Problems in Lang's Algebra

Edward Kim

July 17, 2019

Lang Chapter 1 (Groups)

Problem 6

Question: Prove that the group of inner automorphisms of a group G are normal in $Aut(G)$.

Proof. Let $\mathcal{L} \in Aut(G)$ and $Inn(G)$ be the subgroup of inner automorphisms of G. It follows from our definitions that for any $y \in G$,

$$(\mathcal{L} \circ Inn(G) \circ \mathcal{L}^-1)(y) = (\mathcal{L} \circ Inn(G))(\mathcal{L}^-1(y)) = \mathcal{L}(x\mathcal{L}^{-1}(y)x^{-1}) = \mathcal{L}(x)y\mathcal{L}^{-1}(x) \in Inn(G)$$

Since $x \in G$ was arbitrary, we see that $\mathcal{L} \circ Inn(G) \circ \mathcal{L}^-1 \subseteq Inn(G)$. Hence, $Inn(G) \trianglelefteq Aut(G)$. □

Problem 7

Question: Let G be a group such that $Aut(G)$ is cyclic. Prove that G is abelian.

Proof. By Proposition 4.2 (Lang 42), the group of inner of automorphisms $Inn(G)$ is also cyclic. Let $G \to Inn(G)$ be the surjective homomorphism $x \mapsto c_x$. The kernel of this map is the center of $Z(G)$ of the group. Hence, $G/Z(G) \cong Inn(G)$. It suffices to prove that if $G/Z(G)$ is abelian, then G must be abelian. We can simply take this in two cases. If we have $a, b \in G$, let's take the case where they both occupy the same coset. Thus, $ab^{-1} \in Z(G)$. We can use this for the following equivalences:

$$ab = a(b^{-1}b)b = (ab^{-1})bb = b(ab^{-1})b = ba$$

Hence, any two elements in the same coset must commute. As the factor group is cyclic, let x be a generator for $G/Z(G)$. Then given that $a, b \in G$ live in different cosets, a, b must occupy a coset with some power of x. Since the powers of x trivially commute and a, b commute with the generators, it follows that a, b must commute and the proposition follows. □

Problem 9

1. Question: Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index.

   Proof. Let $(G : H) = n$. We can construct a homomorphism $\phi : G \to S_n$ by conjugating the coset representatives labeled up to n for all $g \in G$. It follows that $Ker(\phi) \subseteq H$. Let $N = Ker(\phi)$. Then by our isomorphism theorems, G/N is isomorphic to it's image which is finite and the proposition follows. □

2. Question: Let G be a group and let H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.

   Proof. Consider the cosets of G/H_1. By assumption, the number of cosets $(G : H_1)$ is finite. Pick any coset C and consider how the elements partition into the cosets of $(G/(H_1 \cap H_2)$ by cases. Let $a, b \in C$ be any two elements of our coset. If $ab^{-1} \in H_2$, then it aligns with a coset of H_2. Otherwise, the two elements split into separate cosets in $G/(H_1 \cap H_2)$, namely a coset where $ab^{-1} \in H_2$ as well. However, the number of cosets it could move into is bounded by $(G : H_2)$. Thus, the number of unique cosets that could be generated by this method is bounded by $(G : H_1)(G : H_2)$ which is finite. Hence, $H_1 \cap H_2$ is of finite index. □

0.1 Problem 12 (Semidirect Product)

1. $x \mapsto \gamma_x$ induces a homomorphism $f : H \to Aut(N)$ since

$$f(yz) = x(yz)x^{-1} = (xyx^{-1})(xzx^{-1}) = f(x)f(y)$$

2. We first note that the kernel of the map $\phi : H \times N \to HN$ is trivial. Let $f(e, n_1) = e$, then $en = e$ and $n = e$. A symmetric argument can be done on the left. Since $H \cap N = \{e\}$, it follows that the kernel is trivial. Surjection follows immediately from the definition of the map. Hence, ϕ is a bijective map. To show that this map is an isomorphism of groups, it suffices to prove that ϕ is a homomorphism if and only if f is the trivial map. Starting with the converse, if f is the trivial map, then $hnh^{-1} = n$ for any $n \in N, h \in H$. Hence,

$$\phi(h_1h_2, n_1n_2) = (h_1h_2)(n_1n_2) = (h_1h_2)(n_1(h_2^{-1}h_2)n_2) =$$
$$h_1(h_2n_1h_2^{-1})h_2n_2 = (h_1n_1)(h_2n_2) - \phi(h_1, n_1)\phi(h_2, n_2)$$

