Notes on Solvability

Here are some notes on solvability which supplement what is in the book. I probably will only cover the first item in class, but you might as well have the other stuff. There are 4 topics:

1. Herstein's claim about solvability and normal extensions.
2. Solvability without roots of unity.
3. The Vandermonde matrix: a technical prelude.
4. The Converse to the Solvability Theorem.

1. A Claim of Herstein's about Solvability: Let F be an arbitrary field of characteristic 0. We say that a pair (F, F') of fields is a *solvable pair* if there is a finite chain

$$F = F_0 \subset F_1 \subset ... \subset F_n = F'$$

such that $F_{i+1} = F_i(\omega_i)$ where $\omega_i^{r_i} = a_i \in F_i$. Here $i = 0, ..., n-1$.

The polynomial $p(x) \in F(x)$ is *solvable* if there is a solvable pair (F, F') such that F' contains all the roots of p. That is, F' contains the splitting field for p. The following result proves Herstein's claim in the book. This is also the solution to problem 5.7.1.

Theorem 0.1 *Suppose that $p(x) \in F[x]$ is solvable. Then there is a solvable pair (F, F'') such that F'' contains all the roots of p and F'' is a normal extension of F.*

Proof: Let $\omega_1, ..., \omega_n$ be the elements involved in the construction of (F, F'). Since ω_j is algebraic over F, there is some polynomial $P_j(x) \in F[x]$ such that $P_j(\omega_j) = 0$. Define the big polynomial $P = P_1...P_n$ and let E be the splitting field for P over F. Note that $\omega_j \in E$ for all j and also $F \subset E$. Therefore $F_j \subset E$ for all j.

Let $G = G(E, F_0)$ be the Galois group. Define $\widetilde{F}_0 = F_0$. Assuming that $\widetilde{F}_k$ has been defined, let

$$\widetilde{F}_{k+1} = \widetilde{F}_k(\bigcup_{\phi \in G} \phi(\omega_k)).$$

in other words, we are adjoining to $\widetilde{F}_k$ not just the element ω_k but all the images of ω_k under elements of G.

By definition $\phi(\widetilde{F}_0) = \widetilde{F}_0$ for all $\phi \in G$. This is to say that $\widetilde{F}_0$ is G-stable. Assuming that $\widetilde{F}_k$ is G-stable, so is $\widetilde{F}_{k+1}$. So, by induction $\widetilde{F}_n$ is G-stable. But then $\widetilde{F}_n$ is a normal extension of F_0.

At the same time, we can get from $\widetilde{F}_k$ to $\widetilde{F}_{k+1}$ by adjoining the elements one at a time. Since $\omega_k^{r_k} \in \widetilde{F}_k$ the same is true for each $\phi(\omega_k)$. So, when we add the elements one at a time and consider the corresponding tower of fields, we see that $(\widetilde{F}_0, \widetilde{F}_n)$ is a solvable pair. Remembering that $\widetilde{F}_0 = F$ and setting $F'' = \widetilde{F}_n$, we are done. ♠

2: Roots of Unity Not Necessary: Let F be a field of characteristic 0. Let $p(x) \in F[x]$ be a polynomial which is solvable by radicals. Herstein proves that the Galois group of $p(x)$ is solvable, assuming the side-condition that F contains all n-th roots of unity. Here we eliminate the side condition.

The proof in Herstein only uses finitely many roots of unity. Let's say that the proof uses roots $\alpha_1, ..., \alpha_k$. Let $n_1, ..., n_k$ be the corresponding orders of these roots of unity. Let $N = n_1 ... n_k$, and let $\omega = \exp(2\pi i/N)$. Then every α_j has the form ω^k for some k. So, Herstein's proof works if F contains ω.

Now we will not suppose that F contains ω. Let E be the splitting field of p. Let $\widetilde{F} = F(\omega)$. Let $\widetilde{E}$ be the splitting field of p over $\widetilde{F}$. Since $\widetilde{E}$ contains all the roots of p, we know that $\widetilde{E}$ contains an isomorphic copy of E. So, we might as well assume that $E \subset \widetilde{E}$. We have two different chains,

$$F \subset \widetilde{F} \subset \widetilde{E}, \qquad F \subset E \subset \widetilde{E}.$$

The result in Herstein says that $G(\widetilde{E}, \widetilde{F})$ is solvable. We now prove that $G(E, F)$ is solvable.

Note that $\widetilde{E}$ is the splitting field, over F, of the polynomial $p(x)(x^N - 1)$. Hence $\widetilde{E}$ is normal over F. Also E is normal over F. Therefore

$$G(E, F) = G(\widetilde{E}, F)/G(\widetilde{E}, E).$$

The quotient of a solvable group is solvable so, to finish our proof, we just have to show that $G(\widetilde{E}, F)$ is solvable.

Now, $\widetilde{F}$ is normal over F, because it is the splitting field for $x^N - 1$. Therefore,

$$G(\widetilde{F}, F) = G(\widetilde{E}, F)/G(\widetilde{E}, \widetilde{F}).$$

Let

$$\psi : G(\widetilde{E}, F) \to G(\widetilde{F}, F)$$

be the restriction map. Consider the commutator series for $G(\widetilde{E}, F)$. This series of subgroups is mapped into the commutator series for $G(\widetilde{F}, F)$, an abelian group. Hence, the commutator series for $G(\widetilde{E}, F)$ eventually shrinks down until it is in the kernel of ψ, namely in $G(\widetilde{E}, \widetilde{F})$. But this group is solvable. So, our original commutator series eventually lies in a solvable group and therefore shrinks down to the trivial group. This proves that $G(\widetilde{E}, F)$ is solvable.

