Math 562 **Spring 2012**
Homework 6 **Drew Armstrong**

Problems on Galois Connections

Let S, T be sets and let $R \subseteq S \times T$ be a relation (we will write aRb to denote the statement $(a,b) \in R$). For all subsets $A \subseteq S$ and $B \subseteq T$ let us write

$$A^* := \{t \in T : aRt \ \ \forall\, a \in A\} \subseteq T,$$
$$B^* := \{s \in S : sRb \ \ \forall\, b \in B\} \subseteq S,$$

thus defining two functions $* : \wp(S) \to \wp(T)$ and $* : \wp(T) \to \wp(S)$. (Here $\wp(U)$ is the set of subsets of U. The $\wp$ is for "power" set.) We use the symbol $*$ twice for aesthetic reasons; hopefully no confusion will result. Such a pair of maps is called a Galois connection.

1. Prove that for all $A, A' \subseteq S$ and $B, B' \subseteq T$ we have

$$A \subseteq A' \Rightarrow A^* \supseteq A'^* \quad \text{and} \quad B \subseteq B' \Rightarrow B^* \supseteq B'^*.$$

Proof. **Since all of the definitions are symmetric upon interchanging $A \leftrightarrow B$ and $S \leftrightarrow T$, we will only prove the first statement. This applies to the other problems as well.**

Suppose that $A \subseteq A'$ and consider an element $t \in A'^*$. By definition this means that aRt for all $a \in A'$. Then since $A \subseteq A'$ we also have aRt for all $a \in A$, hence $t \in A^*$. We conclude that $A'^* \subseteq A^*$. □

2. Prove that for all $A \subseteq S$ and $B \subseteq T$ we have

$$A \subseteq A^{**} \quad \text{and} \quad B \subseteq B^{**}.$$

Proof. Given $s \in A$, we wish to show that $s \in A^{**}$. Recall that A^* is the set of $t \in T$ such that aRt for all $a \in A$. That is, for all $t \in A^*$ we have aRt for all $a \in A$. In particular, for all $t \in A^*$ we have sRt (since $s \in A$). By definition this means $s \in A^{**}$. □

3. Prove that for all $A \subseteq S$ and $B \subseteq T$ we have

$$A^{***} = A^* \quad \text{and} \quad B^{***} = B^*.$$

Proof. Consider $A \subseteq S$. By Problem 2 we know that $A \subseteq A^{**}$. Then applying Problem 1 gives $A^{***} = (A^{**})^* \subseteq A^*$. On the other hand, applying Problem 2 to $A^* \subseteq T$ gives $A^* \subseteq (A^*)^{**} = A^{***}$. We conclude that $A^{***} = A^*$.

□

Let X be a set. A function $\mathsf{cl} : \wp(U) \to \wp(U)$ is called a closure operator if it satisfies

- $X \subseteq \mathsf{cl}(X)$ for all $X \subseteq U$,
- $X \subseteq Y \Rightarrow \mathsf{cl}(X) \subseteq \mathsf{cl}(Y)$ for all $X, Y \subseteq U$,
- $\mathsf{cl}(\mathsf{cl}(X)) = \mathsf{cl}(X)$ for all $X \subseteq U$.

(I'm sure you've met at least two examples before.)

4. Prove that $** : \wp(S) \to \wp(S)$ and $** : \wp(T) \to \wp(T)$ are closure operators.

Proof. We will show that $** : \wp(S) \to \wp(S)$ is a closure operator. The first closure property is proved by Problem 2: for all $A \subseteq S$ we have $A \subseteq A^{**}$. To show the second closure property, consider $A, A' \subseteq S$. If $A \subseteq A'$, then we apply Problem 1 twice to get $A \subseteq A' \Rightarrow A^* \supseteq A'^* \Rightarrow A^{**} \subseteq A'^{**}$. Finally, let $A \subseteq S$. By applying Problem 3 we find that $(A^{**})^{**} = (A^{***})^* = (A^*)^* = A^{**}$, which proves the third closure property. We conclude that $**$ is a closure operator. □

5. Prove that $* : \wp(S) \to \wp(T)$ and $* : \wp(T) \to \wp(S)$ are inverse (and order-reversing) bijections between the $**$**-closed** subsets of S and the $**$**-closed** subsets of T. (They also preserve the "lattice structure" on closed sets, but you don't need to prove this.)

