considering possibilities of signs gives that the Galois group is what you think it is, acting how you think it acts, and the last part again follows by observing that $\mathbb{Q}(\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n})$ corresponds to the trivial subgroup.

A 4. (i) We know $X^p - 1 = (X-1)(1+X+X^2+\cdots+X^{p-1})$, and $f(X) = 1+X+X^2+\cdots+X^{p-1}$ is irreducible over $\mathbb{Q}$ (by Eisenstein after a coordinate change). Hence if $\zeta = e^{2\pi\,\mathtt{i}/p}$ then $f(X)$ must be the min poly of ζ. Note that the roots of $p(X)$ are just the roots of $X^p - 1$ other than $X = 1$, so they're ζ^j for $1 \le j \le p-1$. Moreover if $F = \mathbb{Q}(\zeta)$ then $[F : \mathbb{Q}] = \deg(f) = p-1$, and K contains ζ^j for all j, so $X^p - 1$ splits completely in K. Hence K is the splitting field of $X^p - 1$ and it has degree $p - 1$.

Now $\mathbb{Q} \subset F$ is finite, normal and separable, so the fundamental theorem applies, so we know that the Galois group G will have size $p - 1$. If $\tau \in G$ then, because $F = \mathbb{Q}(\zeta)$, τ is determined by $\tau(\zeta)$, which is a root of $\tau(f) = f$, so is ζ^j for some $1 \le j \le p-1$. It's perhaps not immediately clear that, given j, some field automorphism τ of F sending ζ to ζ^j will exist – but it has to exist because we know there are $p-1$ field automorphisms. So the elements of the Galois group can be called τ_j for $1 \le j \le p-1$. The remaining question is what this group is. We can figure out the group law thus: $\tau_i \circ \tau_j$ – where does this send ζ? Well $\tau_j(\zeta) = \zeta^j$, and $\tau_i(\zeta) = \zeta^i$ so $\tau_i(\zeta^j) = \zeta^{ij}$ as τ_i is a field homomorphism. Note finally that ζ^{ij} only depends on ij mod p, as $\zeta^p = 1$. So if we identify G with $\{1, 2, \ldots, p-1\}$ then the group law is just "multiplication mod p" , and we see $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

(I write = because our isomorphism — which seemed to depend on a choice of ζ, our pth root of unity — is in fact independent of that choice, so G is *canonically* isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. The notation in mathematics for a canonical isomorphism is "=", so we can write $G = (\mathbb{Z}/p\mathbb{Z})^\times$ in this situation.) This concludes part (i).

For Part (ii), you need to know that, in fact, $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ is always a cyclic group[1] and hence it has a unique subgroup of index 2: the fixed field of that subgroup is the field K that you are looking for.

Part (iii) is really easy.

For Part (iv): first ,when $p = 3$, $K = F$ and hence $K = \mathbb{Q}(\sqrt{-3})$.

When $p = 5$, I claim that $K = \mathbb{Q}(\sqrt{5})$. Indeed from part (i) $G = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, -2, -1\}$. It is clear that $H = \{1, -1\} \subset G$ has index 2 and that $K = H^\star$ in the notation of the Galois correspondence. Writing as in Part (i) $\zeta = e^{\frac{2\pi\,\mathtt{i}}{5}}$, it is clear that

$$\alpha = \zeta + \frac{1}{\zeta} \in H^\star$$

and it is reasonable to guess $K = \mathbb{Q}(\alpha)$. It is easy to finish from here:

$$\alpha^2 + \alpha - 1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

hence $\alpha = \frac{-1+\sqrt{5}}{2}$ and from this we conclude that $K = \mathbb{Q}(\sqrt{5})$.

Part (v). For p general, writing as above $\zeta = e^{\frac{2\pi\mathtt{i}}{p}}$, and denoting by $H \le (\mathbb{Z}/p\mathbb{Z})^\times$ the unique subgroup of index 2, we want to evaluate something like

$$\sum_{h \in H} h(\zeta)$$

[1] This is a non-completely trivial fact. In general, every finite subgroup of the multiplicative group of a field is cyclic. I don't normally like to prove this result — sometimes I give it as a worksheet question — but I encourage you to look it up.

because this thing being the average over all of H is manifestly H-invariant. The next observation is that H is the image of the "squaring homomorphism"

$$(\mathbb{Z}/p\mathbb{Z})^\times \ni k \mapsto k^2 \in (\mathbb{Z}/p\mathbb{Z})^\times$$

so we are led to evaluating:

$$\alpha = \sum_{k=0}^{\frac{p-1}{2}} e^{\frac{2\pi i k^2}{p}}$$

You can find this thing in number theory books under the name of "quadratic Gauss sum" and the upshot is

$$K = \begin{cases} \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \bmod 4 \\ \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \bmod 4 \end{cases}$$

(The exact evaluation of the Gauss sum is a bit tricky, but you may be able to evaluate it up to sign, and this is enough to determine K. This, however, is a number theory question, not a Galois theory question.)

