Lecture 12: digression on algebraic integers.

1) Basics.

2) Sums & products of algebraic integers.

Refs: Sec 5.2 in [E], Sec 9.5 in [V].

1) Basics.

In Section 3 of Lec 11 we have mentioned some results on character values that require algebraic integers. The goal of this lecture is to provide necessary background.

Our base field is $\mathbb{C}$.

1.1) Main definitions.

Definition 1: Let $z \in \mathbb{C}$. We say that z is an algebraic number (resp., algebraic integer) if $\exists$ a monic (leading coefficient 1) polynomial $f(x) \in \mathbb{Q}[x]$ (resp. $f(x) \in \mathbb{Z}[x]$) s.t. $f(z)=0$.

Example 1: 0) Every algebraic integer is an algebraic number.

1) If $z \in \mathbb{Q}$ (resp., $z \in \mathbb{Z}$), then z is an algebraic number (resp. algebraic integer).

2) Every root of unity is an algebraic integer.

Notation: $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$ are sets of algebraic integers & algebraic numbers.

Definition 2: • By the minimal polynomial of $z \in \overline{\mathbb{Q}}$ we mean the (unique) minimal degree ($\Leftrightarrow$ irreducible in $\mathbb{Q}[x]$) monic polynomial $f \in \mathbb{Q}[z]$ w. $f(z) = 0$.

• The roots of the minimal polynomial of z are called conjugates of z.

Example 2: Let z be a primitive nth root of 1. It's minimal polynomial is the cyclotomic polynomial φ_n defined inductively $\varphi_1 = x - 1$ & $\prod_{d|n} \varphi_d = x^n - 1$ (e.g. $\varphi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$; $\varphi_4(x) = x^2 + 1$). The conjugates of z are precisely the primitive nth roots of 1.

Lemma: The minimal polynomial of $z \in \overline{\mathbb{Z}}$ is in $\mathbb{Z}[x]$. In particular, all conjugates of z are algebraic integers.

Proof: Let f be an irreducible monic polynomial in $\mathbb{Z}[x]$ w. $f(z)=0$. Then f is irreducible in $\mathbb{Q}[x]$ (Eisenstein criterion), hence is the minimal polynomial $\square$

Corollary: $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Exercise: 1) Let $\alpha \in \overline{\mathbb{Q}}$, and $f(x) \in \mathbb{Q}[x]$ satisfy $f(\alpha)=0$. Then f is divisible by the minimal polynomial of α.

2) Let $\alpha \in \overline{\mathbb{Q}}$, $a \in \mathbb{Q}$. If $\alpha_1, \dots \alpha_k$ are all conjugates of α, then $a\alpha_1, \dots, a\alpha_k$ are all conjugates of $a\alpha$.

1.2) Equivalent characterization of algebraic integers.

Proposition: for $z \in \mathbb{C}$ TFAE

(a) z is an algebraic integer,

(b) $\mathrm{Span}_{\mathbb{Z}}(z^i \mid i \geq 0)$ is a finitely generated abelian group.

Proof:

(a) $\Rightarrow$ (b): Assume (a) holds $\iff \exists\, n>0,\ a_0,\dots a_{n-1}\in\mathbb{Z}$ s.t.
$z^n=\sum_{i=0}^{n-1}a_i z^i \Rightarrow z^{n+k}=\sum_{i=k}^{n+k-1}a_i z^{i+k}\Rightarrow \mathrm{Span}_{\mathbb{Z}}(z^i\,|\,i\geq 0)=$
$\mathrm{Span}_{\mathbb{Z}}(z^i\,|\,0\leq i\leq n-1)$ – finitely generated $\Rightarrow$ (b).

