MATH 123 SOLUTION SET 4

MD

Lang 4.1

Since $x^n - 1$ is of degree n, it has n roots in some algebraic closure; since the elements $e^{\frac{2\pi i r}{n}}$ $(1 \leq k \leq n)$ are all nth roots of unity, they are the roots. However, if $(r, n) \neq 1$, say $(r, n) = k$, then the root has period $\frac{n}{k}$ $(\frac{n}{k} < n)$. So the primitive roots of unity are the others.

Lang 4.2

K is Galois over F because it is the splitting field for $x^n - 1$ (since ζ generates all roots of that equation, as above). Since all roots of $x^n - 1$ are ζ^k for some k, and automorphisms carry roots to roots, and an automorphism of $F(\zeta)$ is completely defined by action on ζ, we can write $\sigma(\zeta) = \zeta^{r(\sigma)}$ and thereby describe all automorphisms. But then

$$\sigma \circ \tau(\zeta) = \sigma(\zeta^{r(\tau)}) = (\zeta^{r(\sigma)})^{r(\tau)} = \zeta^{r(\sigma)r(\tau)} = \tau \circ \sigma(\zeta).$$

So the Galois group is abelian.

Lang 4.3(a)

We claim that $K_1K_2 = K(\alpha_1, \alpha_2)$ is the splitting field of $f_1 \cdot f_2$, where $f_i = \mathrm{irr}(\alpha_i, F)$. Since K_i are Galois, they contain all roots of the respective polynomials, and K is the smallest field containing both. Conclude that K is a Galois extension.

Now where G is the Galois group of K over F, consider the map

$$\begin{aligned} \phi : G &\rightarrow \mathrm{Gal}(K_1, F) \times \mathrm{Gal}(K_2, F) \\ \sigma &\mapsto (\sigma_1, \sigma_2) \end{aligned}$$

where the $\sigma_i = \sigma|_{K_i}$. The key fact is that if $a \in K_i$, then $\sigma_i(a) \in K_i$ as well; this is true because K_i are given to be Galois, so all embeddings are automorphisms, so the σ_i keep elements of K_i within K_i. This means that $(\sigma\tau)_i = \sigma_i\tau_i$, which means that ϕ is a homomorphism.

Now consider an arbitrary $\mu \in \ker \phi$. μ must restrict to the identity on both K_1 and K_2, so it must fix both α_1 and α_2, but then it fixes all of $K = F(\alpha_1, \alpha_2)$. Thus ϕ is injective.

Finally, assume $K_1 \cap K_2 = F$. This means that $[K_1K_2 : K_2] = [K_1 : F]$ (Lang p. 267), or equivalently $[F(\alpha_1, \alpha_2) : F(\alpha_2)] = [F(\alpha_1), F]$.

But the full extension degree has

$$[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_2)][F(\alpha_2) : F] = [F(\alpha_1) : F][F(\alpha_2) : F]$$

and we know that the degree of the Galois group is the degree of the extension. But $|\mathrm{Gal}(K_i, F)| = [K_i : F] = [F(\alpha_i) : F]$, so

$$|\mathrm{Gal}(K_1, F) \times \mathrm{Gal}(K_2, F)| = [F(\alpha_1) : F][F(\alpha_2) : F].$$

But then since ϕ is injective and the dimensions of domain and range match, we conclude that ϕ is an isomorphism.

Date: March 3, 1997.

Lang 4.4

(a) $\mathrm{Gal}(K, K\cap E)$ is a subgroup of $\mathrm{Gal}(K,F)$, and a subgroup of an abelian group must be abelian. But then $\mathrm{Gal}(KE,E) \simeq \mathrm{Gal}(K, K\cap E)$ by Theorem 4.5, page 266. So KE is abelian over E.

(b) We know from the last problem that the compositum of Galois extensions is Galois, so K_1K_2 is Galois over F. Under the same map ϕ that we used in the last problem (a useful map), we find the image of $\sigma\tau$ to be $(\sigma_1\tau_1, \sigma_2\tau_2)$ for an arbitrary $\sigma, \tau \in \mathrm{Gal}(K_1K_2, F)$. But since the K_i are assumed abelian, this is the same as $(\tau_1\sigma_1, \tau_2\sigma_2)$, which certainly has $\tau\sigma$ as a preimage under ϕ. But since ϕ is injective, the preimage is unique, so $\sigma\tau = \tau\sigma$. So $\mathrm{Gal}(K_1K_2, F)$ is abelian, so we say K_1K_2 is abelian over F.

(c) & (d). We will solve these together by letting G^c denote the commutator subgroup of $\mathrm{Gal}(K,F)$ and then demonstrating that K^{G^c}, its fixed field, is a maximal abelian subextension.

Let G^c be the subgroup of $G = \mathrm{Gal}(K,F)$ generated by all elements of the form $\sigma\tau\sigma^{-1}\tau^{-1}$.

First, we show that $G^c \lhd \mathrm{Gal}(K,F)$. Take an arbitrary generator for G^c and conjugate it by some $\mu \in \mathrm{Gal}(K,F)$. Notice

$$\mu \cdot \sigma\tau\sigma^{-1}\tau^{-1} \cdot \mu^{-1} = (\mu\sigma\mu^{-1})(\mu\tau\mu^{-1})(\mu\sigma\mu^{-1})^{-1}(\mu\tau\mu^{-1})^{-1},$$

which is of the right form to ensure that it is in G^c. So G^c is a normal subgroup. This means also that its fixed field, K^{G^c}, is a Galois extension of F.