A 5. (a) Well $z^3 = \omega^3\alpha^3 = 1 \times 2 = 2$ so z is a root of $X^3 - 2 = 0$, which is irreducible over $\mathbb{Q}$ because it has no root in $\mathbb{Q}$, so $X^3 - 2$ is the min poly of z, and by what we did in class this means $[\mathbb{Q}(z) : \mathbb{Q}] = 3$. Although we don't need it, we can note that in fact $\mathbb{Q}(z)$ is isomorphic to, but not equal to, $\mathbb{Q}(\alpha)$, as an abstract field.

(b) We know $\omega^3 = 1$ but $\omega \neq 1$ so ω is a root of $(X^3 - 1)/(X - 1) = X^2 + X + 1$. This polynomial is irreducible as it has no rational (because no real) roots, so $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Note also while we're here that solving the quadratic gives $\omega = \frac{-1+i\sqrt{3}}{2}$ (plus sign because the imaginary part of ω is positive; the other root is ω^2).

(c) We have $\alpha \in \mathbb{R}$. Furthermore $\overline{\omega}$ is another cube root of 1 so it must be ω^2. Hence $\overline{z} = \overline{\omega\alpha} = \omega^2\alpha = \omega z$. In particular if $\overline{z} \in \mathbb{Q}(z)$ then $\omega = \overline{z}/z \in \mathbb{Q}(z)$. This means $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(z)$, and by the first two parts and the tower law we deduce $[\mathbb{Q}(z) : \mathbb{Q}(\omega)] = \frac{3}{2}$, which is nonsense because the dimension of a (finite-dimensional) vector space is an integer.

(d) If $x \in \mathbb{Q}(z)$ then $\overline{z} = -z + 2x \in \mathbb{Q}(z)$, contradiction. So x is not in. If $i \in \mathbb{Q}(z)$ then $\mathbb{Q}(i) \subseteq \mathbb{Q}(z)$ and this contradicts the tower law like in part(c). Finally because the imaginary part of ω is $\sqrt{3}/2$ we see $y = \alpha\sqrt{3}/2$, so if $y \in \mathbb{Q}(\omega)$ then $y^3 = 3\alpha^3/8\sqrt{3} = 3/4\sqrt{3} \in \mathbb{Q}(z)$, implying $\sqrt{3} \in \mathbb{Q}(z)$ which again contradicts the tower law.

A 6. You really have to do it yourself if you want to understand what is going on. Let me tell you what is going on. Let $\psi\colon \mathbb{Z}[y_1, \dots, y_n] \to R = \mathbb{Z}[x_1, \dots, x_n]^{\mathfrak{S}_n}$ be the homomorphism defined in (c); that is, $\psi(y_i)$ is the i^{th} elementary symmetric polynomial $\sigma_i(x_1, \dots, x_n)$.

(a, b) The largest monomial in σ_i is $x_1 \cdots x_i$; therefore

$$\psi(y_1^{c_1} \cdots y_n^{c_n}) = x_1^{c_1+\dots+c_n} x_2^{c_2+\dots+c_n} \cdots x_n^{c_n} + \text{l.o.t.}$$

where"l.o.t." stands for (strictly) *lower order terms*. To prove the surjectivity of ψ, let $f = f(x_1, \dots, x_n) \in R$ be a symmetric polynomial; f has a highest monomial $x_1^{k_1} \cdots x_n^{k_n}$.

Because f is symmetric, $k_1 \geq k_2 \geq \cdots \geq k_n$. Writing $k_i - k_{i+1} = c_i$, we have that $\psi(y_1^{c_1} \cdots y_n^{c_n})$ and f have the same highest monomial; therefore for some nonzero constant λ

$$f = \psi(\lambda y_1^{c_1} \cdots y_n^{c_n}) + \text{l.o.t.}$$

where the lower order term is also a symmetric polynomial and we may assume by induction that it is in the image of ψ. Thus f also is in the image of ψ.

(c) To prove that ψ is injective we apply the same method to show that $\text{Ker}(\psi) = (0)$. The hint suggests to work with a particular ordering on the monomials in $\mathbb{Z}[y_1, \ldots, y_n]$ that is defined there. The important property, which I leave to you to verify is: If $y_1^{c_1} \cdots y_n^{c_n} > y_1^{c_1'} \cdots y_n^{c_n'}$, then the leading monomial of $\psi(y_1^{c_1} \cdots y_n^{c_n})$ (measured with the good old ordering of monomials in $x_1, \ldots, x_n$) is strictly larger than the leading monomial of $\psi(y_1^{c_1'} \cdots y_n^{c_n'})$. Suppose now that a polynomial $f(y_1, \ldots, y_n)$ is in the kernel of ψ. Assume that $f \neq 0$, then f has a monomial of highest order and we can write (for some nonzero constant λ):

$$f = \lambda y_1^{c_1} \cdots y_n^{c_n} + \text{l.o.t.}$$

Then by what we just said

$$\psi(f) = \lambda x_1^{c_1 + \cdots + c_n} x_2^{c_2 + \cdots + c_n} \cdots x_n^{c_n} + \text{l.o.t.}$$

and this, if you think about it, means that $\psi(f) \neq 0$. We have shown that $f \neq 0$ implies $\psi(f) \neq 0$.