Summaries, May 10 and 12

Recall that from now on our fields are assumed to have characteristic zero.

Let K be an extension of a field F. The Galois group $G(K/F)$ is the group of F-automorphisms of K. A splitting field K of a polynomial $f(x)$ with coefficients in F is also called a Galois extension of F.

We have seen that if K is a Galois extension, then the order of the Galois group is equal to the degree of the extension: $|G(K/F)| = [K : F]$.

It is also true that, for any finite field extension K/F,
$|G(K/F)| \leq [K : F]$, and that if $|G(K/F)| = [K : F]$, then K is a Galois extension of F. However, we didn't go over this in class.

We have also seen that, if G is a finite group of automorphisms of a field K and $F = K^G$ is the fixed field, then $[K : F] = |G|$. Therefore K is a Galois extension of F.

Corollary 1. If K/F is a Galois extension and G is its Galois group, then F is the fixed field K^G.

This is true because, by definition of an F-automorphism, $F \subset K^G$. Then the formula $[K : F] = [K : K^G][K^G : F]$ shows that $[K^G : F] = 1$, and therefore $F = K^G$. □

adjoining square roots

Any field extension K/F of degree two is a splitting field, and it can be obtained by adjoining a square root. If α is in K and not in F, then $F \subset F[\alpha] \subset K$, and by counting degrees, one sees that α has degree 2 over F and that $F[\alpha] = K$. If α is a root of the quadratic polynomial $f(x) = x^2 + bx + c$ and D is the discriminant $b^2 - 4c$, then $F[\alpha] = F[\delta]$, where $\delta = \sqrt{D}$.

Now let F be the field of rational numbers, and let $K = F[\alpha, \beta]$, be the field obtained by adjoining two sqaure roots to F. We'll use $\alpha = \sqrt{3}$ and $\beta = \sqrt{5}$ as an example. Then β isn't in the field $F[\alpha]$. It has degree 2 over that field, and $[K : F] = 4$.

We ask: Are there other square roots in K?

Of course, a number such as $7^2\alpha$ shouldn't be considered different. We should really ask for other field extensions of degree 2 that are contained in K. The field $F[\gamma]$, where $\gamma = \alpha\beta = \sqrt{15}$ is an example of another such field.

The elements $1, \alpha, \beta, \gamma$ form a basis for K over F. So to find all square roots algebraically, one would take a combination $\delta = d + a\alpha + b\beta + c\gamma$ of this basis, and find a, b, c, d such that δ^2 is in F. This leads to the equations

$$ad + 5bc = 0, \quad bd + 3ac = 0, \quad cd + ab = 0$$

I've never tried to solve these equations, because there is a much easier method, which is to look at the Galois group.

The field K is the splitting field of the polynomial $f(x) = (x^2 - 3)(x^2 - 5)$ over F, so it is a Galois extension, and the Galois group G has order $[K : F] = 4$. Since α^2 is in F, an element σ of G must send α to $\pm\alpha$, and similarly, it must send β to $\pm\beta$. And, when we know the images of α and β, σ is determined. Thus the four elements of G are $1, \sigma, \tau, \sigma\tau$, where

$$\sigma(\alpha) = -\alpha, \quad \sigma(\beta) = \beta$$
$$\tau(\alpha) = \alpha), \quad \tau(\beta) = -\beta$$
$$\sigma\tau(\alpha) = -\alpha, \quad \sigma\tau(\beta = -\beta$$

Since $\sigma^2 = \tau^2 = 1$, G is the product $C_2 \times C_2$ of cyclic groups of order 2.

Now suppose that $\delta = \sqrt{d}$ is in K, with d an element of F that isn't a square in F, and let $L = K[\delta]$. Then $[L : F] = 2$, and since $F \subset L \subset K$, $[K : F] = 2$. Also, K is a splitting field over L. Let its Galois group (of order 2) be H. Since $F \subset L$, an L-automorphism of K is also an F-automorphism, so $H \subset G$. Therefore L is the fixed field K^H of the subgroup H of G oforder 2.

