UT Putnam Prep 2017-10-06 — Group Theory – some answers

1. In the additive group of ordered pairs of integers (m, n) (with addition defined componentwise), consider the subgroup H generated by the three elements

$$(3, 8) \qquad (4, -1) \qquad (5, 4).$$

Then H has another set of generators of the form

$$(1, b) \qquad (0, a)$$

for some integers a, b with $a > 0$. Find a. [Putnam 1975-B1]

ANSWER: To clarify, H is the set of ordered pairs of the form $x(3, 8) + y(4, -1) + z(5, 4)$ where x, y, z range over all integers. This set includes both $u = (-1)(3, 8) + (-3)(4, -1) + (3)(5, 4) = (0, 7)$ and $v = (1)(3, 8) + 2(4, -1) + (-2)(5, 4) = (1, -2)$ and hence the group K that they generate; that is, $K \subseteq H$. On the other hand $2u + 3v = (3, 8)$, $u + 4v = (4, -1)$, and $2u+5v = (5, 4)$, so K contains the subgroup that these three pairs generate, i.e. $H \subseteq K$. Together, these inclusions show $H = K$, i.e. we have a pair of generators of the type desired.

It's not obvious but it is true that $a = 7$ is the *only* positive value for which this is true. (On the other hand, b is only determined mod 7.) In group-theoretic terms we are saying that H is a subgroup of index 7 in $\mathbf{Z}^2$. Warning: there are groups generated by 2 elements with subgroups which cannot be generated by 2 elements.

2. Let r, s, t be positive integers that are relatively prime in pairs. Let G be an abelian group and a, b be elements of G. Suppose $a^r = b^s = (ab)^t = e$ (the identity element of G). Show that $a = b = e$.

ANSWER: Since r and t are coprime there exist integers x, y with $rx + ty = 1$. Then $a = a^1 = a^{rx+ty} = (a^r)^x(a^t)^y = e^x(b^{-t})^y = b^{-ty}$, that is, a is a power of b, which means a^s is a power of $b^s = e$. But the only way we can have $a^r = a^s = e$ with r, s coprime is if $a = e$ in the first place: write as above $rz + sw = 1$; then $a = (a^r)^z(a^s)^w = e$, In the same way we discover $b = e$.

Caution: the conclusion is false in non-abelian groups. For example in the icosahedral group there are elements of orders 2 and 3 whose product has order 5.

3. Show that a finite group can not be the union of two of its proper subgroups. Does the statement remain true if "two is replaced by "three? [Putnam 1969-B2]

ANSWER: There is no need to assume the group is finite. Suppose $G = H \cup K$ and that H and K are proper subgroups of G. Pick elements $h \in G \setminus K$ and $k \in G \setminus H$; then $hk \in G$ must lie in either H or K (or both) but this is a contradiction either way: if, say, $hk \in H$ then $k = (h^{-1})(hk)$ would be the product of two elements in H and hence also in H, contrary to its definition. Similarly $hk \in K$ would be a contradiction.

For the desired example let $G = \mathbf{Z}_2 \times \mathbf{Z}_2$, the non-cyclic group of order 4. Then G is the union of its three subgroups of order 2.

4. Let H be a group generated by two elements $x, y \in H$ which satisfy $x^5y^3 = x^8y^5 = e$. Prove that $x = y = e$.

ANSWER: We have $y^3 = (x^{-1})^5$ so $y^6 = (x^{-1})^{10}$. Also $(y^{-1})^5 = x^8$, so we can multiply these last two together and discover $y = x^{-2}$. Then the original equations read $x^{-1} = x^{-2} = e$. Then $x = e$ and as a consequence $y = e^{-2} = e$ as well.