Proof. If $A \subseteq S$ is closed (i.e. $A = A^{**}$) then Problem 3 implies that $A^* = A^{***} = (A^*)^{**}$, hence A^* is also closed. We conclude that $* : \wp(S) \to \wp(T)$ sends closed sets to closed sets, and by symmetry the same is true for $* : \wp(T) \to \wp(S)$. Next observe that these are inverse maps, since for all closed $A \subseteq S$ and closed $B \subseteq T$ we have $(A^*)^* = A^{**} = A$ and $(B^*)^* = B^{**} = B$. It follows immediately that $* : \wp(S) \to \wp(T)$ and $* : \wp(T) \to \wp(S)$ are bijections between closed sets.

(Here's the part you don't need to show. Given closed sets $A, A' \subseteq S$, note that the intersection $A \cap A'$ is closed. Indeed we know $A \cap A' \subseteq (A \cap A')^{**}$. Then applying $**$ to the inclusions $A \cap A' \subseteq A$ and $A \cap A' \subseteq A'$ gives $(A \cap A')^{**} \subseteq A^{**} = A$ and $(A \cap A')^{**} \subseteq A'^{**} = A'$, hence $(A \cap A')^{**} \subseteq A \cap A'$. We conclude that $(A \cap A')^{**} = A \cap A'$. Given closed $A, A' \subseteq S$ it is not true that $A \cup A'$ is closed, but we can define $A \vee A'$ as the intersection of all closed sets containing $A \cup A'$ (which will be closed). Finally, one should verify that for all closed sets $A, A' \subseteq S$ we have $(A \cap A')^* = A^* \vee A'^*$ and $(A \vee A')^* = A^* \cap A'^*$. Try it if you like.) $\square$

6. Now let $S = K$ be a field and let $T = G$ be a finite group of field automorphisms $G \leq \mathsf{Aut}(K)$. For $a \in K$ and $g \in G$, let aRg mean that $g(a) = a$ (we say g "fixes" a).

(a) Let $F = G^*$. Prove that F is a subfield of K.
(b) For each sub**set** $H \subseteq G$ prove that $F \subseteq H^* \subseteq K$ is an intermediate field.
(c) For each sub**set** $L \subseteq K$ prove that $L^* \subseteq G$ is a subgroup.
(d) Prove that every $**$-closed subset $L \subseteq K$ is an intermediate field $F \subseteq L \subset K$ and every $**$-closed subset $H \subseteq G$ is a subgroup $H \leq G$. (The Fundamental Theorem of Galois Theory says that every intermediate field and every subgroup is $**$-closed. This does not follow from the results of this homework; it requires a careful study of polynomials — cf. everything we did this semester.)

Proof. Given subsets $H \subseteq G$ and $L \subseteq K$ we will use that notations $K^H := H^*$ (the $\mathsf{fixed\ field}$ of H) and $\mathsf{Gal}(K/L) := L^*$ (the $\mathsf{Galois\ group}$ of the extension K/L).

To prove (a), note that G consists of field-automorphisms of K, hence we have $\varphi(1) = 1$ and $\varphi(0) = 0$ for all $\varphi \in G$, which implies that $0, 1 \in F := K^G$. Next, given $a, b \in F$ we have $\varphi(a + b) = \varphi(a) + \varphi(b) = a + b$ and $\varphi(ab) = \varphi(a)\varphi(b) = ab$ for all $\varphi \in G$, hence $a + b, ab \in F$. We conclude that F is a field.

To prove (b), let $H \subseteq G$ be any subset. The same argument used in (a) shows that K^H is a subfield of K. Then we have $F \subseteq K^H$ since if $a \in F$ (i.e. every element of G fixes a), it must be true that every element of $H \leq G$ fixes a, hence $a \in K^H$.