There are three subgroups of $G(K/F)$ of order 2. They are generated by the three elements of order 2 in G, which are σ, τ, and $\sigma\tau$. Therefore K contains three fields of degree 2 over F, and they are $F[\alpha], F[\beta]$ and $F[\alpha\beta]$. There are no others.

cubic equations

Let K be a splitting field over F of an irreducible polynomial $f(x) = x^3 - a_1qx^2 + a_2x - a_3$ in $F[x]$ of degree 3, and let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f in K, listed in an arbitrary order. We form a tower of fields:

$$F \subset F[\alpha_1] = F_1 \subset F[\alpha_1, \alpha_2] = F_2 \subset F[\alpha_1, \alpha_2, \alpha_3] = K$$

Since f is an irreducible cubic polynomial in $F[x]$, the degree $[F_1 : F]$ is 3. Next, $f(x)$ has a root α_1 in F_1. so in $F_1[x]$, $f(x) = (x - \alpha_1)q(x)$ for some quadratic polynomial $q(x)$ in $F_1[x]$ whose roots are α_2, α_3. That polynomial may be irreducible in $F_1[x]$ or not. If it is reducible, then α_2 and α_3 are in F_1, so $F_1 = F_2 = K$, and $[K : F] = 3$. On the other hand, if $q(x)$ is an irreducible element of $F_2[x]$, then $[F_2 : F_1] = 2$ and $[K : F] = 6$. In any case, the third root α_3 will be in F_2, one reason being that the sum of the roots is the quadratic coefficient a_1 of f. It is in F, and $\alpha_3 = a_1 - \alpha_1 - \alpha_2$. Summing up, the splitting field K will have degree either 3 or 6 over F.

The Galois group $G = G(K/F)$ operates on the roots α_i, and then because $K = F[\alpha_1, \alpha_2, \alpha_3]$, an element σ of G that fixes every one of the roots will be the identity automorphism. So G operates *faithfully* on the roots, and by that operation, it becomes a subgroup of the symmetric group S_3. Since we know that $|G| = [K : F]$, we will have $G = S_3$ if $[K : F] = 6$, and $G = A_3$ if $[K : F] = 3$. The alternating group A_3 is the only subgroup of S_3 of order 3.

How can we tell which of these two possibilities we have in a particular case?

Recall that the discriminant of f is the product $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ of the squares of the differences of the roots. The discriminant is an element of F. Its square root $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ is an element of K. If δ isn't in F, then K contains a quadratic extension $F[\delta]$ of F, and the degree $[K : F]$ is divisible by 2. Therefore $[K : F] = 6$ if δ isn't in F.

Next, you will be able to check that a permutation σ of the roots multiplies δ by the sign of that permutation. Therefore, if δ is an element of F, then an F-automorphism of K must be an even permutation. In that case, $G = A_3$ and $[K : F] = 3$. So the element δ determines the degree $[K : F]$ and the Galois group $G(K/F)$.

intermediate fields

Let K/F be a Galois extension. An *intermediate field* L is a field extension of F that is contained in K: $F \subset L \subset K$. As we see in the cases discussed above, the intermediate fields are useful tools for determining the structure of the extension. The Main Theorem describes these fields:

Main Theorem. Let K/F be a Galois extension with Galois group G. There is a bijective correspondence between intermediate fields and subgroups of G. If H is a subgroup of G, the corresponding intermediate field is the fixed field K^H, and if L is an intermediate field, the corresponding subgroup is the Galois pgroup $G(K/L)$. If a subgroup H corresponds to the intermediate field L, then the degree $[K : L]$ is equal to the index $[G : H]$ of H in G, and the degree $[L : F]$ is the order of H.

proof We must show two things:

• If H is the Galois group $G(K/L)$ of an intermediate field L, then L is its fixed field K^H.

• If L is the fixed field K^H of a subgroup H of G, then H is the Galois group $G(K/L)$.

Both are easy. If K is a splitting field over F of a polynomial $f(x)$ in $F[x]$, then it is also a splitting field for the smae polynomial over an intermediate field L. Therefore K/L is a Galois extension, and $|G(K/L)| = [K : L]$.