5. Let S be a non-empty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a^n : n = 1, 2, 3, \ldots\}$ is finite. Must S be a group? [Putnam 1989-B2]

ANSWER: Yes. For each a the finitude of the set of powers of a means there exist positive integers $m < n$ with $a^m = a^n$. Let $e = a^{m-n}$. I first claim $ae = ea = a$, i.e. $a^{m-n+1} = a$. This follows from using (left- or right-)cancellation $n-1$ times on the equation $a^m = a^n$. Then note that for any other $b \in S$ we have $a(eb) = (ae)b = ab$ and then $eb = b$ by left cancellation; similarly $be = b$ using right cancellation. So this e is indeed a 2-sided identity element. Now, $a^{m-n-1}a = e$ by definition of e; in the same way b has an inverse among the powers of b in the sense that for some $k > 0$ we have $b^k = e'$ where e' will be a 2-sided identity element for S as well; but then $e = ee' = e'$ forces these two to be equal, so b^{k-1} will be an inverse for b.

6. Let S be a set of real numbers which is closed under multiplication (that is, if a and b are in S, then so is ab). Let T and U be disjoint subsets of S whose union is S. Given that the product of any three (not necessarily distinct) elements of T is in T and that the product of any three elements of U is in U, show that at least one of the two subsets T, U is closed under multiplication. [Putnam 1995-A1]

ANSWER: Suppose neither is closed under multiplication. Then there exist elements $t_1, t_2 \in T$ with $t_1t_2 \notin T$, and elements $u_1, u_2 \in U$ with $u_1u_2 \notin U$. Now all four of these are in S which *is* closed under products, and $S = T \cup U$, so t_1t_2 is an element of U and u_1u_2 is an element of T.

Well then, where is $t_1t_2u_1u_2$? This product can now be interpreted as a product of three elements of T, and hence it lies in T by the premise, or it can likewise be interpreted as the product of three elements of U, and hence also in U. But $T \cap U = \emptyset$ so we have a contradiction.

So one of the two sets must be closed under multiplication.

(I'm guessing that this problem is inspired by the example in which T and U are the set of positive numbers and the set of negative numbers, respectively.)

7. Consider a set S and a binary operation * on S (that is, for each $a, b \in S$, $a * b$ is also in S). Assume that $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$. [Putnam 2001-A1]

ANSWER: Note that unlike the situation in problem 2, these equations hold for *all* a, b in the set, rather than for *particular* a, b. So it may be helpful to rewrite the problem like this: we assume that for each $x, y \in S$ we have $(x * y) * x = y$; then we are given two elements $a, b \in S$ and asked to show $a * (b * a) = b$. To do this, simply use the promised identity first when $x = b$ and $y = a$; then when $x = b * a$ and $y = b$. This tells us first that $(b * a) * b = a$ and second that $((b * a) * b) * (b * a) = b$. Substitute the first into the second to conclude $a * (b * a) = b$.

8. Let x and y be elements in a ring-with-identity ("1"). Prove that if $1 - xy$ is invertible then so is $1 - yx$.

ANSWER: Dennis showed me how to make the answer seem natural. In your heart of hearts you know you expect the inverse of $1 - yx$ to be $1 + yx + (yx)^2 + \ldots$, whatever that means. (Admittedly, this series would usually be meaningless!) But this expression looks rather like $1 + y \cdot r \cdot x$ where $r = 1 + xy + xyxy + \ldots$ which, again just by wishful thinking, you sort of think might be the inverse of $1 - xy$!

So we have proven nothing yet but we have an idea. Let r be the inverse of $1 - xy$, which was given to exist in this ring. Then let $s = 1 + yrx$. We will show that s is indeed an inverse of $1 - yx$. Well, since $r(1 - xy) = 1$, we have that $rxy = r - 1$ so

$$s(1 - yx) = (1 + yrx)(1 - yx) = 1 + yrx - yx - yrxyx = 1 + yrx - yx - y(r - 1)x = 1$$

and similarly from $(1 - xy)r = 1$ we deduce $(1 - yx)s = 1$. Thus s is a two-sided inverse to $1 - yx$, as claimed.

