Modern Algebra 2 (MATH 6140)
HANDOUT 6 (April 14, 2008)

GALOIS CONNECTIONS

Let S and T be classes, and let $R \subseteq S \times T$ be a relation. For each subset $U \subseteq S$ define

$$U^\perp = U^R := \{t \in T \mid \forall u \in U((u,t) \in R)\}$$

and for each $V \subseteq T$ define

$$V^\perp = {}^R V := \{s \in S \mid \forall v \in V((s,v) \in R)\}.$$

These are two mappings, $\perp\colon \mathcal{P}(S) \to \mathcal{P}(T)$ and $\perp\colon \mathcal{P}(T) \to \mathcal{P}(S)$. It is immediate from the definition of $\perp$ that:

Lemma 1. $U \times V \subseteq R \iff U \subseteq V^\perp \iff V \subseteq U^\perp$.

The last bi-implication in Lemma 1 motivates the following definition.

Definition 2. (Galois connection) A *Galois connection (GC)* between classes S and T is a pair of mappings $\perp\colon \mathcal{P}(S) \to \mathcal{P}(T)$ and $\perp\colon \mathcal{P}(T) \to \mathcal{P}(S)$ such that for all $U \subseteq S$ and $V \subseteq T$ it is the case that $U \subseteq V^\perp \iff V \subseteq U^\perp$. (I usually refer to $U^\perp$ as the *Galois complement* of U.)

Lemma 3. *A Galois connection between S and T arises from a uniquely determined relation in the manner described before Lemma 1.*

Proof. If a GC between S and T arises from a relation $R \subseteq S \times T$, then, according to Lemma 1, $(u,v) \in R$ iff $\{u\} \subseteq \{v\}^\perp$ iff $\{v\} \subseteq \{u\}^\perp$. So, given an arbitrary GC, the natural candidate for the associated relation is $R = \{(u,v) \in S \times T \mid v \in \{u\}^\perp\}$.

To see that the GC induced by this relation R is the same as the starting GC we must show that $U^R = U^\perp$ for all $U \subseteq S$. (Since everything is symmetric so far, the same argument will show ${}^R V = V^\perp$.) Note that R is defined so that the desired statement is true for singleton sets: $\{u\}^R = \{u\}^\perp$. So it suffices to prove that two GC's that agree on singletons are equal.

Claim 4. *For any GC, $(\bigcup U_i)^\perp = \bigcap U_i^\perp$.*

$x \in (\bigcup U_i)^\perp$ iff $\bigcup U_i \subseteq \{x\}^\perp$ iff $\forall i(U_i \subseteq \{x\}^\perp)$ iff $\forall i(x \in U_i^\perp)$ iff $x \in \bigcap U_i^\perp$.

Now, for any $U \subseteq S$ we have $U^R = (\bigcup_{u \in U} \{u\})^R = \bigcap_{u \in U} \{u\}^R = \bigcap_{u \in U} \{u\}^\perp = U^\perp$.

To prove the uniqueness of R, note that if $(u,v) \in R - R'$, then $v \in \{u\}^R - \{u\}^{R'}$, so different relations induce different GC's. □

So a GC is just an alternative way to describe a binary relation.

Theorem 5. *(Properties of GC's) Assume that $U \subseteq V \subseteq S$ and $X \subseteq Y \subseteq T$.*

(1) $\perp$ *reverses inclusions:* $U^\perp \supseteq V^\perp$ *and* $X^\perp \supseteq Y^\perp$.
(2) $\perp\perp$ *is increasing:* $U \subseteq U^{\perp\perp}$ *and* $X \subseteq X^{\perp\perp}$.
(3) $\perp\perp\perp{=}\perp$*:* $U^\perp = U^{\perp\perp\perp}$ *and* $X^\perp = X^{\perp\perp\perp}$.
(4) *The operations*
$$\mathsf{cl} : \mathcal{P}(S) \to \mathcal{P}(S) : U \mapsto U^{\perp\perp}$$
and
$$\mathsf{cl} : \mathcal{P}(T) \to \mathcal{P}(T) : U \mapsto U^{\perp\perp}$$
are closure operators.
(5) *A set is closed if and only if it is in the image of* $\perp$.
(6) *If* $\mathcal{L}_S$ *and* $\mathcal{L}_T$ *are the lattice of closed subsets of* S *and* T*, then* $\perp$ *induces a dual isomorphism* $\partial : \mathcal{L}_S \to \mathcal{L}_T : C \mapsto C^\perp$.

Proof. Item (1) follows from Claim 4 of Lemma 3.

For (2), it follows from the definition of GC that $U \subseteq U^{\perp\perp}$ iff $U^\perp \subseteq U^\perp$, which obviously holds.

For (3), apply $\perp$ to the inclusion in (2) and use (1) to get $U^\perp \supseteq U^{\perp\perp\perp}$. But by part (2) we have $U^\perp \subseteq (U^\perp)^{\perp\perp}$. Hence $U^\perp = U^{\perp\perp\perp}$.