3. The Vandermonde Matrix: The second portion of these notes discusses what is known as the Vandermond matrix. We will use the result here in the next section. Let p be prime and let $\alpha_k = \exp(2\pi ik/p)$. The numbers $\alpha_1, ..., \alpha_p$ are the distinct pth roots of unity. Actually, the result we prove doesn't use the fact that p is prime, but this is the case that we will need below.

Let

$$M_j = (\alpha_j, \alpha_{2j}, ..., \alpha_{pj}) \tag{1}$$

Let M be the matrix with rows $M_1, ..., M_p$. Our goal is to show that M has nonzero determinant. This is equivalent to showing that the vectors $M_1, ..., M_p$ are linearly independent in the vector space $\boldsymbol{C}^p$.

We introduce the *Hermitian inner product*

$$\langle (z_1, ..., z_p), (w_1, ..., w_p) \rangle = \sum_{i=1}^{p} z_i \overline{w}_i. \tag{2}$$

Here $\overline{w}_i$ is the complex conjugate of w_i. This gadget works very much like a dot product. It obeys the following rules.

- $\langle Z_1 + Z_2, W \rangle = \langle Z_1, W \rangle + \langle Z_2, W \rangle$
- $\langle aZ, W \rangle = a\langle Z, W \rangle$.
- $\langle W, Z \rangle = \overline{\langle Z, W \rangle}$.

(We don't actually need to know the third rule, but it is worth stating anyhow.)

We check easily that

$$\langle M_i, M_i \rangle = p; \qquad \langle M_i, M_j \rangle = 0 \tag{3}$$

when $i \neq j$. Supposing that $c_1 M_1 + ... c_p M_p = 0$, we would get

$$\langle c_1 M_1 + ... + c_p M_p, M_j \rangle = p c_j = 0. \tag{4}$$

Hence $c_j = 0$. But j is arbitrary. Hence $c_1, ..., c_p = 0$. This proves that the vectors $M_1, ..., M_p$ are linearly independent. Hence $\det(M)$ is nonzero.

4. Converse to the Solvability Result: Now we prove the converse to the result in Herstein – without any assumptions about roots of unity. I'm adapting this proof from Jacobsen's book, *Algebra*. Let F be a field of characteristic zero and let $p(x) \in F[x]$ be a polynomial. Let E be the splitting field of $p(x)$. Suppose that $G(E, F)$ is solvable.

Let N be the order of $G(E, F)$. Let $\omega = \exp(2\pi i N)$. Let $\widetilde{F} = F(\omega)$ and let $\widetilde{E}$ be the splitting field of p over $\widetilde{E}$. Note that $\widetilde{E} = E(\omega)$. An argument similar to the one above shows that $G(\widetilde{E}, \widetilde{F})$ is also solvable. So, in our proof, we can assume without loss of generality that $\omega \in F$.

Let $G = G(E, F)$. We can find a sequence $(e) = G_n \subset G_{n-1} ... \subset G_0 = G$ such that each G_i is normal in G_{i-1} and $H_i = G_{i-1}/G_i$ is abelian. Suppose there is some index i such that H_i is not cyclic of prime order. We have a surjection $\phi : G_{i-1} \to H_i$ and we let $G_i' = \phi^{-1}(H_i')$, where H_i' is some nontrivial subgroup of H_i. Then G_i' is normal in G_i and G_{i-1} is normal in G_i', and the two quotients G_{i-1}/G_i' and G_i'/G_i are both abelian. In short, if H_i is not cyclic of prime order, we can insert another group in our sequence. So, we can assume that G_{i-1}/G_i is cyclic of prime order for all i. Note that all these prime orders divide N. Corresponding the sequence of groups, we can find a tower of fields

$$F = F_0 \subset ... \subset F_n = E$$

such that $[F_i : F_{i-1}]$ has prime order for all i.

Note that all the primes involved divide N. In particular, if $[F_{i-1} : F_i] = p$ then F_{i-1} contains all the pth roots of unity. The following lemma finishes the proof.

Lemma 0.2 *Let K be a normal field extension of F of degree p, with p prime. Suppose also that F contains all the pth roots of unity. Then we have $K = F(a)$ where $a^p \in F$.*

Proof: Let $\alpha_k = \exp(2\pi i k/p)$. Then $\alpha_1, ..., \alpha_p$ are the pth roots of unity. We can write $K = F(c)$ for some $c \in K$. The group $G(K, F)$ has order p

and hence is cyclic. Let η be a generator of $G(K,F)$. Note that $\eta(\alpha_k)=\alpha_k$ since $\alpha_k \in F$. Consider the sums

$$d_k = \alpha_k \eta(c) + \alpha_{2k}\eta^2(c) + ... + \alpha_{pk}\eta^p(c). \tag{5}$$

We have $\eta(d_k) = d_k/\alpha_k$. Therefore $\eta(d_k^p) = d_k/\alpha_k^p = d_k^p$. So, d_k^p is fixed by $G(K,F)$. Since K is normal over F, we have $d^k \in F$. To finish the proof, we just have to show that some d_k does not belong to F.

We can write Equation 5 in matrix form, as $D = MC$, where

$$D = (d_1, ..., d_p), \qquad C = (c_1, ..., c_p).$$

Here $c_j = \eta^j(c)$ and M is the *Vandermonde matrix*. We have already seen that $\det(M) \neq 0$. Hence M is invertible and we can write $C = M^{-1}D$. But then c is expressible as a linear combination of $d_1, ..., d_p$. Since $c \notin F$, we must have $d_k \notin F$ for some k. This means that $K = F(d_k)$ because the irreducible polynomial for d_k must have degree p. ♠