Let L be an intermediate field, and let $H = G(K/L)$. Since K is a Galois extension of L, L is the fiexed field of H

Let H be a subgroup and let L be the fixed field K^H. Every element of H fixes L, so it is an L-automorphism of K. Therefore $H \subset G(K/L)$. By the Fixed field Theorem, $[K : L] = |H|$. Therefore $|H| = |G(K/L)|$, which shows that $H = G(K/L)$. □

Let's exhibit the correspondence in the case that K is a splitting field of an irreducible cubic polynomial and $[K : F] = 6$. So the Galois group is the symmetric group

$$G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

with the usual relations $\sigma^3 = 1$, $\tau^2 = 1$, and $\tau\sigma = \sigma^2\tau$. Let's say that $\sigma = (1\,2\,3)$ and $\tau = (2\,3)$.

There are four proper subgroups, all cyclic: $< \sigma >, < \tau >, < \sigma\tau >$, and $< \sigma^2\tau >$. Therefore there are exactly four intermediate fields in addition to F and K. They are $F[\delta], F[\alpha_1], F[\alpha_2]$, and $F[\alpha_3]$. In the correspondence between subgroups and intermediate fields, $< \sigma >$ corresponds to $F[\delta]$ and $< \tau >$ corresponds to $F[\alpha_1]$.

Proposition 1. Let K be a splitting field of a polynomial $f(x)$ in $F[x]$, let G be the Galois group $G(K/F)$, and let $\alpha_1, ..., \alpha_n$ be the roots of f in K. Then G operates on the set of roots.
(i) The operation of G on the roots of f is faithful: if an element σ of G fixes every root, then σ is the identity. Therefore the operation on the roots embeds G as a subgroup of the symmetric group S_n.
(ii) If $f(x)$ is an irreducible polynmoial in $F[x]$, then the operation is transitive: Fpor every $i = 1, ..., n$, there is an element σ in G such that $\sigma(\alpha_1) = \alpha_i$.

proof (i) If an F-automorphism σ of K fixes every root, then because K is generated by the roots, σ is the identity.
(ii) We must show that the roots form a G-orbit. Say that we have an orbit of order k. We number the roots so that the orbit is $\alpha_1, ..., \alpha_k$. The coefficients of the polynomial $g(x) = (x - \alpha_1) \cdots (x - \alpha_k)$ with these roots are symmetric functions in the orbit, so they are invariant, which means that g has coefficients in F. If f is irreducible, it generates the ideal of all polynomials with roots α_1, so f divides g, and therefore $f = g$. □

quartic equations

Let K be an splitting field of an irreducible quartic polynomial $f(x) = x^4 - a_1x^3 + a_2x^2 - a_3x + a_4$ in $F[x]$, and let G be the Galois group of K/F. According to the proposition, G embeds as a transitive subgroup of S_4. Therefore its order is divisible by 4, and of course $|G|$ divides $|S_4| = 24$. The order can be $4, 8, 12$ or 24.

The transitive subgroups of S_4 are: S_4, A_4, D_4, C_4, D_2, and they have orders $24, 12, 8, 4, 4$, respectively. We form a tower of field extensions:

$$F \overset{4}{\subset} F[\alpha_1] \overset{\leq 3}{\subset} F[\alpha_1, \alpha_2] \overset{\leq 2}{\subset} F[\alpha_1, \alpha_2, \alpha_3] = K$$

The degrees of the field extensions are given above the $\subset$ symbols. The last root α_4 is in the field $F[\alpha_1, \alpha_2, \alpha_3]$ because the sum of the roots is a coefficient of f, and is in F.

How can we decide, in a given case, which group is the Galois group? The first thing is to look at the discriminant D of f. (Of course we don't want to compute the discriminant unless it is absolutely necessary.) Let

$$\delta = \sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4)$$

Lemma 1. With notation as above, $\delta \in F$ if and only if the Galois group G is a subgroup of the alternating group A_4.