9. Suppose R is a ring in which for every element $a \in R$ we have $a^2 = a$. Show that R is commutative.

ANSWER: For any two elements $x, y \in R$ we may use the premise three times to conclude

$$x^2 = x, \qquad y^2 = y \qquad \text{and} \qquad x^2 + xy + yx + y^2 = (x + y)^2 = x + y$$

Subtracting the first two equations from the third shows that $xy + yx = 0$, i.e. $xy = -yx$. This appears to imply that the ring is *anti-commutative* but notice that if z is any element of R we could apply this conclusion with $x = y = z$ to conclude that $z^2 + z^2 = 0$; since $z^2 = z$ this means $z + z = 0$, i.e., every element of R is its own negative. (The terminology is that R is "of characteristic 2".) Anyway this applies in particular to the element $z = yx$: since it is its own negative, we now have $xy = yx$. Thus every pair of elements of R commute with each other, i.e. R is a commutative ring.

It also happens to be true that if $a^3 = a$ for every $a \in R$ then R is commutative, but this takes a bit longer to prove. The strongest possible conjecture in this direction — "If for every $a \in R$ there is an exponent $a(n) > 1$ for which $a^{n(a)} = a$ then R is commutative — is actually a true theorem, but the proof is quite difficult.

10. Show that if p is prime then $p | F_{2p(p^2-1)}$, where F_k is the kth Fibonacci number. $(F_1 = F_2 = 1)$

ANSWER: I can answer this number-theory question with a bit of group theory.

First define the *Fibonacci vectors* to be the column vectors $v_n = (F_{n+1}, F_n)^t$; then the usual recurrence relation on the Fibonacci numbers shows that

$$v_n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} v_{n-1} \qquad \text{where} \qquad v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and as a consequence $v_n = F^n v_0$ where F is that 2×2 matrix. (This observation allows us to quickly compute e.g. F_{1000} by simply computing a high power of F, which can be done quickly by successive squarings.) We can likewise reduce the Fibonacci numbers modulo p by simply computing F^n mod p, i.e. by computing F^n in the mod-p matrix group $GL(2,p)$. Actually since $\det(F) = -1$ we know F^2 already lies in the smaller group $SL(2,p)$ of matrices with determinant 1.

But this group has order $p(p^2-1)$ (it's the kernel of the determinant surjection $GL(2,p) \to \mathbf{Z}_p^\times$) so by Lagrange's Theorem $(F^2)^{p(p^2-1)} = I$, meaning that $v_{2p(p^2-1)} \equiv v_0 \pmod{p}$. Looking at the lower entry in the vectors then shows $p | F_{2p(p^2-1)}$, as desired.

11. Suppose S is the collection of all subsets of a finite set X. For any $A, B \in S$ we write $A \Delta B$ for the *symmetric difference* of A and B, that is, the set of elements of X which lie in precisely one of A and B (not both). Show that for every $A, B, C, D \in S$

$$A \Delta B = C \Delta D \qquad \iff \qquad A \Delta C = B \Delta D$$

ANSWER: This is a group theory question because under the operation Δ, S becomes a group (of order $2^{|X|}$), with identity element being the empty set, and the inverse of any element $A \in S$ being A itself. The hard part is to prove the associative law but that's not hard once you realize that both $A\Delta(B\Delta C)$ and $(A\Delta B)\Delta C$ may be described as the set of elements of X contained in an odd number of the sets A, B, C, that is, it's the set of $x \in X$ contained either in precisely one of those three sets or in all three of them.

Then we simply use group-theoretic language: if $A\Delta B = C\Delta D$ then "add" first B and then C to both sides of the equation to conclude $A\Delta C = B \Delta D$, and conversely.

(Actually this S is now a group of exponent 2, making it necessarily commutative and thus a vector space over $\mathbf{Z}_p$. You might want to explore this vector space; for example, a natural basis would be the set of singletons $\{x\}$.)