To prove (c), let $L \subseteq K$ be any subset. Note that the identity automorphism is in $\mathsf{Gal}(K/L)$ since it fixes every element of L. If $\varphi, \mu \in \mathsf{Gal}(K/L)$ then $\varphi \circ \mu(a) = \varphi(\mu(a)) = \varphi(a) = a$ for all $a \in L$, hence $\varphi \circ \mu \in \mathsf{Gal}(K/L)$. Furthermore, if $\varphi \in \mathsf{Gal}(K/L)$ (i.e. $\varphi(a) = a$ for all $a \in L$) then applying φ^{-1} gives $a = \varphi^{-1}(a)$ for all $a \in L$, hence $\varphi^{-1} \in \mathsf{Gal}(K/L)$. We conclude that $\mathsf{Gal}(K/L)$ is a subgroup of G.

To prove (d), let $L \subseteq K$ be $**$-closed, i.e. $L^{**} = L$. But then $L = (L^*)^*$ for some $L^* \subseteq G$ and part (b) implies that $F \subseteq L \subseteq K$ is an intermediate field. Similarly, let $H \subseteq G$ be a $**$-closed subset, i.e. $H^{**} = H$. Then $H = (H^*)^*$ for some $H^* \subseteq K$, so part (c) implies that $H \leq G$ is a subgroup. $\square$

Combining Problems 1–6, we have an anti-isomorphism between the lattice of $**$-closed intermediate fields $F \subseteq L \subseteq K$ and the lattice of $**$-closed subgroups $H \leq G$. (But **which** fields/groups are the $**$-closed?) This leads us to

The Fundamental Theorem of Galois Theory. If we define $F := K^G$ (so that the extension K/F is "normal" by definition), then **every** intermediate field $F \subseteq L \subseteq K$ and **every** subgroup $H \leq G$ is $**$-closed. (The theorem also characterizes the normal subgroups of G — it says that $\mathsf{Gal}(K/L) \trianglelefteq \mathsf{Gal}(K/F)$ if and only if L/F is "normal" — but I won't prove that part here.)

For the proof, we will assume the following (Theorem 16.6.4 in the text). Let K/F be a finite field extension with Galois group G. Then the following are equivalent:

- $[K : F] = |G|$,
- $F = K^G$,
- K is a splitting field for some polynomial over F.

If any (hence all) of these is true, we say that the extension K/F is "normal".

Proof. Let $F \subseteq L \subseteq K$ be an intermediate field, and note that we can write $L^{**} = K^{\mathsf{Gal}(K/L)}$. Abstract nonsense (Problems 2 and 6) tells us that $L \subseteq L^{**} \subseteq K$ are field extensions, hence we can apply the Tower Law to get

$$[K : L] = [K : K^{\mathsf{Gal}(K/L)}] \cdot [K^{\mathsf{Gal}(K/L)} : L].$$

Since $F = K^G$ by assumption, we know (from above) that K is a splitting field for some polynomial $f(x) \in F[x]$. But since $f(x) \in F[x] \subseteq L[x]$, this implies that K/L is a splitting field, hence $[K : L] = |\mathsf{Gal}(K/L)|$ (from above). Finally, the Fixed Field Theorem (pg 487) says $[K : K^{\mathsf{Gal}(K/L)}] = |\mathsf{Gal}(K/L)|$, and we conclude that $[K^{\mathsf{Gal}(K/L} : L] = 1$, hence $L = K^{\mathsf{Gal}(K/L)} = L^{**}$, as desired.

Let $H \leq G$ be a subgroup, and note that we can write $H^{**} = \mathsf{Gal}(K/K^H)$. By abstract nonsense (Problems 2 and 6) we know that $H \leq \mathsf{Gal}(K/K^H) \leq G$ are subgroups. Now the Fixed Field Theorem says that $[K : K^H] = |H|$. Finally, since K is a splitting field over F, it must be a splitting field over $K^H \supseteq F$, hence we know (from above) that $|H| = [K : K^H] = |\mathsf{Gal}(K/K^H)|$. It follows that $H = \mathsf{Gal}(K/K^H) = H^{**}$, as desired. □

[A Galois connection is an example of a "functor". The example in Problem 6 was the original Galois connection, but it is certainly not the only one. In fact these creatures are at the heart of several branches of mathematics. (Another prominent example is the Nullstellensatz of algebraic geometry.) A functor is like a bridge between two worlds; once you find one, you never know what magical things will happen.]