The proof is similar to the proof for cubic equations.

Next, one can use Lagrange's *resolvent cubic* to determine whether or not G contains an element of order 3. Let

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

These are all of the elements that are sums of products of the roots α_i. Therefore they form an S_4-orbit. The coefficients of the polynomial

$$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3) = x^3 - b_1x^2 + b_2x - b_3$$

are symmetric functions in α_i, so they are in the field F. For example, b_2, the sum of the roots β_i is the symmetic function $s_2(\alpha)$, which is the coefficient a_2 of x^2 in f. It isn't hard to determine the other coefficients in terms of the symmetric functions $s_i(\alpha) = a_i$. You can do this as an exercise.

One happy accident is that the discriminant of g is equal to the discriminant of f, from which it follows that the discriminant of g isn't zero. The discriminant of f isn't zero because f is irreducible, but g may be reducible. The discriminant of g is $(\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2$. Using the following computation, it is easy to check that the two dicriminants are the same:

$$(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) = \alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4 = \beta_1 - \beta_2$$

Proposition 2. Let g bethe resolveny cubic of an irreducible polynomial f in $F[x]$ of degree 4, and let K be a splitting field for f over F.
(i) If the resolvent cubic g is irreducible over F, then $G = S_4$ or A_4.
(ii) If g has one root in F, then G is either D_4 or C_4.
(iii) If g has three roots in F, then G is D_2.

We ran out of time for the proof, but it is simple:

proof The resolvent cubic g has roots in a splitting field. If g is irreducible, its roots will have degree 3 over F, and therefore $[K : F]$ will be divisible by 3. Then $G = S_4$ or A_4.

With variable u_1, u_2, u_3, u_4, let $w_1 = u_1u_2 + u_3u_4$, $w_2 = u_1u_3 + u_2u_4$, and $w_3 = u_1u_4 + u_2u_3$. The symmetric group S_4, operating on the set $\{u_i\}$ permutes w_1, w_2, w_3, and the permutations that fix all three of these three elements form the group D_2 whose elements are $(1), (12)(34), (13)(24), (14)(23)$. Therefore, $\beta_1, \beta_2, \beta_3$ are all in F, if and only if G is that dihedral group. The remaining possibility is that g has just one root in F. Then $G \neq S_4, A_4, D_2$, so $G = D_4$ or C_4. □

adjoining two square roots in succession

We consider an element $\alpha = \sqrt{r + s\sqrt{t}}$ with r, s, t in F. To find its irreducible polynomial $f(x)$ over F, one way is to guess the other roots. Here, we guess that $\alpha' = \sqrt{r - s\sqrt{t}}$ is also a root of f, and then $-\alpha$ and $-\alpha'$ might also be roots. We expand the polynomial

$$f(x) = (x - \alpha)(x - \alpha')(x + \alpha)(x + \alpha') = (x^2 - \alpha^2)(x^2 - \alpha'^2) = (x^2 - (r + s\sqrt{t}))(x^2 - (r - s\sqrt{t})) =$$

$$= (x^2 - r)^2 - s^2t = x^4 - 2rx^2 + (r^2 - s^2t)$$

If this polynomial is irreducible, it will be the irreducible polynomial for α over F, and the splitting field will be $K = F[\alpha, \alpha']$.

Let's take for example $F = \mathbb{Q}$ and $\alpha = \sqrt{2 + 3\sqrt{5}}$. Then $\alpha' = \sqrt{2 - 3\sqrt{5}}$, and $f(x) = x^4 - 4x^2 - 41$. This polynomial is irreducible over F, as expected, so it is the irreducible polynomial for α over F. Then $[F[\alpha] : F] = 4$. Since $2 + 3\sqrt{5}$ is positive, α is real, and since $2 - 3\sqrt{5}$ is negative, α' is complex. Therefore $\alpha' \notin F[\alpha]$. On the other hand, $\sqrt{5}$ is in $F[\alpha]$. Therefore α' has degree 2 over $F[\alpha]$, and since $K = F[\alpha, \alpha']$, $[K : F] = 8$. So the Galois group of K/F has order 8. It is the dihedral group D_4.