For (4), we have that $\perp\perp$ is extensive from (2). To prove that $\perp\perp$ is isotone we use (1) twice:
$$U \subseteq V \Longrightarrow U^\perp \supseteq V^\perp \Longrightarrow U^{\perp\perp} \subseteq V^{\perp\perp}.$$
For idempotence we $\perp$ the equation from (3) to get
$$U^{\perp\perp} = U^{\perp\perp\perp\perp} = (U^{\perp\perp})^{\perp\perp}.$$

For (5), note that any closed set is in the image of $\perp$, since $U = U^{\perp\perp}$ implies that U is the result of applying $\perp$ to $U^\perp$. Conversely, if $U = W^\perp$, then
$$U^{\perp\perp} = W^{\perp\perp\perp} = W^\perp = U,$$
so U is closed.

(6) follows from (5), (3), and (1). □

If we use the same symbol ∂ for the inverse of the dual isomorphism in Theorem 5 (6), then it is easy to see that the $\perp$-maps are recoverable from ∂ and the closure operators via the formula $\perp = \partial \circ \mathsf{cl}$. This fact suggests that the information encoded in a GC between S and T is equivalent to that encoded in the pair of associated closure operators on S and T and the dual isomorphism between their lattices of closed sets. This suggestion turns out to be true:

Theorem 6. *Given classes* S *and* T *equipped with closure operators (both denoted* cl*) and a dual isomorphism* $\partial\colon \mathcal{L}_S \to \mathcal{L}_T$ *between their lattices of closed sets (with the inverse of* ∂ *also denoted* ∂*), the functions* $\perp = \partial \circ \mathsf{cl}$ *constitute a GC between* S *and* T *whose associated closure operators are* cl *and whose associated dual isomorphisms are* ∂.

The proof is easy, but doesn't fit in the margin.

GC's are of interest in mathematics because they provide a link between something common and easily recognizable — a binary relation — and something that is not always obvious, but of mathematical interest — closure operators. Once one identifies an important binary relation, one is mathematically obligated to discover and prove an internal characterization of the associated closure operators. (That is, describe how to compute $\mathsf{cl}(U)$ without reference to the GC.)

Examples.

(1) Let E be a finite dimensional Euclidean space with inner product $\langle \cdot, \cdot \rangle$. Let $R \subseteq E \times E$ be the relation of orthogonality: $(u, v) \in R$ iff $\langle u, v \rangle = 0$. Then for $U \subseteq E$ the set $U^\perp$ is the orthogonal complement of U, and $U^{\perp\perp}$ is the subspace generated by U.

(2) Let $\mathcal{S}$ be the class of all algebras in the language of groups. Let $\mathcal{T}$ be the collection of all equations in this language. Let R denote the relation of satisfaction. (This means that $(\mathbf{A}, \varepsilon)$ is in R if and only if $\mathbf{A} \models \varepsilon$, which is a way of writing that the algebra $\mathbf{A}$ satisfies the equation ε.)

In this example, $\{(x \cdot (y \cdot z)) = ((x \cdot y) \cdot z), x \cdot 1 = x, x \cdot x^{-1} = 1\}^\perp$ is the class of all groups. More generally, if $\Sigma \subseteq \mathcal{T}$, then $\Sigma^\perp$ is the variety of all algebras axiomatized the equations in Σ.

If $\mathcal{K} \subseteq \mathcal{S}$, then $\mathcal{K}^\perp$ is the set of all equations that hold in all members of $\mathcal{K}$. This set of equations is called *the equational theory of* $\mathcal{K}$.

The lattice of closed subclasses of $\mathcal{S}$ is the lattice of all varieties of algebras defined with operations $\cdot, ^{-1}, 1$. The lattice of closed subsets of $\mathcal{T}$ is the lattice of equational theories in this language. These lattices are dual to each other.

(3) Let S be a set and let G be a group of permutations of S. The relation $R = \{(s, g) \mid g(s) = s\}$ determines a Galois connection between S and G.

If $s \in S$, then $\{s\}^\perp$ is the stabilizer subgroup of s. If $g \in G$, then $\{g\}^\perp$ is the set of fixed points of g.

(4) (The Galois Connection of Galois Theory) Let $\mathbb{F} < \mathbb{E}$ be a finite extension. Let $G = \mathrm{Aut}_{\mathbb{F}}(\mathbb{E}) = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ be the group of all $\mathbb{F}$-algebra automorphisms of $\mathbb{E}$. Let $R \subseteq \mathbb{E} \times G$ be the relation $R = \{(e, g) \mid g(e) = e\}$. This relation determines a Galois connection between $\mathbb{E}$ and G.

Exercises.

(1) Show that a function $\sigma : \mathbb{E} \to \mathbb{E}$ is an $\mathbb{F}$-algebra automorphism iff it is a field automorphism that fixes the elements of $\mathbb{F}$.

(2) Show that any closed subset of $\mathbb{E}$ is a subfield of $\mathbb{E}$ containing $\mathbb{F}$.

(3) Show that any closed subset of G is a subgroup.