Lemma. *For any $H \lhd G$, G/H abelian $\iff G^c \subset H$.*

Proof. For $x \in G$, let $\dot{x}$ denote the coset of x in G/H. $(\Rightarrow)$ $\dot{x}\dot{y}\dot{x}^{-1}\dot{y}^{-1} = 1$ for all $\dot{x}, \dot{y} \in G/H$. Thus, $xyx^{-1}y^{-1}$ is in the kernel of the projection map, so it is in H. So $G^c \subset H$.
$(\Leftarrow)$ $\forall x, y \in G, xyx^{-1}y^{-1} \in G^c \implies xyx^{-1}y^{-1} \in H \implies \dot{x}\dot{y}\dot{x}^{-1}\dot{y}^{-1} = 1$ in G/H. But this means $\dot{x}\dot{y} = \dot{y}\dot{x}$ always. ☐

Now we check that K^{G^c} is a maximal abelian subextension. First of all, K^{G^c} itself is abelian by a direct application of the lemma, since $G/G^c = \mathrm{Gal}(K^{G^c}, F)$.

Now for any other $E \subset K$ which is abelian over F, we need to show that $E \subset K^{G^c}$. Well, $\mathrm{Gal}(E,F) = \mathrm{Gal}(K,F)/\mathrm{Gal}(K,E)$ and $\mathrm{Gal}(E,F)$ is abelian by construction, so by the lemma we conclude that $G^c \subset \mathrm{Gal}(K,E)$. But then G^c fixes everything $\mathrm{Gal}(K,E)$ fixes and maybe more, so $E \subset K^{G^c}$.

Lang 4.5

(a) We have $\mathrm{Gal}(KE,E) \simeq \mathrm{Gal}(K, K\cap E)$ by Theorem 4.5, page 266. But we notice that $\mathrm{Gal}(K, K\cap E)$ is a subgroup of $\mathrm{Gal}(K,F)$, which is cyclic by hypothesis. Subgroups of cyclic groups are cyclic, as we know from our deep mastery of group theory. This gives the result, since the image of the generator for $\mathrm{Gal}(K, K\cap E)$ under the isomorphism with $\mathrm{Gal}(KE,E)$ will be the generator we desire.

(b) No. A canonical counterexample:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}) = \mathbb{Z}_2; \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{3}), \mathbb{Q}) = \mathbb{Z}_2; \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Lang 4.7 and 4.8 Since 7 is a special case of 8, we will solve the generalization.

Let α be (say) the real root of $t^n - a$. Then all of the roots are $\{\alpha\zeta^k\}$, for ζ a primitive nth root of unity. Since F contains the roots of unity, $\operatorname{split}(t^n - a) = F(\alpha)$, so its automorphisms are totally determined by their action on α. Thus $\sigma : \alpha \mapsto \alpha\zeta$ generates a cyclic group of automorphisms. The automorphism group will always be a subgroup of this copy of $\mathbb{Z}_n$. Now, if the polynomial is irreducible, then we know we have $[F(\alpha), F] = n$, so there are n embeddings, thus n automorphisms, thus the full cyclic group is realized as automorphisms.

[A note on the special case in problem 7: reducibility occurs precisely when $\alpha^2 \in F$ because then $t^4 - a = (t^2 - \alpha^2)(t^2 + \alpha^2)$. This forces us to discard two of the four potential automorphisms because the maps taking $\alpha \mapsto i\alpha$ and $\alpha \mapsto -i\alpha$ do not fix α^2, which must be fixed if it is in F.]

Lang 4.9 Oops. I did this in section, didn't I?

Well, $t^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein. Its roots, where $\alpha = \sqrt[4]{2}$, are $\{\pm\alpha, \pm i\alpha\}$, and $\mathbb{Q}(\alpha, i)$ is a splitting field. Now we note that $i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, and so $\operatorname{irr}(i, \mathbb{Q}) = t^2 + 1$ is still irreducible over $\mathbb{Q}(\alpha)$, giving $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$. Since $[Q(\alpha) : \mathbb{Q}] = 4$, we get $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$, so this is the size of the Galois group.

Note that the result from problem 8 applies to tell us that $\operatorname{Gal}(\mathbb{Q}(\alpha, i) : \mathbb{Q}(i)) \subset \mathbb{Z}_4$ and since $t^4 - a$ remains irreducible over $\mathbb{Q}(i)$, it is a full copy of $\mathbb{Z}_4$; this is the cyclic subgroup of order 4 in the Galois group of the splitting field.

Lang 4.10

For a quick-n-dirty example, consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. $\mathbb{Q}(\sqrt{2})$ splits $x^2 - 2$ over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2}$ splits $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$ but $\mathbb{Q}(\sqrt[4]{2})$ does not split $\operatorname{irr}(\sqrt[4]{2}, \mathbb{Q}) = x^4 - 2$ since you need some complex numbers to do that. Subtler examples are available.