It is possible that the polynomial $f(x)$ of degree 4 is reducible. This happens for example when $\alpha = \sqrt{1 + 2\sqrt{2}}$. Computing as above, one finds that $f(x) = x^4 - 6x^2 + 1$, which factors:

$$x^4 - 6x^2 + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1)$$

This reflects the fact that $\sqrt{1 + 2\sqrt{2}} = 1 + \sqrt{2}$:

$$(1 + \sqrt{2})^2 = 1 + 2\sqrt{2} + 2 = 3 + 2\sqrt{2}$$

Howver, for most choices of r, s, t, the Galois group of $\alpha = \sqrt{r + s\sqrt{t}}$ tends to be the dihedral group.

One more example. Let $\alpha = \sqrt{5 + \sqrt{5}}$, $\alpha' = \sqrt{5 - \sqrt{5}}$. Proceeding as above,

$$f(x) = (x - \alpha)(x - \alpha')(x + \alpha)(x + \alpha') = x^4 - 10x^2 + 20$$

which is irreducible over $F = \mathbb{Q}$, by the Eisenstein Criterion. In this case, $\alpha\alpha' = \sqrt{20} = 2\sqrt{5}$. Therefore, since $\sqrt{5}$ is in the field $F[\alpha]$, so is α'. Then $K = F[\alpha]$ and $[K : F] = 4$. The Galois group G of K/F operates transitively on the roots of f, so there is an element σ in G such that $\sigma(\alpha) = \alpha'$. Then $\sigma(5 + \sqrt{5}) = \sigma(\alpha^2) = \alpha'^2 = 5 - \sqrt{5}$, and $\sigma(\sqrt{5}) = -\sqrt{5}$. Therefore $\sigma(\alpha\alpha') = \sigma(2\sqrt{5}) = -2\sqrt{5} = -\sigma(\alpha\alpha')$. Since $\sigma(\alpha) = \alpha')$, we must have $\sigma(\alpha') = -\alpha$. Then when the roots are listed in the order $\alpha, \alpha', -\alpha, -\alpha'$, $\sigma = (1\,2\,3\,4)$. The Galois group G is the cyclic group of order 4.

roots of unity

Let $F = \mathbb{Q}$. Let p be a prime, and let ζ be the pth root of unity $e^{2\pi i/p}$. The irreducible polynomial for ζ over F is $f(x) = x^{p-1} + \cdots + x + 1 = (x^p - 1)/(x - 1)$. It was proved that this polynomial is irreducible using the Eisenstein Criterion. The roots of f are the powers $\zeta, \zeta^2, ..., \zeta^{p-1}$, so the splitting field K is generated over F by ζ, and $[K : F] = p - 1$.

Proposition 3. **(i)** The Galois group G of K/F is isomorphic to the multiplicative group $\mathbb{F}_p^\times$ of nonzero integers modulo p.
(ii) G is a cyclic group.

proof The group G operates transitively on the roots of f. Let σ_i, $i = 1, ..., p-1$, be the elements such that $\sigma_i(\zeta) = \zeta^i$. The fact that $G \approx \mathbb{F}_p^\times$ follows from this equation, in which indices are to be read modulo p:

$$\sigma_i\sigma_j(\zeta) = \sigma_i(\zeta^j) = \zeta^{ij}$$

Then G is cyclic because $\mathbb{F}_p^\times$ is cyclic. We're supposed to know that. □

A generator for the cyclic group $\mathbb{F}_p^\times$ called a *primitive root* modulo p, but which residue classes are primitive roots is a mystery. When $p = 5$, 2 is a primitive root. Its powers run through the nonzero residue classes in this order: $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1$. (We won't bother to put bars over the residue classes.) However, 2 isn't a primitive root moduulo 7, because $2^3 \equiv 1$ modulo 7. Instead, 3 is a primitive root modulo 7: $3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$. The primitive root isn't unique: 5 is also a primitive root modulo 7.