Now if ϕ is a homomorphism, then by our observation above,

$$(h_1h_2)(n_1n_2) = (h_1n_1)(h_2n_2)$$

Taking the proper left and right inverses yield the following:

$$h_2n_1h_2^{-1} = n_1$$

By taking h_2, n_1 to be any element in H, N respectively, we conclude that f is indeed trivial.

3. Let N, H be subgroups. Define $\psi : N \to Aut(H)$ to be our above homomorphism. We will construct the semidirect product as follows: Let $x \in N, h \in H$ and construct the set made of elements of the form (x, h). Define the composition law as follows:

   $$(x_1, h_1)(x_2, h_2) = (x_1\psi(h_1)x_2, h_1h_2)$$

   We will first show that this indeed follows the group laws. Associativity easily follows from the underlying property of groups N, H. The identity exists from $e_N, e_H, \psi(e_N) = id_H$. The inverse also exists since

   $$(x, h)(\psi^{-1}(h)x^{-1}, h^{-1}) = (e_N, e_H)$$

   Hence, the set is a group. We will now show that this yields a semidirect product on N and H by associating N with $(n, 1)$ and H with $(1, h)$.

   We immediately note that $N \cap H = \{e\}$. Thus, it suffices to prove that NH is isomorphic to our group through a map $\theta : NH \to G, nh \mapsto (n, h)$. First, we show that θ is indeed a homomorphism.

Note: We can extend this definition for H be the normalizer of any subgroup N. Then the map f would be the homomorphism from $Norm(N) \to Aut(N)$.

Note: We note why the map f above is so significant. What's stopping the map $H \times N \to HN$ is precisely the conjugation issue $(hnh^{-1} = n)$ for all $n \in N, h \in H$.

Problem 17

Question: Let X, Y be finite sets and let $C \subseteq X \times Y$. For $x \in X$, let $\phi(x) = |\{y \in Y | (x, y) \in C\}|$. Verify that $|C| = \sum_{x \in X} \phi(x)$

Proof. Let $|X| = n_1$ and $|Y| = n_2$. □

Problem 18

Proof. We use Problem 17 by taking our set to be $S \times T$ and our subset C to be the entirety of $S \times T$. The result follows from the finite sum shown above. □

Problem 19

1. *Proof.* This follows by weighting the cardinality of orbit G_s for each element. □
2. *Proof.* By Lagrange's Theorem, we know that $|G : G_s| = |G|/|G_s|$ where G_s is the stabilizer of $s \in S$. By the part above:

$$\sum_{t \in Gs} \frac{1}{|Gt|} = \frac{1}{|G|} \sum_{t \in Gs} |G_t| = 1$$

Hence, we can add this sum over all coset representatives S_r:

$$\frac{1}{|G|} \sum_{s_r \in \mathcal{O}} \sum_{t \in Gs_r} |G_t| = |\{\mathcal{O}_i\}|$$

where $\{\mathcal{O}_i\}$ is the set of orbits of G in S. Finally, we note that the following sums are equivalent:

$$\sum_{s \in Gs} |Gs| = \sum_{g \in G} f(x)$$

where $f(x)$ is the number of fixed points $x \in G$ exhibits. Substituting the sum yields our desired result:

$$\frac{1}{|G|} \sum_{g \in G} f(x) = |\{\mathcal{O}_i\}|$$

□

Lang Chapter 2 (Rings)

0.2 Problem 10

Let D be an integer greater than or equal to 1, and let R be the set consisting of elements in the form $a + b\sqrt{-D}$ where $a, b \in \mathbb{Z}$.