(b) $\Rightarrow$ (a): Let $f_1,\dots f_k\in\mathbb{Z}[x]$ be s.t. the elements $f_1(z),\dots,f_k(z)$ span $\mathrm{Span}_{\mathbb{Z}}(z^i)$. Then if $d=\max_i \deg f_i$, then $1,z,\dots,z^d$ span $\mathrm{Span}_{\mathbb{Z}}(z^i)$. In particular, $z^{d+1}=\sum_{i=0}^{d}a_i z^i$ for some $i=0,\dots,d$, which is (a) $\square$

We will also need the following fact:

Fact: Every subgroup, Γ' in a finitely generated abelian group Γ is finitely generated.

Proof (when Γ is torsion-free – the only case we need)
By the classification of finitely generated abelian groups, $\Gamma\simeq\mathbb{Z}^k$ for some k. The base, $k=1$, is left as an exercise

(hint: GCD!). Suppose now that we know the claim for all subgroups of $\mathbb{Z}^\ell$ w. $\ell < k$. Consider $\mathbb{Z}^{k-1} = \{(z_1, \dots z_{k-1}, 0)\} \subset \mathbb{Z}^k$. By induction, $\mathbb{Z}^{k-1} \cap \Gamma'$ is finitely generated, say by elements $f_1, \dots f_m$. Next,

$$\Gamma'/(\Gamma' \cap \mathbb{Z}^{k-1}) = (\Gamma' + \mathbb{Z}^{k-1})/\mathbb{Z}^{k-1} \hookrightarrow \mathbb{Z}^k/\mathbb{Z}^{k-1} \xrightarrow{\sim} \mathbb{Z}.$$

Let $\bar{g}_1, \dots \bar{g}_p$ be generators of $\Gamma'/(\Gamma' \cap \mathbb{Z}^{k-1})$ and let g_i be a preimage of $\bar{g}_i$ in Γ'. Then $f_1, \dots f_m, g_1, \dots, g_p$ generate Γ', left as an exercise $\square$

2) Sums & products of algebraic integers.

Our goal in this section is to prove the following:

Proposition: Let $\alpha, \beta \in \overline{\mathbb{Z}}$. Then:

1) $\alpha + \beta, \alpha\beta \in \overline{\mathbb{Z}}$

2) any conjugate of $\alpha + \beta$ is of the form $\alpha' + \beta'$, where α' is a conjugate of α, and β' is a conjugate of β.

The analog of 2) holds also for products.

2.1) Digression^2: symmetric polynomials.

Our proof of Proposition is based on the fundamental theorem about symmetric polynomials.

Let R be a commutative (associative unital) ring. An element $f \in R[x_1,\dots,x_n]$ is called symmetric if it doesn't change under any permutation of the variables.

Example: elementary symmetric polynomial $e_k = \sum_{i_1<\dots<i_k} x_{i_1}\dots x_{i_k}$ whose important property is

$$\prod_{i=1}^{n}(z-x_i) = z^n - e_1 z^{n-1} + e_2 z^{n-2} + \dots + (-1)^n e_n \in \mathbb{Z}[z, x_1, \dots x_n].$$

Note that symmetric polynomials form an R-subalgebra in $R[x_1,\dots x_n]$ to be denoted by $R[x_1,\dots,x_n]^{S_n}$ (this is indeed the subalgebra of invariants for the S_n-action by permutation of variables).

Here's a basic result known as the fundamental theorem of symmetric polynomials, see Sec 3.8 in [V].

Thm: Every symmetric polynomial can be uniquely written as a polynomial in the elementary symmetric polynomials e_i, $i=1,2,\dots,n$.

Here is an application to the proof of Proposition in Sec 2. Let $x_1,\dots x_n$, $x_1',\dots x_m'$ be two collections of variables and let $e_1,\dots,e_n$ & $e_1',\dots e_m'$ be the elementary symmetric polynomials in these variables. Consider the expression:

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(z-x_i-x_j') \in \mathbb{Z}[z,x_1,\dots,x_n,x_1',\dots,x_m'] \qquad (1)$$

Lemma: For each i, the coefficient, F_i, of z^i in (1) (a priori, an element of $\mathbb{Z}[x_1,\dots,x_n,x_1',\dots x_m']$) is a polynomial in $e_1,\dots,e_n,e_1',\dots,e_m'$ w. coeff's in $\mathbb{Z}$.