Let $p = 7$, and let σ be the element of G such that $\sigma(\zeta) = \zeta^3$. The powers of the primitive root 3 runs through the nonzero classes modulo 7 in the order listed above, and σ runs through the roots of $f(x)$ in the corresponding order:

$$\sigma : \zeta^1 \to \zeta^3 \to \zeta^2 \to \zeta^6 \to \zeta^4 \to \zeta^5 \to \zeta^1$$

Next, 2 is a primitive root modulo 11. Its powers modulo 11, listed, in order, are $1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$. 8, 7, and 6 are also primitive roots modulo 11.

We go back to the case $p = 7$, in which G is a cyclic group of order 6 generated by the element σ described above. This group has two proper subgroups: $H =< \sigma^2 >$, and $N =< \sigma^3 >$. So there are just two intermediate fields K^H and K^N properly between F and the splitting field K. Since H has order 3, the degree $[K : K^H]$ is 3, and since $[K : F] = 6$, $[K^H : F] = 2$. To determine the fixed field, we look at the orbit of σ^2, operatng on the powers of ζ. The element σ^2 runs through the powers in the order shown above. Therefore σ^2 operates as

$$\zeta \to \zeta^2 \to \zeta^4 \to \zeta \quad \text{and} \quad \zeta^3 \to \zeta^6 \to \zeta^5 \to \zeta^3$$

Let α be the sum over the first orbit: $\alpha = \zeta + \zeta^2 + \zeta^4$and let $\alpha' = \zeta^3 + \zeta^6 + \zeta^5$. These elements are roots of a quadratic polynomial: $\alpha + \alpha'$ is the sum of all powers of 3, which is the negative of the cofficient 1 of x^{p-2} in $f(x)$: $\alpha + \alpha' = -1$. Next, to compute $\alpha\alpha'$ we must multiply the three terms making up α by those making up α'. There will be a large number of occurences of the symbol ζ. So we use a shorthand notation. Let $[1, 2, 4]$ denote the sum $\zeta + \zeta^2 + \zeta^4$. Then $\alpha = [1, 2, 4]$. Similarly, $\alpha' = [3, 6, 5]$. These are the exponents, so when we multiply, we must add them, modulo 7. For example, $[1][3, 6, 5] = [4, 0, 6]$. Then

$$\alpha\alpha' = [1, 2, 4][3, 6, 5] = [4, 0, 6, 5, 1, 0, 0, 3, 2]$$

Here 0 stands for $\zeta^0 = 1$. Besides the zeros, right side of the equation is the sum of all powers of ζ different from 1, which is -1. So the right side is $-1 + 3 = 2$: $\alpha\alpha' = 2$. The irreducible equation for α ovr F is $x^2 + x + 2$. Its roots α, α' are $\frac{1}{2}(1 \pm \sqrt{-7})$. Looking at the roots of unity on the unit circle, one sees that the imaginary part of α is positive. So the sign is $+$ for α and $-$ for α'. Since $[K^H : F] = 2$, $K = f[\alpha] = F[\sqrt{-7}]$.

The fixed field H^N of the subgroup $N =< \sigma^2 >$ can be determined in the same way. We take ths sums of every third power of ζ in the list of power of 3. Let $\beta_1 = [1, 6]$, $\beta_2 = [3, 4]$, and $\beta_3 = [2, 5]$. These elements are roots of a cubic polynomial. Here $\beta_1 + \beta_2 + \beta_3 = -1$. Next $\beta_1\beta_2 = [4, 5, 2, 3]$. We don't get any zeros here. The second symmeric function $s_2(\beta) = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$ is a sum of 12 products. This sum must include every nonzero class twice. So $s_2(\beta) = -2$. Finally, since we have computed $\beta_1\beta_2$, $\beta_1\beta_2\beta_3 = [4, 5, 2, 3][2, 5] = [6, 2, 0, 3, 4, 0, 5, 1] = 1 + 1 - 1 = 1$. The irreducible polynomial for β_i over F is $x^3 + x^2 - 2x + 1$.