1. *Proof.* We begin by showing that R is indeed a ring under the usual addition and multiplication operations over $\mathbb{C}$. We can see that indeed $r + s = (a_1 + b_1\sqrt{-D}) + (a_2 + b_2\sqrt{-D} = (a_1 + a_2) + (b_1 + b_2)\sqrt{-D}$ for $r, s \in R$. Similarly, $rs = a_1a_2 - b_1b_2D + (a_1b_2 + a_2b_1)\sqrt{-D} \in R$. □

2. *Proof.* We observe that the above observations make R into a subring of $\mathbb{C}$. Thus, there exists an embedding $\phi : R \to \mathbb{C}$ which is a ring homomorphism. Let $\star : \mathbb{C} \to \mathbb{C}$ denote the complex conjugation map. As $\star$ is an automorphism, we can compose the maps $\phi^{-1} \circ \star \circ \phi : R \to R$ to yield an automorphism for R.s □

0.3 Problem 11

- Define the ring of trigonometric functions as the polynomial ring $\mathbb{R}[\sin(x), \cos(x)]$.

1. *Proof.* We shall prove that the elements $f(x)$ of the trigonometric polynomial ring R above can be expressed in the following form:

$$f(x) = a_0 + \sum_{m=1}^{n} a_m \sin(mx) + b_m \cos(mx)$$

where $a_m, b_m, a_0 \in \mathbb{R}$.

Every $f \in \mathbb{R}[\sin(x), \cos(x)]$ can be reduced to the form above by associativity and commutivity of the addition and multiplication operations in the field $\mathbb{R}$ and subsequently point-wise multiplication of $\sin(x), \cos(x) \in C(\mathbb{R})$. We invoke the following identities to reduce products of $\sin^m(x), \cos^m(x)$ to products of $\sin(mx), \cos(mx)$:

$$\cos^2(x) = \frac{1 + \cos(2x)}{2}$$

$$\sin^2(x) = \frac{1 - \cos(2x)}{2}$$

We note that by the first and second identities, we can reduce terms of the forms $\cos^{2m}(x), \sin^{2n}(x)$ to the desired forms $(\frac{1+\cos(2x)}{2})^m, (\frac{1-\cos(2x)}{2})^m$ respectively. Futhermore, we have the product-to-sum identities:

$$\sin(x)\sin(y) = \frac{1}{2}[\cos(x - y) - \cos(x + y))]$$

$$\cos(x)\cos(y) = \frac{1}{2}[\cos(x - y) + \cos(x + y))]$$

It is routine verification to see that the combination of the above identities with associativity yields the desired forms for terms $\sin^m(x), \cos^m(x)$. We handle terms of mixed powers of $\sin(x), \cos(x)$ by the similar product-to-sum identity:

$$\sin(x)\cos(y) = \frac{1}{2}[\sin(x - y) + \sin(x - y))]$$

Once again, we inductively reduce the powers of $\sin(x), \cos(x)$ to the forms above then invoke the mixed product-to-sum identity. Combining these reductions, we can inductively reduce the elements of the trigonometric polynomial ring to the desired form, thus concluding the proof.

□

2. *Proof.* We now prove that $\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$. Without loss of generality, let $f = a_0 + ... + a_r \cos(rx)$ and $g = b_0 + ... + b_s \cos(sx)$. By multiplying f, g, we yield $fga_0b_0 + .. + a_rb_s \cos(rx)\cos(sx)$. By the product-to-sum identities above, we can reduce this product to the sum

$$a_rb_s \cos(rx)\cos(sx) = \frac{a_rb_s}{2}[\cos((r - s)x) + \cos((r + s)x)]$$

Since $a_r, b_r \neq 0$, $a_rb_r \neq 0$, and $\cos(r + s)x$ is the term with maximum degree by definition above. The equality immidiately follows and we see that R cannot have any zero divisors since the sum of two positive degrees can never be zero. □

0.4 Problem 12

• Let P be the set of positive integers. Define the ring R as the set of the functions defined on the set P with values in a commutative ring K with the sum defined to be the pointwise addition of functions and the convolution product to be dictated by the formula

$$(f \star g)(m) = \sum_{xy=m} f(x)g(y)$$

1. *Proof.* We first prove that R is a commutative ring with the unit of R defined to be the function δ which takes $\delta(1) = 1_K$ and $\delta(x) = 0_K$ for $x \neq 1$. To see that R is commutative we note that by the commutativity of K,

   $$\sum_{xy=m} f(x)g(y) = \sum_{yx=m} g(y)f(x)$$

   By commutativity of P, taking the sum over all factors of m yields

   $$\sum_{yx=m} g(y)f(x) = \sum_{xy=m} g(x)f(y) = (g \star f)(m)$$

   Let δ be the function as defined above. For $f \in R$.