Proof: Let $R_1=\mathbb{Z}[x_1,\dots,x_n]$ and view F_i as an element of $R_1[x_1',\dots,x_m']$. Note that (1) doesn't change under permuting $x_1',\dots x_m'$ - so, neither does F_i. So $F_i\in R_1[x_1',\dots x_m']^{S_m} =$ [Thm for R_1] $R_1[\sigma_1',\dots,\sigma_m'] = \mathbb{Z}[x_1,\dots x_n,\sigma_1',\dots \sigma_m']$.

Now let $R_2 = \mathbb{Z}[\sigma_1', \dots, \sigma_m']$. Since (1) is also S_n-invariant, so is F_i viewed as an element of $R_2[x_1, \dots, x_n]$. So by Thm, applied to R_2, we see that $F_i \in R_2[\sigma_1, \dots, \sigma_n] = \mathbb{Z}[\sigma_1, \dots, \sigma_n, \sigma_1', \dots, \sigma_m']$ $\square$

We can also consider

$$\prod_{i=1}^{n} \prod_{j=1}^{m} (z - x_i x_j') \in \mathbb{Z}[z, x_1, \dots, x_n, x_1', \dots, x_m'] \qquad (2)$$

The coefficients of z^i are again in $\mathbb{Z}[\sigma_1, \dots, \sigma_n, \sigma_1', \dots, \sigma_m']$.

2.2) Proof of Proposition.

We will prove 2) & the part of 1) about the sum.

Let $f, g \in \mathbb{Z}[x]$ be the minimal polynomials of α, β, respectively.

$f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \dots + (-1)^n a_n$, $g(x) = x^m - b_1 x^{m-1} + b_2 x^{m-2} - \dots + (-1)^m b_m$, $a_i, b_j \in \mathbb{Z}$.

Let $\alpha_1 = \alpha, \dots \alpha_n$, be the conjugates of α so that $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$, and $\beta_1 = \beta, \beta_2, \dots, \beta_m$ be the conjugates of β so that $g(x) = \prod_{j=1}^{m} (x - \beta_j)$.

Consider the polynomial $h(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i - \beta_j) \in \mathbb{C}[x]$. If we know that the coefficients are in $\mathbb{Z}$ we are done: $h(x)$ has $\alpha + \beta$ as a root and it's monic, so $\alpha + \beta \in \mathbb{Z}$. And $h(x)$ is divisible by the minimal polynomial of $\alpha + \beta$ (Exercise in Sec 1.1). So every conjugate of $\alpha + \beta$ is a root of h, hence $\alpha_i + \beta_j$.

So we need to show $h(x) \in \mathbb{Z}[x]$. But note that $h(x) = x^{mn} + F_{mn-1}(\alpha_1, \dots \alpha_n, \beta_1, \dots, \beta_m) x^{mn-1} + \dots + F_0(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$, where $F(x_1, \dots x_n, x_1', \dots, x_m') \in \mathbb{Z}[x_1, \dots x_n, x_1', \dots x_m']$. By Lemma in the previous section, F is a polynomial of $e_1, \dots, e_n, e_1', \dots, e_m'$ w. integral coefficients.

So $F_i(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ is a polynomial w. integral coefficients evaluated at $a_i = e_i(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ & $b_j = e_j'(\beta_1, \dots, \beta_m) \in \mathbb{Z}$. So $F_i(\alpha_1, \dots \alpha_n, \beta_1, \dots, \beta_m) \in \mathbb{Z}$, finishing the proof for sums

To show $\alpha\beta \in \overline{\mathbb{Z}}$ we use the direct analog of Lemma for (2) $\square$

Remark: By Proposition, $\overline{\mathbb{Z}}$ is a subring of $\mathbb{C}$. And one can also show that $\overline{\mathbb{Q}} \subset \mathbb{C}$ is a subfield.