   $$(f \star \delta)(m) = \sum_{xy=m} f(x)\delta(y) = f(m)\delta(1) = f(m)$$

   for $m \in P$. As the convolution product agrees with f for all elements in P, δ serves as our unit 1_R. □

2. *Proof.* Suppose we have multiplicative functions $f, g \in R$. Let $m, n \in P$ be relatively prime postive integers. Then:

   $$(f \star g)(mn) = \sum_{xy=mn} f(x)g(y)$$

   We note that x, y can be decomposed into $x = x_1y_1$ and $y = x_2y_2$ where $x_1x_2 = m$ and $y_1y_2 = n$. Since m, n are relatively prime, it follows that x_1, y_1 and x_2, y_2 are also relatively prime. Hence, we can decompose the product as such

   $$\sum_{xy=mn} f(x)g(y) = \sum_{xy=mn} f(x_1)f(y_1)g(x_2)g(y_2) = \sum_{xy=mn} f(x_1)g(x_2)f(y_1)g(y_2) =$$

$$[\sum_{x_1y_1=m} f(x_1)g(y_1)][\sum_{y_1y_2=n} f(y_1)g(y_2)] = (f \star g)(m)(f \star g)(n)$$

Thus, we see that the product is also multiplicative. We see in particular that the set of multiplicative functions endowed with the addition and multiplication operations of R forms a subring of R. □

3. *Proof.* Let μ be the Mobius function defined as follows: $\mu(1) = 1, \mu(p_1...p_r) = (-1)^r$ for $p_1, ..., p_r$ distinct primes, and $\mu(x) = 0$ if $p^2|x$ for some prime p. We first prove that μ is multiplicative. Indeed, let m, n be relatively prime postive integers. We can product mn as a product of distinct prime powers. $\mu(mn) = 0$ if either m, n contains a non-trivial prime power. Thus, it suffices to take the case where mn can be written as a product of single prime powers. Let $m = p_1...p_r$ and $n = p_{r+1}...p_{r+s}$ where all primes are distinct, then $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. Hence, μ is multiplicative.

   Now consider the convolution product $(\mu * \phi_1)$ where ϕ_1 is the constant function taking values to 1. We can expand the product as follows: Let $m = p_1^{a_1}...p_r^{a_r}$

$$(\mu \star \phi_1)(p_1^{a_1}...p_r^{a_r}) = \sum_{i=1}^{r} \binom{r}{i} (-1)^i$$

   If $m = 1$, then the product is 1 trivially. If $m \neq 1$, then the sum vanishes (proof?). Thus, $(\mu \star \phi_1) = \delta$. □

Lang Chapter 3 (Modules)

0.5 Problem 14

Consider the following commutative diagram:

$$\begin{tikzcd}
 & M' \arrow[r, "\phi_1"] \arrow[d, "f"] & M \arrow[r, "\phi_2"] \arrow[d, "g"] & M'' \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\psi_1"] & N \arrow[r, "\psi_2"] & N'' &
\end{tikzcd}$$

1. Let us prove that if f, h are monomorphisms, then g is also a monomorphism. It suffices to show that if $g(x) = 0_N$, then $x = 0_M$. Since h is a monomorphism, $\ker h = \{0_{M''}\}$. Thus, by the exactness of the top row and commutativity of the rightmost square, $x \in \text{img } \phi_1 \cap \ker g$. Since $x \in \text{img } \phi_1$, there exists $a \in M'$ such that $\phi(a) = x$. By commutativity of the leftmost square, $\psi(f(a)) = 0_N$. However, f is a monomorphism and so is ψ_1 by the exactness of the bottom row. Hence, $a = 0_{M'}$ and $x = \phi_1(a) = 0_M$

Lang Chapter 4 (Polynomials)

0.6 Problem 1

1.